

Data Protection by Design and by Default: A Novel
Business Compliance Framework for Effective Adherence
to EU General Data Protection Regulation (GDPR)

A thesis submitted to the
School of Law, University of Reading
in fulfilment of the requirements
for the degree of Doctor of Philosophy

Virgílio Emanuel Lobato Cervantes

June 2023

Abstract

The General Data Protection Regulation (GDPR) was introduced to safeguard the privacy and personal data of individuals within the European Union. However, despite the legislators' best intentions, organisations have encountered significant challenges in adhering to its requirements, which can sometimes result in a "command that cannot be obeyed."

An area that has been underexplored in the existing literature is Data Protection by Design and by Default (PbDD), which mandates that organisations implement appropriate technical and organisational measures to integrate data protection into their operations. However, issues of GDPR applicability arise due to factors such as the Regulation's lack of certainty, its complexity, and cost of implementation, as well as constraints related to storage limitation and technological compatibility.

My thesis proposes a novel strategy for implementing PbDD, placing emphasis on the principles of data protection and individuals' rights. By adopting this approach, organisations are expected to mitigate many of the risks associated with processing personal data, in line with the requirements of PbDD expressed in Article 25 of the GDPR. This comprehensive PbDD-based compliance framework is referred to as the Data Protection Principles Approach (DPPA).

The DPPA addresses tensions between data security, organisational data needs, and GDPR requirements. It helps ensuring compliance, considering the impact of technological advances and the legal landscape in the EU. It provides stronger mechanisms to safeguard

individuals' rights and enhance control over personal data, while advocating for a policy-driven approach over outdated "win-win" evaluations based on business economics.

In addition to critical reflection and doctrinal legal research, the methodology employed incorporates a distinctive approach to analysing primary data collected specifically for this research, both quantitatively and qualitatively. The data focuses on GDPR fines imposed by regulators in the EU and UK, providing rigorous insights into the edge issues that contribute to the development of the DPPA.

Statement of Original Authorship

I confirm that this is my own work and the use of all material from other sources has been properly and fully acknowledged.

I confirm that this thesis underwent partial electronic proofreading with the assistance of commercial software. The purpose of this proofreading was to identify and correct grammatical errors, capitalisation errors, spelling or typographical errors, misplaced words, errors in sentence structures, and mistakes in punctuation. However, it is important to note that this electronic proofreading did not affect the authorship of the thesis in any way.

Virgilio Emanuel Lobato Cervantes

Word count: 93,402

[This Page Intentionally Left Blank]

List of abbreviations

BCP	Business Continuity Plan
CFR	Charter of Fundamental Rights
CISO	Chief Information Security Officer
CJEU	Court of Justice of the European Union
DPD	Data Protection Directive
DPO	Data Protection Officer
DPPA	Data Protection Principles Approach
DSAR	Data Subject Access Request
ECHR	European Convention of Human Rights
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EC	European Commission
EEA	European Economic Area
EU	European Union
GDPR	General Data Protection Regulation
ICO	Information Commissioner's Office
IRM	Incident Response Methodology
IRMT	Incident Response Management
IP	Internet Protocol
MS	Member State
PbD	Privacy by Design

PbDD Data Protection by design and by default
PET Privacy Enhancing Technology
ROPA Record of Processing Activities
SA Supervisory authority
SME Small and Medium-sized Enterprises
SOP Standard Operational Procedures
SSL Secure Sockets Layer
SSH Secure Shell
TOM Technical and Organisational Measure

Table of Cases

European Court of Human Rights

Amann v Switzerland ECHR 2000-II

Antović and Mirković v Montenegro, App no 70838/13 (ECtHR, 28 November 2017)

Axel Springer AG v Germany [GC], App no 39954/08 (ECtHR, 07 February 2012)

Axel Springer AG v Germany [GC], App no 39954/08 (ECtHR, 7 February 2012)

Bărbulescu v Romania (2017) ECHR 742

Bărbulescu v Romania, App no 61496/08 ECHR 742

Benedik v Slovenia, App no 62357/14 (ECtHR, 24 April 2018)

Biriuk v Lithuania, App no 23373/03 (ECtHR, 25 November 2008)

Bohlen v Germany, App no 53495/09 (ECtHR, 19 February 2015)

Brunet v France, App no 21010/10 (ECtHR, 18 September 2014)

Cemalettin Canlı v Turkey, App no 22427/04 (ECtHR, 18 November 2008)

Ciubotaru v Moldova, App no 27138/04 (ECtHR, 27 April 2010)

Couderc and Hachette Filipacchi Associés v France (2015) ECHR 604

Gaskin v the United Kingdom (1989) Series A no 160

Haralambie v Romania, App no 21737/03 (ECtHR, 27 October 2009)

I v Finland, App no 20511/03 (ECtHR, 17 July 2008)

KH and Others v Slovakia, App no 32881/04 (ECtHR, 28 April 2009)

Khelili v Switzerland, App no 16188/07 (ECtHR, 18 October 2011)

Kirdök and Others v Turkey, App no 14704/12 (ECtHR, 03 December 2019)

Liebscher v Austria, App no 5434/17 (ECtHR, 6 April 2021)

Mikulić v Croatia, App no 53176/99 (ECtHR, 07 February 2002)

Mosley v United Kingdom, App no 48009/08 (ECtHR, 10 May 2011)

Odièvre v France [GC] ECHR 2003-III

PG and JH v the United Kingdom, App no 44787/98 (ECtHR, 25 September 2001)

S and Marper v the United Kingdom (2008) ECHR 1581

Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland ECHR 2017/213

Stefanetti and Others v Italy, Apps nos 21838/10, 21849/10, 21852/10, 21855/10, 21860/10, 21863/10, 21869/10 and 21870/10 (ECtHR, 15 April 2014)

Z v Finland ECHR 1997-I

Court of Justice of the European Union

Case C-101/01, Bodil Lindqvist v Åklagarkammaren i Jönköping EU:C:2003:596, [2003] ECR I-12971

Case C-105/03 Criminal proceedings against Maria Pupino (Reference for a preliminary ruling: Tribunale di Firenze) EU:C:2005:386, [2005] ECR I-05285

Case C-131/12 Google Spain SL, Google Inc v Agencia Española de Protección de Datos, Mario Costeja González EU:C:2014:317

Case C-201/14 Smaranda Bara and Others v Presedintele Casei Nationale de Asigurari de Sanatate and Others (Third Chamber) EU:C:2015:638

Case C-25/17 Jehovan todistajat (GC) (2018) ECLI:EU:C:2018:551

Case C-275/ 06 Productores de Música de España (Promusicae) v Telefonica de España EU:C:2008:54, [2008] ECR I-271

Case C-28/08 P Commission v Bavarian Lager EU:C:2010:378, [2010] ECR I-6005

Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems (Request for a preliminary ruling from the High Court (Ireland)) EU:C:2020:559

Case C-362/14 Maximilian Schrems v Data Protection Commissioner EU:C:2015:650

Case C-398/15 Salavtori Manni v Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce EU:C:2017:197

Case C-40/17 Fashion ID GmbH & CoKG v Verbraucherzentrale NRW eV EU:C:2019:629

Case C-434/16 Peter Nowak v Data Protection Commissioner EU:C:2017:994

Case C-461/10 Bonnier Audio AB and Others v Perfect Communication Sweden AB (Reference for a preliminary ruling from the Högsta domstolen) EU:C:2012:219

Case C-486/12 X, Request for a preliminary ruling from the Gerechtshof te 's-Hertogenbosch EU:C:2013:836

Case C-507/17 Google LLC successor in law to Google Inc v Commission nationale de l'informatique et des libertés (CNIL) EU:C:2019:772

Case C-518/07 European Commission v Federal Republic of Germany (GC) EU:C:2010:125, [2010] ECR I-01885

Case C-524/06 Heinz Huber v Bundesrepublik Deutschland EU:C:2008:724, [2008] ECR I-09705

Case C-536/15 Tele2 (Netherlands) BV and Others v Autoriteit Consument en Markt (Opinion of Advocate General Bot delivered on 9 November 2016 (ACM)) EU:C:2016:845

Case C-543/09 Deutsche Telekom AG v Bundesrepublik Deutschland EU:C:2011:279, [2011] ECR I-03441

Case C-553/07 College van burgemeester en wethouders van Rotterdam v MEE Rijkeboer EU:C:2009:293

Case C-557/07 Lsg-Gesellschaft Zur Wahrnehmung Von Leistungsschutzrechten GmbH v Tele2 Telecommunication GmbH EU:C:2009:107

Case C-582/14 Patrick Breyer v Bundesrepublik Deutschland (Request for a preliminary ruling from the Bundesgerichtshof (Germany)) EU:C:2016:779

Case C-61/19 Orange Romania SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) (Request for a preliminary ruling from the Tribunalul București) EU:C:2020:901

Case C-615/13 P ClientEarth and Pesticide Action Network Europe (PAN Europe) v European Food Safety Authority EU:C: 2015:489

Case C-615/13 P ClientEarth and Pesticide Action Network Europe (PAN Europe) v European Food Safety Authority EU:C:2015:489

Case C-673/17 Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband eV v Planet49 GmbH (Request for a preliminary ruling from the Bundesgerichtshof) EU:C:2019:801

Case C-7/11 Fabio Caronna Reference for a preliminary ruling from the Tribunale di Palermo [2012] EU:C:2012:396

Case C-70/10 Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) EU:C:2011:771

Case C-73/07 Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy EU:C:2008:727, [2008] ECR I-09831

Case C-80/86 Criminal proceedings against Kolpinghuis Nijmegen BV EU:C:1987:431, [1987] ECR 1987 -03969

Case C-91/92, Paola Faccini Dori v Recreb Srl EU:C:1994:292, [1994] ECR I-03325

Case T-259/03 Kalliopi Nikolaou v Commission of the European Communities EU:T:2007:254 206

Joined Cases 205-215/82 Deutsche Milchkontor GmbH and others v Federal Republic of Germany EU:C: 1983:233, [1993] ECR 1983-02633

Joined Cases C-141/12 and C-372/12 YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S EU:C:2014:2081

Joined cases C-201/10 and C-202/10 Ze Fu Fleischhandel GmbH (C-201/10) and Vion Trading GmbH (C-202/10) v Hauptzollamt Hamburg-Jonas EU:C:2011:282, [2011] ECR I-03545

Joined cases C-293/12 and C-594/12 (GC) Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others (C-594/12) EU:C:2014:238

Joined cases C-465/00, C-138/01 and C-139/01 Österreichischer Rundfunk and Others EU:C:2003:294, [2003] ECR I-04989

Joined cases C-468/10 and C-469/10 Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v Administración del Estado EU:C: 2011:777

Table of EU legislation

Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Text with EEA relevance.) OJ L 303, 28.11.2018, p. 59–68

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018.

Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.1.2001, p. 1–22, OJ L 119, 4.5.2016, p. 89–131

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23/11/1995 P. 0031 - 0050 1995 31

Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services, OJ L 337, 18.12.2009, p. 37–69

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly

Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC, 2006

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ L 201, 31.7.2002, p. 37–47 (as amended by Directive 2009/136/EC)

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

Table of International Treaties and Conventions

Charter of Fundamental Rights of the European Union (2000/C 364/01) C/326 18.12.2000.

Consolidate Version of the Treaty on European Union (2012 C/326) C/326 26.10.2012.

Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (L/350/60).

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No.108 1981.

Council of Europe, Protocol (CETS No. 223) amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) 2018 (No 223).

Convention on the protection of the European Communities' financial interests (OJ C 316, 27.11.1995, pp. 48-57).

Table of EU documents, official papers, and policy documents

Article 29 Data Protection Working Party and Working Party on Police and Justice, 'The Future of Privacy - Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data' (Article 29 Data Protection Working Party, Working Party on Police and Justice 2009) 02356/09/EN, WP 168.

Guidelines for identifying a controller or processor's lead supervisory authority, WP 244 Rev.01, 05.04.2017.

Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251 Rev.01, 06.02.2018.

Guidelines on consent under Regulation 2016/679 (GDPR), WP 259 Rev.01, 10.04.2018.

Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248 Rev.01, 04.10.2017.

Guidelines on Data Protection Officers ('DPOs'), WP 243 Rev.01, 05.04.2017.

Guidelines on Personal data breach notification under Regulation 2016/679 (GDPR), WP250 Rev.01, 06.02.2018.

Guidelines on the right to data portability, WP 242 Rev.01, 05.04.2017.

Guidelines on Transparency under Regulation 2016/679 (GDPR), WP260 Rev.01, 11.04.2018.

Opinion 01/2010 on the concepts of 'controller' and 'processor', WP 169, 16.02.2010

Opinion 03/2010 on the principle of accountability, WP 173, 13.07.2010.

Opinion 03/2013 on purpose limitation, WP 203, 02.04.2013.

Opinion 05/2014 on Anonymisation Techniques, WP126, 0829/14/EN.

Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC (2014).

Opinion 15/2011 on the definition of consent, WP 187, 13.7.2011.

Opinion 4/2007 on the concept of personal data, WP 136, 20.06.2007.

Opinion 8/2014 on the on Recent Developments on the Internet of Things 14/EN WP 223.

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS, COM/2021/206 final.

Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks (2014) 14/EN WP 218.

Table of Contents

ABSTRACT	I
STATEMENT OF ORIGINAL AUTHORSHIP	III
LIST OF ABBREVIATIONS	V
TABLE OF CASES	VII
TABLE OF EU LEGISLATION	XII
TABLE OF INTERNATIONAL TREATIES AND CONVENTIONS	XIV
TABLE OF EU DOCUMENTS, OFFICIAL PAPERS, AND POLICY DOCUMENTS	XV
TABLE OF CONTENTS	XVII
LIST OF FIGURES	XXII
LIST OF TABLES	XXVII
ACKNOWLEDGEMENTS	XXVIII
CHAPTER 1 – INTRODUCTION	1
1.1. CONTEXT AND SCOPE OF THE STUDY	16
1.2. DESCRIPTION OF THE RESEARCH PROBLEM AND RESEARCH QUESTION	25
1.3. CONTRIBUTION OF THIS THESIS	36
1.4. DIFFICULTIES ENCOUNTERED THROUGHOUT THE RESEARCH	45
1.5. LIMITATIONS	46
1.6. OUTLINE OF THE CHAPTERS	49
1.7. CONCLUDING REMARKS	52
CHAPTER 2 – LITERATURE REVIEW AND METHODOLOGY	54
2.1. LITERATURE REVIEW AND METHODOLOGY	55
2.2. DATA SOURCES	63
2.3. DATA ANALYSIS (GDPR FINES)	64

2.4.	CORRELATIONAL METHODOLOGY -----	70
2.5.	STEPS CARRIED OUT IN THE ANALYTICAL PROCESS -----	75
CHAPTER 3 – THEORETICAL FRAMEWORKS SHAPING THE DPPA -----		79
3.1.	THE STRATEGY TOWARDS RISK AND THE CONCEPT OF "COLLECTIVE DPIA" WITHIN THE CONTEXT OF THE DPPA-----	87
3.2.	TACKLING THE OPERATIONAL CHALLENGES POSED BY NEW TECHNOLOGIES -----	90
3.3.	SECURING LEGAL CERTAINTY THROUGH THE DPPA -----	96
3.3.1.	<i>Achieving Clarity and Consistency: Exploring the Impact of the EU Principle of Legal Certainty on Data Protection Law</i> -----	99
3.3.2.	<i>Navigating Legal Uncertainty: Examining How the DPPA Addresses Legal Certainty</i> -----	103
3.4.	CONCLUDING REMARKS-----	113
CHAPTER 4 – A CONCEPTUAL ANALYSIS OF PBDD -----		115
4.1.	AN INVESTIGATION INTO THE (PRACTICAL) APPLICATION OF THE PbDD THEORY IN THE CONTEXT OF THE GDPR- 118	
4.1.1.	<i>Overview of the principles of lawfulness, fairness, and transparency underpinning PbDD</i> --	121
4.1.2.	<i>Interrelationships of the lawfulness principle: the rights of data subjects</i> -----	123
3.1.2.1.	The right to be informed-----	125
3.1.2.2.	The right of access-----	126
3.1.2.3.	The right of rectification -----	126
3.1.2.4.	The right of erasure ('right to be forgotten')-----	127
3.1.2.5.	The right to restrict processing-----	127
3.1.2.6.	The right to object-----	129
3.1.2.7.	Rights related to automated decision making and profiling -----	129
4.1.3.	<i>PbDD as a guarantor of the fairness principle</i> -----	131
4.1.4.	<i>A lever for PbDD implementation: the purpose limitation principle</i> -----	134
4.1.5.	<i>PbDD enables information rights: the new principle of transparency in context</i> -----	136
4.1.6.	<i>Data minimisation: PbDD's most powerful ally in achieving GDPR compliance</i> -----	138
4.1.7.	<i>To what degree does PbDD ensure the accuracy of data?</i> -----	139
4.1.8.	<i>Storage limitation: the most significant challenge for PbDD?</i> -----	140
4.1.9.	<i>The data security principle: A "trust-building" facilitator</i> -----	148

4.1.10. <i>PbDD beyond stated intentions: the accountability principle</i> -----	150
4.2. COMPLIANCE THROUGH ACCOUNTABILITY: SHOULD THE LEGISLATOR AIM FOR A MORE PRESCRIPTIVE MODEL OF GDPR INSTEAD? -----	153
4.3. THE DEVELOPMENT OF THE PRACTICAL APPLICATION OF PbDD -----	162
4.4. ASSESSING THE FEASIBILITY OF GDPR'S PbDD IMPLEMENTATION IN PRACTICE -----	168
4.5. CONCLUDING REMARKS -----	175
CHAPTER 5 – REFLECTIONS ON THE CHALLENGES THAT EMERGING TECHNOLOGIES POSE TO PbDD -----	177
5.1. LOOKING AHEAD: THE BLOCKCHAIN PARADOX-----	182
5.2. IS PbDD A MIRAGE, GIVEN THAT GDPR UNDERVALUES IOT, A TECHNOLOGY THAT SUPPORTS OVER THIRTY BILLION DEVICES? 195	
5.3. ARTIFICIAL INTELLIGENCE AND BIG DATA: QUO VADIS?-----	209
5.4. ASSESSING THE PREPAREDNESS OF PbDD FOR CLOUD COMPUTING-----	218
5.5. CONCLUDING REMARKS -----	225
CHAPTER 6 – SHINING A LIGHT ON THE PbDD'S APPLICABILITY -----	227
6.1. THE PbDD ROLE IN LEGACY DATA CLEAN-UP FOR GDPR COMPLIANCE-----	228
6.2. STORAGE LIMITATION: DATA QUALITY AND SECURITY ARE A PbDD CONCERN-----	242
6.3. PbDD THE FIRST LINE OF DEFENCE TO PREVENT DATA BREACHES -----	256
6.4. CONCLUDING REMARKS -----	261
CHAPTER 7 – EXAMINING ADDITIONAL CHALLENGES ARISING FROM GDPR: DATA SECURITY, AMBIGUITY IN INTERNATIONAL TRANSFERS, AND IMPLEMENTATION COSTS -----	262
7.1. DEVISING A PbDD APPROACH TO DATA SECURITY-----	264
7.2. THE LACK OF CLARITY IN THE GDPR UNDERMINES INTERNATIONAL DATA TRANSFERS-----	269
7.3. HOW DOES THE COST OF IMPLEMENTATION AFFECT PbDD?-----	273
7.4. CONCLUDING REMARKS -----	295
CHAPTER 8 – DPPA (PART I): OPERATIONS AND IMPLEMENTATION OF DATA PROTECTION PRINCIPLES-----	296
8.1. GDPR REQUIREMENTS MUST BE MET VIA OPERATIONAL PbDD ACTIONS -----	302
8.1.1. <i>Transparency behind PbDD operations</i> -----	304

8.1.2. <i>PbDD: operations focused on TOMs</i> -----	305
7.1.2.1. Data confidentiality -----	308
7.1.2.2. Data integrity -----	318
7.1.2.3. Data Availability and Resilience -----	322
7.1.2.4. Data Protection Governance and Compliance-----	325
8.2. IMPLEMENTING THE GDPR PRINCIPLES THROUGH PbDD -----	336
CHAPTER 9 – DPPA (PART II): THE ROADMAP FOR GDPR COMPLIANCE -----	355
9.1. MANAGING DATA SUBJECT RIGHTS THROUGH PbDD -----	355
9.2. IMPLEMENTING PbDD MEASURES TO ADDRESS THE RESPONSIBILITIES OF CONTROLLER AND PROCESSOR -----	384
9.3. IMPLEMENTING PbDD MEASURES ALLOWING FOR TRANSFERS OF DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS -----	412
9.4. IMPLEMENTING PbDD MEASURES IN THE CONTEXT OF THE PROVISIONS RELATING TO SPECIFIC PROCESSING SITUATIONS-----	419
CHAPTER 10 – OVERARCHING CONCLUSIONS -----	423
10.1. ENHANCING DATA SECURITY -----	426
10.2. SAFEGUARDING DATA PROTECTION PRINCIPLES -----	430
10.3. DATA SUBJECT RIGHTS: ENSURING COMPLIANCE AND OPERATIONAL EFFICIENCY-----	435
10.4. THE GDPR ARTICLES RELEVANT TO THE IMPLEMENTATION OF PbDD -----	439
10.5. CONTRIBUTIONS AND FUTURE WORK-----	441
BIBLIOGRAPHY -----	446
ANNEX 1 – ANALYSIS OF GDPR FINES 2018 – 2023 -----	467
ANNEX 1.A - FREQUENCY OF FINES -----	476
ANNEX 2 - CORRELATION TABLE ANALYSIS (EXAMPLE) -----	479
ANNEX 3 – TABLE OF VARIABLES {CNT.X}, {ART.X}, {VIOLATION_X} -----	480
ANNEX 3 - SUPERVISORY AUTHORITIES – LIST OF PUBLIC DATA SOURCES -----	506
ANNEX 4 – URLS TO DECISIONS -----	510

ANNEX 5 – GDPR ARTICLES ADDRESSED IN THE DPPA	548
ANNEX 6 - ETHICS REVIEW APPLICATION FORM	551
SECTION 1: APPLICATION DETAILS	551
SECTION 2: PROJECT DETAILS	553
SECTION 3: PARTICIPANT DETAILS	558
CHECKLIST	564
VERSION CONTROL	564
APPROVAL	565

List of Figures

Figure 1 - PbDD and GDPR lineages.....	19
Figure 2 - An illustration of the GDPR fines imposed by the EU supervisory authorities, based on the type of violation.....	21
Figure 3 - Correlational methodology	73
Figure 4 - Top 5 themes by total number of fines (2018-2023)	78
Figure 5 - Top 5 themes by total sum of fines (2018-2023)	78
Figure 6 - Course of overall number of GDPR fines (cumulative, May 2018-January 2023)	103
Figure 7 - The principle of accountability - Federico Marengo, Data Protection Law in Charts, 2021 (adapted).	152
Figure 8 - Juniper Research. (March 23, 2021). B2B cross-border transactions on blockchain in various regions worldwide in 2020 with forecasts from 2021 to 2025 (in millions) [adapted]. In Statista. < https://www.statista.com/statistics/1228825/b2b-cross-border-transactions-on-blockchain-worldwide/ >.....	186
Figure 9 - PwC. (November 7, 2018). Importance of emerging technologies and confidence in their adoption in organisations worldwide as of 2018 [adapted]. In Statista. < https://www.statista.com/statistics/945047/worldwide-emerging-technology-importance-confidence/ >.....	196
Figure 10 - Ponemon Institute, & Thales Group. (September 30, 2019). Share of organisations that will make significant changes in cloud governance after the introduction of the GDPR as of 2019, by country [adapted]. In Statista, 04 February 2022, < https://www.statista.com/statistics/1063528/worldwide-cloud-governance-changes-due-to-gdpr/ >.....	220
Figure 11 - Varonis. (May 18, 2017). Opinion of IT decision makers on the benefits of the EU General Data Protection Regulations (GDPR) for organisations in the United Kingdom (UK) in 2017	

[adapted]. In Statista. < https://www.statista.com/statistics/796130/gdpr-on-benefits-for-organisations-in-the-uk/ >.	231
Figure 12 - Varonis. (May 18, 2017). Opinion of IT decision makers on the benefits of the EU General Data Protection Regulations (GDPR) for independent citizens in the United Kingdom (UK) in 2017 [adapted]. In Statista. < https://www.statista.com/statistics/796041/gdpr-opinion-on-benefits-for-citizens-in-the-uk/ >.	232
Figure 13 - Example of a business data retention and deletion circular procedure.....	238
Figure 14 - TrustArc. (July 1, 2018). Main challenges in GDPR compliance in Europe and the UK in 2018, by reason [adapted]. In Statista. < https://www.statista.com/statistics/1005011/main-challenges-in-gdpr-compliance-in-europe-and-uk/ >.	263
Figure 15 - Clifford Chance, & Milltown Partners. (November 9, 2021). Priority issues for new technology legislation or Regulation worldwide in 2021 [adapted]. In Statista, < https://www.statista.com/statistics/1279546/new-legislation-priority-issues-worldwide/ >.	266
Figure 16 - Varonis. (May 18, 2017). Opinion of IT decision makers on the drawbacks of the EU General Data Protection Regulations (GDPR) for citizens in the United Kingdom (UK) in 2017 [adapted]. In Statista. < https://www.statista.com/statistics/796083/gdpr-opinion-on-drawbacks-for-citizens-in-the-uk/ >.	274
Figure 17 - EY, & IAPP. (May 25, 2018). Average company's additional spending resulting from GDPR in the European Union and the United States in 2018 (in 1,000 U.S. dollars) [adapted]. In Statista. < https://www.statista.com/statistics/1008320/average-firm-additional-spending-resulting-from-gdpr-in-eu-and-us/ >.	278
Figure 18 - Bitkom. (September 17, 2019). How much effort was required in the following aspects of compliance with the General Data Protection Regulation (GDPR)? [adapted]. In Statista. < https://www.statista.com/statistics/1175341/gdpr-compliance-procedures-germany/ >.	281

Figure 19 - Guardum. (May 1, 2020). What is the average cost for completing a Data Subject Access Request (DSAR)? [adapted]. In Statista. < <https://www.statista.com/statistics/1177135/average-cost-of-a-data-subject-access-request-uk/>>. 283

Figure 20 - European Commission (gdpr.eu). (May 20, 2019). Share of European small businesses spending on compliance with the General Data Protection Regulation (GDPR) in 2019, by budget range [adapted]. In Statista. <<https://www.statista.com/statistics/1176050/gdpr-compliance-spending-in-small-businesses-europe/>>. 285

Figure 21 - Statista. (May 8, 2019). Estimated market value of services for GDPR compliance in Europe in selected years from 2017 to 2023 [adapted]. In Statista. <<https://www.statista.com/statistics/1005111/estimated-value-of-gdpr-services-market-in-europe/>>..... 287

Figure 22 - PwC. (September 13, 2017). Anticipated GDPR related expenditure 2017, by stage of preparedness [adapted]. In Statista. <<https://www.statista.com/statistics/945975/anticipated-gdpr-expenditure/>>. 288

Figure 23 - Sia Partners. (May 1, 2018). Average estimated GDPR costs for FTSE100 companies in the United Kingdom (UK) in 2018, by sector (in million GBP) [adapted]. In Statista. <<https://www.statista.com/statistics/869613/gdpr-implementation-cost-by-sector/>>..... 289

Figure 24 - Thales Group. (November 26, 2018). Intentions of consumers in case of data breach under the General Data Protection Regulation (GDPR) in Germany and in the United Kingdom in 2018 [adapted]. In Statista. <<https://www.statista.com/statistics/1004907/consumers-intentions-in-case-of-data-breach-in-germany-and-uk/>>..... 291

Figure 25 - IBM, & DataEndure. (July 28, 2021). Average cost of a data breach by security automation level in organisations worldwide from 2018 to 2022 [adapted]. In Statista. <<https://www.statista.com/statistics/1176688/data-breach-cost-security-automation-level/>>. 293

Figure 26 - GOV.UK. (March 30, 2022). Average cost of all cyber security breaches for businesses in the United Kingdom (UK) as of 2022 (in GBP) [Graph]. In Statista.

< https://www.statista.com/statistics/586788/average-cost-of-cyber-security-breaches-for-united-kingdom-uk-businesses/ >	294
Figure 27 – Scope of applicability of the DPPA	300
Figure 28 - Technical measures to consider in the PbDD plan.....	306
Figure 29 - Organisational measures to consider in the PbDD plan.	307
Figure 30 - Operational example: implementing a principle through PbDD	338
Figure 31 - Lawfulness of processing, Federico Marengo, Data Protection Law in Charts, 2021 (adapted).....	342
Figure 32 - Consent under GDPR, Federico Marengo, Data Protection Law in Charts, 2021 (adapted).	346
Figure 33 - Conditions applicable to child's consent, Federico Marengo, Data Protection Law in Charts, 2021 (adapted).	349
Figure 34 - Processing special categories of personal data, Federico Marengo, Data Protection Law in Charts, 2021 (adapted).....	351
Figure 35 - Processing of personal data relating to criminal convictions and offences, Federico Marengo, Data Protection Law in Charts, 2021 (adapted).	353
Figure 36 - General transparency obligations of the data controllers, Federico Marengo, Data Protection Law in Charts, 2021 (adapted).	356
Figure 37 - The right to be informed, Federico Marengo, Data Protection Law in Charts, 2021 (adapted).....	359
Figure 38 - The right to access, Federico Marengo, Data Protection Law in Charts, 2021 (adapted).	363
Figure 39 - The right to rectification, Federico Marengo, Data Protection Law in Charts, 2021 (adapted).....	365
Figure 40 - The right to erasure, Federico Marengo, Data Protection Law in Charts, 2021 (adapted).	369

Figure 41 - The right to restriction of processing, Federico Marengo, Data Protection Law in Charts, 2021 (adapted). 371

Figure 42 - The right to data portability, Federico Marengo, Data Protection Law in Charts, 2021 (adapted). 375

Figure 43 - The right to object processing, Federico Marengo, Data Protection Law in Charts, 2021 (adapted). 378

Figure 44 - The right not to be subject to ADM, Federico Marengo, Data Protection Law in Charts, 2021 (adapted). 382

Figure 45 - DPPA framework: approach to PbDD implementation..... 388

List of Tables

Table 1 - Legal Bases for Processing vs. Data Subject's Rights.....	124
Table 2 - Example of a data retention schedule entry.....	238
Table 3 - Example of a data protection risk matrix.....	246

Acknowledgements

I am sincerely grateful for the support and assistance I have received during the completion of this thesis. Firstly, I would like to express my deepest appreciation to the University of Reading for granting me the opportunity to pursue my academic aspirations through the Wilkie Calvert co-supported PhD studentship. This programme has played a vital role in enabling professionals to pursue part-time PhD research, nurturing their career development while concurrently fulfilling strategic objectives for their respective organisations. In this regard, I extend my heartfelt thanks to both Countrywide Plc and the charity Anthony Nolan for their invaluable support.

Additionally, I would like to convey my deep appreciation to my thesis supervisors, Professor Stavroula Karapapa, Dr Mathilde Pavis, and Dr Anne Thies, for their invaluable guidance, insightful criticism, and unwavering support throughout this research. Their astute observations, recommendations, and constructive critiques have played a vital role in shaping my research and producing a rigorous work. I am truly grateful for their contributions.

I would also like to express my heartfelt gratitude to my wife, Elisabete Cervantes, who has been a constant source of encouragement, support, and inspiration. Her unconditional love and unwavering support have been instrumental in helping me navigate the challenges and successes of this academic pursuit. Furthermore, I am thankful to my sons, Miguel Cervantes and Alexandre Cervantes, and my daughter, Mariana Cervantes, for their patience, understanding, and support, which enabled me to dedicate the necessary time and effort to complete this thesis. Their support has significantly eased the burdens of this journey.

This thesis is dedicated to my family: to my mother and to the memory of my father, to my beloved wife, and to my remarkable sons and daughter.

Chapter 1 – Introduction

‘[T]he rights to privacy and to the protection of personal data are fundamental rights enshrined in the Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. They shall not be considered as absolute values, but carefully balanced with other rights at stake. The Court of Justice of the European Union has developed case law on the principles of necessity in a democratic society and proportionality of limitations to fundamental rights and principles, ensuring their appropriate protection.’^{1,2}

Privacy is now widely regarded as one of the most important premises of democratic societies, not only because it is inextricably connected to human dignity and freedom,³ but also because it allows us to choose how and with whom we want to share our thoughts, concerns, and feelings.⁴ Besides protecting information that we want to keep out of the public domain, privacy protects us from those who are more powerful than us or on whom

¹ Andrea Jelinek, ‘EDPB Letter to the European Institutions on the Privacy and Data Protection Aspects of a Possible Digital Euro’ (18 June 2021) <https://edpb.europa.eu/system/files/2021-07/edpb_letter_out_2021_0113-digitaleuro-toconsiliumsi_en.pdf>.

² All websites referenced in this work were last accessed on 27 June 2023.

³ The right to freedom of thought (FoT), for example, receives absolute protection under international human rights law. Article 9 of the ECHR gives us the right to free thought in our inner life, or forum *internum*. In all other cases where thoughts are shown in the forum *externum*, freedom of thought is considered a qualified right. See Patrick O’Callaghan and Bethany Shiner, ‘The Right to Freedom of Thought in the European Convention on Human Rights’ (2021) 8 *European Journal of Comparative Law and Governance* 112. However, some argue that technological advancements of the twenty-first century could pose a significant threat to FoT. For further discussion on this topic, see Simon McCarthy-Jones, ‘The Autonomous Mind: The Right to Freedom of Thought in the Twenty-First Century’ (2019) 2 *Frontiers in Artificial Intelligence* 19.

⁴ Shoba Sreenivasan and Linda Weinberger, ‘The Importance of Privacy—Both Psychological and Legal | Psychology Today’ <<https://www.psychologytoday.com/us/blog/emotional-nourishment/202007/the-importance-privacy-both-psychological-and-legal>>.

we rely. Without privacy, we could be easily controlled and manipulated, and in the worst-case scenario, we could lose control over our own lives.⁵

Data protection emerges in the EU legal framework 'as an offspring of privacy and the two rights still seem inextricably tied up together with a birth cord.'⁶ The General Data Protection Regulation ('GDPR')⁷ is conceptually derived from the legal advancements of these two closely related, but 'distinct' rights:⁸ the right to privacy and the right to data protection. The former has been embedded in international human rights law through the 1948 Universal Declaration of Human Rights (UDHR)⁹ and is referred to as 'the right to respect for private life', and immediately following, in the 1950 European Convention on Human Rights (ECHR).¹⁰ The latter emerged following a period of 'informational privacy' and 'informational self-determination' in the early 1970s as a result of the accelerated advance of electronic data processing,¹¹ particularly, the appearance of mainframe computers and thus the collecting, processing and sharing of large amounts of personal data, and the development of telecommunications, which facilitated the national and international electronic transfer of such data.¹²

⁵ Marcel Becker, 'Privacy in the Digital Age: Comparing and Contrasting Individual versus Social Approaches towards Privacy' (2019) 21 Ethics and Information Technology 307.

⁶ Maria Tzanou, 'Data Protection as a Fundamental Right next to Privacy? "Reconstructing" a Not so New Right' (2013) 3 International Data Privacy Law 88.

⁷ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

⁸ Tzanou (n 6).

⁹ Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR) art 5.

¹⁰ Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No.108 1981.

¹¹ PJA de Hert and S Gutwirth, 'Privacy, Data Protection and Law Enforcement' in E Claes, A Duff and S Gutwirth (eds), *Opacity of the individual and transparency of power* (Intersentia 2006).

¹² Eduardo Ustraran, *European Data Protection, Law and Practice* (Second Edition, IAPP 2019).

The world has seen a truly amazing digital revolution that has led to the development of new computer and technological systems, such as smart devices, the Internet of Things (IoT), facial recognition, biometric identification, and AI-powered personal assistants. These systems have changed our daily lives. However, those digital facilities are very data-hungry,¹³ so there has been a huge rise in the movement of personal data between people and governments and private businesses.¹⁴

The simple act of purchasing a new pair of shoes can trigger several mechanisms designed to collect, transfer, and store a large amount of data, particularly if "plastic" money is used. A substantial amount of data is captured during online purchases, including information such as credit card numbers that are directly communicated with financial organisations, as well as email addresses, postal addresses, names, and ages, among others. Often, an individual also shares "inferred data"¹⁵ such as their preferences about a particular product or brand, which is collected by organisations and later used in marketing analysis, targeting, and profiling. Data privacy and security, as well as data management and cybersecurity, are therefore deemed to be crucial factors for businesses to succeed in

¹³ AI algorithms and models, for example, rely on large amounts of data to learn and make accurate predictions or classifications. This is because AI algorithms learn by identifying patterns and relationships within the data they collect. The more data an AI system has access to, the better it is likely to perform. This is particularly true for machine learning algorithms, which are designed to automatically improve their performance with more data. For example, a speech recognition system needs a large amount of speech data in order to accurately recognise and transcribe spoken words. For a short discussion on this topic, see 'Data-Hungry Algorithms and the Thirst for AI' *ICT Monitor Worldwide* (30 March 2017) <<https://link.gale.com/apps/doc/A488389720/IOTF?u=rdg&sid=summon&xid=b19557a3>>.

¹⁴ Albert Opher, Alex Chou and Andrew Onda, 'The Rise of the Data Economy: Driving Value through Internet of Things Data Monetization' <https://hosteddocs.ittoolbox.com/rise_data_econ.pdf>.

¹⁵ Inferred data is data that has been deduced, derived, or extrapolated from other data rather than being explicitly provided. It is data that is not directly observable or measurable but is instead estimated or assumed based on other available information. Inferred data is often generated through data analysis techniques such as machine learning, where patterns and relationships are identified within existing data, and new data is then inferred based on those patterns. For example, a machine learning algorithm may analyse a dataset of customer purchase histories and infer which products are likely to be purchased together, even if those exact combinations have not been explicitly observed in the data.

today's digital world and global marketplace,¹⁶ where protecting the privacy rights of individuals is strongly emphasised.

Simultaneously, personal data flows are becoming an increasingly important aspect of modern-day economies, affecting the way organisations do business around the world.¹⁷ Unfortunately, privacy-intrusive technologies¹⁸ are also being used more often by both public and private organisations.¹⁹ Since technological advances have changed how personal data is processed and exchanged, new laws have been enacted requiring organisations to further enclose the data they hold, or otherwise process, in order to protect the fundamental rights and freedoms of individuals.²⁰

In the EU, the GDPR is the most comprehensive data protection legislation, giving citizens more control over their data by simplifying and consolidating data protection laws while allowing the free flow of personal data. An increasingly important factor contributing to the acceleration of the economic growth and productivity of EU Member States is the

¹⁶ Rosnata Eugene, 'A Delphi Study: A Model to Help IT Management within Financial Firms Reduce Regulatory Compliance Costs for Data Privacy and Cybersecurity' (DIT, Capella University 2020).

¹⁷ W Gregory Voss, 'Cross-Border Data Flows, The GDPR, And Data Governance' (2020) 29 Pacific Rim law & policy journal 485.

¹⁸ For a discussion of impact of Privacy-intrusive technologies, see Stéphanie Héroult and Bertrand Belvaux, 'Privacy paradox et adoption de technologies intrusives Le cas de la géolocalisation mobile/Privacy paradox and the adoption of intrusive technologies. The case of mobile location-based services' [2014] *Décisions Marketing* 67. See also Ira Zunin, 'Intrusive Technology Means Privacy Rights Are Necessary' *Honolulu Star-Advertiser* (Honolulu, Hawaii, 25 February 2012) <<https://www.proquest.com/newspapers/intrusive-technology-means-privacy-rights-are/docview/923427687/se-2?accountid=13460>>.

¹⁹ See Carissa Véliz, *Privacy Is Power* (Bantam Press 2020). 'It is a world in which your every step, word uttered, search online, purchase, and swipe of your finger on your smartphone is recorded, analysed, and shared with governments and companies.' p.203.

²⁰ See, Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press 2015). 'One of the reasons why the European Parliament initially called for data protection legislation in the mid-1970s was as a reaction to the emergence of a data processing industry in the EU. Forty years later technological changes continue to preoccupy and test lawmakers. In 2012, the European Commission, in its proposal for a new Data Protection Regulation, stated that "rapid technological developments have brought new challenges for the protection of personal data," highlighting in particular the unprecedented scale of data sharing and collection by private companies and public authorities.' pp.3-4.

cross-border flow of data.²¹ For example, one can use the internet to promote and deliver digital goods and services,²² in the same way that physical goods can be ordered for delivery to a buyer regardless of where they are manufactured or acquired. Both are examples of the benefits of the free flow of personal data. In parallel with the GDPR, the Regulation 2018/1808 on the free flow of non-personal data in the EU,²³ which came into force on 28 May 2019, enables the free movement of non-personal data across the EU in order to contribute to the development of the digital economy by easing these flows of data across national borders.

Since one of the problems attributed to the rapid advances in data technology in recent years is concerns about privacy,²⁴ organisations must now implement appropriate technical and organisational measures (TOMs), such as anonymisation and pseudonymisation, and incorporate the principles introduced by the GDPR, including the concept of Privacy by Design ('PbD'), into the design of their technology.

The concept of Privacy by Design (PbD) was developed by Ann Cavoukian, former Information and Privacy Commissioner for the Canadian province of Ontario, in the 1990s,

²¹ EPIC, 'The Value of Cross-Border Data Flows to Europe: Risks and Opportunities' (*DIGITALEUROPE*) <<https://www.digitaleurope.org/resources/the-value-of-cross-border-data-flows-to-europe-risks-and-opportunities/>>.

²² One matter of concern for data protection law is how the European Union approaches the lack of physical boundaries in the online world. See Shakila Bu-Pasha, 'Cross-Border Issues under EU Data Protection Law with Regards to Personal Data Protection' (2017) 26 *Information & communications technology law* 213.

²³ Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Text with EEA relevance.) OJ L 303, 28.11.2018, p. 59–68.

²⁴ An example of ongoing public concerns about privacy can be linked to Facebook, e.g., Facebook proposed to include profile photos of members in its facial recognition database for automated tagging. See 'Facebook Policy Change Rekindles Privacy Fears and It Turns to Voice' [2013] *Biometric technology today* 2. However, faced with pressure from individuals and European data protection authorities, Facebook removed the facial tagging feature and deleted the facial database (Face Recognition System). See Facebook's VP of Artificial Intelligence, Jerome Pesenti statement, 'An Update On Our Use of Face Recognition' (*Meta*, 2 November 2021) <<https://about.fb.com/news/2021/11/update-on-use-of-face-recognition/>>.

to become the ‘framework to proactively embed privacy directly into information technology, business practices, physical design, and networked infrastructures – making it the default.’²⁵ PbD is founded on the following seven foundational principles that guide its implementation:²⁶ 1) Proactive, not Reactive; Preventative not Remedial. This means that PbD focuses on preventing privacy threats before they happen, rather than reacting to them after they occur; 2) Privacy as the Default. PbD ensures that personal data are automatically secured in any IT system or business activity, without requiring any action from individuals to safeguard their privacy; 3) Privacy Embedded into Design. PbD is integrated into the design and architecture of information technology systems and businesses’ activities, rather than added as an afterthought; 4) Full Functionality – Positive-Sum, not Zero-Sum. PbD seeks to accommodate all legitimate interests and purposes in a positive-sum way that avoids unnecessary trade-offs; 5) End-to-End Security – Lifecycle Protection. PbD ensures that data is safely retained and securely erased when no longer necessary, across the full lifecycle of the data involved; 6) Visibility and Transparency. PbD aims to provide reassurance to all stakeholders that it is working in accordance with its stated promises and objectives, subject to independent verification; and 7) Respect for User Privacy. PbD prioritises individual interests by incorporating safeguards such as strong privacy defaults, appropriate notices, and user-friendly options, maintaining a user-centric approach.

²⁵ Ann Cavoukian, ‘Privacy by Design [Leading Edge]’ (2012) 31 IEEE technology & society magazine 18.

²⁶ Ann Cavoukian, ‘Privacy by Design: The Definitive Workshop. A Foreword by Ann Cavoukian, Ph.D.’ (2010) 3 Identity in the Information Society 247.

As a result, the GDPR mandates that businesses process personal data securely by implementing TOMs; this is the concretisation of the 'integrity and confidentiality' principle expressed in Article 5 of GDPR, and henceforth referred to as the 'security principle'.²⁷

The Regulation also adopts a risk-based approach to data protection²⁸ and data security, with the safeguarding of privacy mainly achieved through the implementation of 'Data Protection by Design and by Default' ('PbDD'), which means that in order to achieve a mature level of data security, data controllers need to take into account factors such as risk analysis, organisational policies, and physical and technical measures. A decision on what appropriate measures to take should be based on the state of the art and costs of implementation. It is crucial that such measures are capable to ensure the 'confidentiality, integrity and availability' of the systems and services, as well as the security of the personal data they process.

However, there are practical issues arising pertaining to this approach - where data protection measures are implemented on a technical and organisational level to guarantee the privacy of individuals - that often prevent data controllers from achieving the legislator's data protection aims expressed in the Regulation. The data protected by the GDPR ranges from simple identifiers such as the name and address of an individual, to highly sensitive genetic and health aspects of a natural person. Therefore, for a correct application of TOMs, it is of utmost importance to understand what counts as personal

²⁷ See, Meriem Benyahya and others, 'The Interface of Privacy and Data Security in Automated City Shuttles: The GDPR Analysis' (2022) 12 Applied Sciences. 'The GDPR introduces pseudonymization and anonymization as prominent countermeasures to protect personal data since they lower the risk of linking personal data to their related data subjects. In legal terms, such schemes are forethought differently and independently, while, technically, they offer incommensurable levels of privacy-preserving.'

²⁸ For a discussion of the risk-based approach to data protection, see Raphaël Gellert, *The Risk-Based Approach to Data Protection* (Oxford University Press 2020) <<https://doi.org/10.1093/oso/9780198837718.001.0001>>.

data within the meaning of the Regulation. The definition of personal data, as the main commodity the GDPR seeks to protect, merits thus a thorough analysis and discussion. Although the term “commodity” may not seem appropriate at first glance, it is meant to underscore some people's perspective that ‘personal data is the new oil of the internet and the new currency of the digital world’²⁹ - a statement that unequivocally captures the significance of the PbDD role as guardian of such valuable information.

The relevance of the definition of personal data in the context of PbDD

In recent years there has been an increasing interest in understanding the precise meaning of ‘personal data.’³⁰ And that interest is certainly legitimate, as the presence of personal data in a dataset determines whether or not a processing activity is subject to the GDPR,

²⁹ Meglena Kuneva, ‘European Consumer Commissioner, Keynote Speech; Roundtable on Online Data Collection, Targeting and Profiling’ (Roundtable on Online Data Collection, Targeting and Profiling, Brussels, 31 March 2009) <https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_09_156>.

³⁰ The case law of the ECtHR has demonstrated that personal data can take many different forms. See, e.g., Internet subscriber information associated with specific dynamic IP addresses assigned at certain times (*Benedik v Slovenia*, App no 62357/14 (ECtHR, 24 April 2018). §§ 108-109); Recordings taken for use as voice samples, being of a permanent nature and subject to a process of analysis directly relevant to identifying a person in the context of other personal data, *PG and JH v the United Kingdom*, App no 44787/98, ECHR 2001-IX.; Cellular samples and DNA profiles, *S and Marper v the United Kingdom (2008)* ECHR 1581., paras. 70- 77); or fingerprints, (ibid., para. 84) which, notwithstanding their objective and irrefutable character, contained unique information on the individual concerned and allowed his/her precise identification in a wide range of circumstances (ibid., para. 85); Information on a given individual obtained from banking documents, whether involving sensitive details or professional activity, *M.N. and Others v. San Marino*, 2015, paras. 51 et seq.; Data on the occupation of an identified or identifiable individual collected and stored by the police, *Khelili v Switzerland*, App no 16188/07, (ECtHR, 18 October 2011)., para. 56; Data on Internet and messaging (Yahoo) usage by an employee in the workplace, obtained through surveillance, *Bărbulescu v Romania (2017)* ECHR 742.74-81.; A copy of electronic data seized in a law firm, even though it had not been deciphered, transcribed or officially attributed to their owners, (*Kırdök and Others v Turkey*, App no 14704/12, (ECtHR, 03 December 2019).); Data collected in the context of non-covert video surveillance in a university, *Antović and Mirković v Montenegro*, App no 70838/13 (ECtHR, 28 November 2017).; Information on the taxable income and assets of a large number of individuals, notwithstanding the fact that the public could access such data under certain conditions, *Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland* ECHR 2017/213.; Data on the birth and abandonment of an individual, including information needed to discover the truth about an important aspect of personal identity, *Gaskin v the United Kingdom (1989)* Series A no 160.; *Mikulić v Croatia*, App no 53176/99, (ECtHR, 07 February 2002).; *Odièvre v France [GC]* ECHR 2003-III.; Data included in a divorce settlement, comprising details as to the division of matrimonial assets, the custody and residence of minor children, the alimony agreement and an overview of the assets/income of the applicant, *Liebscher v Austria*, App no 5434/17, (ECtHR, 6 April 2021).

as the Regulation only applies to the activities involving the processing of personal data.³¹ The purpose of the GDPR is to protect the privacy of individuals from the unjustified collection, storage, use and disclosure of their personal information. Consequently, it is common to describe the protection of personal data as creating an environment in which one person is 'more or less inaccessible' to others. Numerous privacy scholars and practitioners have already tried to understand what is meant by 'personal data.'³² In this regard, the Article 29 Data Protection Working Party (WP29)³³ offers useful guidance; firstly, the concept of personal data is broad and encompasses any information that relates to an identified or identifiable individual. This includes data that directly identifies a person, such as their name or address, as well as data that indirectly identifies them, such as an identification number. Secondly, the Working Party emphasises that personal data can be subjective and context dependent. Therefore, the determination of what constitutes personal data may vary based on the circumstances surrounding its use and the data controller's intended purpose. Thirdly, the advisory body highlights the importance of data protection and privacy rights in relation to personal data. Any processing of personal data

³¹ For a current discussion on the definition of personal data, see, e.g., Alison Mary Knight, 'Towards a New Approach to the Legal Definition of Personal Data and a Jurisdictional Model of Data Protection Law: Surpassing the Requirement for an Assessment of Identifiability from Data with an Effects-Based Approach' (PhD, University of Southampton (United Kingdom) 2017) <<https://search.proquest.com/dissertations-theses/towards-new-approach-legal-definition-personal/docview/2430827794/se-2?accountid=13460>>.

'[T]here is confusion about the legal definition of personal data reliant upon the concept of identification capabilities from information, in interpretation and practical application (in determining what data comes within its scope and data protection obligations apply), when confronted with new technological realities.'

³² See e.g., Daniel J Solove, 'A Taxonomy of Privacy' (2006) 154 *University of Pennsylvania law review* 477. See also, Mireille Hildebrandt, 'Defining Profiling: A New Type of Knowledge?' in Mireille Hildebrandt and Serge Gutwirth (eds), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer Netherlands 2008) <https://doi.org/10.1007/978-1-4020-6914-7_2>.

³³ The Article 29 Working Party (WP29) was an advisory body made up of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor and the European Commission. The composition and purpose of WP29 was set out in Article 29 of the Data Protection Directive (Directive 95/46/EC). It was replaced by the European Data Protection Board (EDPB) on 25 May 2018 in accordance with the EU General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).

must adhere to strict data protection Regulations to ensure individuals' rights are effectively protected. Finally, the Opinion underscores the importance of taking a comprehensive approach to the handling of personal data, including addressing issues such as data security, data accuracy, and transparency in data processing:

‘The Working Party’s analysis has been based on the four main “building blocks” that can be distinguished in the definition of “personal data”: i.e. “any information”, “relating to”, “an identified or identifiable”, “natural person”. These elements are closely intertwined and feed on each other, but together determine whether a piece of information should be considered as “personal data.”³⁴

The Opinion emphasises that the definition of personal data is not always straightforward and can be influenced by the context in which it is used, as well as the intentions of the data controller.³⁵ This assertion opens up a significant degree of ambiguity, creating an opportunity for diverse interpretations and resulting in areas that necessitate additional clarification. The ensuing discussion aims to examine these grey areas in order to achieve a more comprehensive understanding of the application of GDPR.

In a landmark decision in *Lindqvist*,³⁶ the CJEU provided some clarity on which elements of data should be considered as personal data under the Data Protection

³⁴ Article 29 Data Protection Working Party, ‘Opinion 04/2007 on the Concept of Personal Data, (WP136, 20 June 2007).’ 200.

³⁵ The recognition that the definition of personal data is nuanced and can be influenced by context aligns with the principles of PbDD. For example, the emphasis on context in determining whether data falls under the definition of personal data resonates with the PbDD approach, as it underscores the need to consider the specific circumstances and purposes for which data is collected and processed.

³⁶ *Case C-101/01, Bodil Lindqvist v Åklagarkammaren i Jönköping* EU:C:2003:596, [2003] ECR I-12971 01.

Directive (DPD).³⁷ By emphasising that removing only an individual's name from a website was not sufficient since individuals could be identified using their home addresses, telephone numbers, and other information displayed on the website, the Court clarifies that any information that can be used to identify an individual should be considered personal data. Other cases considered the definition of personal data within the context of the DPD. In the *Bavarian Lager*³⁸ case, the Commission brought an appeal seeking annulment of the General Court decision which invalidated a decision by the Commission denying the applicant access to full minutes of a meeting along with the names of those present. The CJEU ruled that, surnames and forenames should be considered personal data and the list of participants in a meeting was considered personal information, since it could be used to identify individuals. Moreover, in the *Scarlet*³⁹ case, a reference for a preliminary ruling by the Cour d'appel de Bruxelles, where a music management company brought proceedings against an Internet service provider (ISP), to take measures in order to bring an end to the copyright violations committed by the ISP's customers, the Court took the view that Internet Protocol (IP) addresses⁴⁰ should be considered personal data. Scarlet was ordered by the Court of first instance to install "peer-to-peer" filtering software in their systems to prevent the sharing of content infringing copyright. The CJEU, at para.

³⁷ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23/11/1995 P. 0031 - 0050 1995 31

³⁸ *Case C-28/08 P Commission v Bavarian Lager EU:C:2010:378, [2010] ECR I-6005 08.*

³⁹ *Case C-70/10 Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) EU:C:2011:771.*

⁴⁰ For insights into the topic of IP addresses, see, e.g., Internet Society, 'A Short Guide to IP Addressing - How Are IP Addresses Managed and Distributed?' (11 September 2015) <<https://www.internetsociety.org/resources/deploy360/2015/short-guide-ip-addressing/>>.

51 of the decision, stated that IP addresses are protected personal data because they allow the concerned users to be precisely identified.⁴¹

The GDPR builds upon the definition of personal data as set out by the DPD, in response to the rapid advancements in digital technology and to account for novel methods through which personal information is collected, processed, and stored by organisations. The GDPR prohibits several processing activities that require the utilisation of personal data, including profiling, analytical scrutiny of web browsing activities, and historical analysis of online transactions, among other data analysis and data aggregation practices that rely on personal data, unless the data subject has granted explicit authorisation. Compared to the DPD, the GDPR (in order to make the processing of personal data more transparent and empower data subjects), makes the legal definition of personal data⁴² more intricate and complex, and consequently more difficult to implement into the information systems and processes of organisations, including through PbDD mechanisms.

Data controllers must possess a comprehensive understanding of the definition of personal data to fulfil their obligations under Articles 12 to 23 of the GDPR. Specifically, compliance with the right to access and the right to erasure, or "the right to be forgotten," necessitates the implementation of appropriate systems and procedures to identify and locate personal data within an organisation's data ecosystems, in addition to systems and procedures that enable the disclosure of the findings to the data subject. If the system is

⁴¹ The ECtHR has established that any element that indirectly discloses the identity of an individual, including a dynamic IP address, constitute personal data. See, *Benedik v. Slovenia (2018)* (n 30).

⁴² The GDPR defines in its Article 4(1) personal data as 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.'

automated, it must facilitate identification of pertinent personal data elements from local structured, unstructured, and cloud-based datasets, relevant to the specific request. Any failure to meet these requirements may result in severe consequences, such as data breaches, fines, and reputational damage.

The risks to personal data that are addressed through the implementation of PbDD

Implementing PbDD to protect personal data in organisations is a difficult, complex, and challenging endeavour. To illustrate, data controllers are required to establish and adopt appropriate TOMs ('appropriate measures') for detecting, investigating, and internally reporting personal data breaches. In addition, the data controller must maintain a comprehensive record of all personal data breaches, regardless of whether or not they were reported to the supervisory authority. Consequently, organisations must ensure that their information system policies and cybersecurity planning meet GDPR requirements, as non-compliance with the Regulation can result in severe financial penalties and a detrimental impact on their reputation. Moreover, those accountable for personal data processing in an organisation must possess a comprehensive understanding of the existing security requirements and Regulations and must be well-versed in the mechanisms employed to prevent personal data compromise. This includes the implementation of appropriate measures to minimise the likelihood of security breaches, data loss, and cyber-attacks. Additionally, controllers must be capable of effectively communicating with data subjects and supervisory authorities, promptly notifying them of any personal data breaches that occur.

My research delves into the implications of data breaches within the scope of the GDPR, examining both conceptual and practical implications. To achieve this, the study

refers to the tenets of PbDD and assesses the practical feasibility of incorporating appropriate TOMs, as mandated by Articles 24, 25 and 32 of the GDPR, into the contemporary systems, processes, and operations of organisations. As the legal and technological research community still grapples with uncertainty surrounding this subject,⁴³ I will address the difficulties in implementing security protection measures and consider different approaches to incorporating them into the lifecycle of an organisation's data processing systems and processing activities. My argument is reinforced by a comprehensive examination of privacy design strategies. These strategies facilitate the systemic integration of the data security principle within the scope of data controllers' processing activities. In accordance with Article 28 of the GDPR, extends to data processors and any sub-processors involved in the processing activities.⁴⁴ Simultaneously, I outline the broader policy context surrounding PbDD, illustrate the limitations of PbDD, and offer recommendations for business stakeholders, data protection practitioners, system developers, supervisory authorities, and policymakers.

By laying the groundwork for a better understanding of the current state of the art in the context of PbDD, this work can also serve as a repository and guide for controllers attempting to incorporate data protection principles and mechanisms to respond to individuals' privacy rights into their systems and processes. Furthermore, this thesis can be regarded as a useful tool for data protection officers (DPOs) and data privacy managers (DPMs), as they can use it in the context of their duties and responsibilities of monitoring the application of the data protection law and providing guidance to their businesses, and

⁴³ See, e.g., Kathrin Bednar, Sarah Spiekermann and Marc Langheinrich, 'Engineering Privacy by Design: Are Engineers Ready to Live up to the Challenge?' (2019) 35 *The Information society* 122.

⁴⁴ It is noteworthy to acknowledge that the term "controllers," as used in this work, encompasses all entities accountable for safeguarding personal data, including processors and sub-processors.

also as groundwork for their task of implementing PbDD. My thesis is also intended to help regulators and legislators to better understand the opportunities, challenges, and limitations of PbDD so that they can better formulate and implement policy in the future - *de lege ferenda*.

It is my contention that a fundamental aspect of this study sits in its proposition of practical and feasible solutions that facilitate the incorporation of PbDD by legal and technological actors in a manner that effectively mitigates, or in certain cases eradicates, the risks arising from the processing of personal data. This includes the risk of infringing upon data subjects' rights and freedoms, as well as the potential for regulatory penalties and reputational harm.⁴⁵

With the departure of the United Kingdom (UK) from the EU on 31 January 2020, the GDPR remained in force in the UK until the end of the transition period ending on 31 December 2020, after which it became a "third country." Thereafter, the GDPR was retained⁴⁶ in UK domestic law as the "UK GDPR",⁴⁷ sitting alongside an amended version of the Data Protection Act 2018 (DPA 2018).⁴⁸ As the key principles, rights and obligations remain the same⁴⁹ and the UK benefits now from a EC "Adequacy Decision," for the

⁴⁵ For a discussion of the risk to reputation in the context of GDPR, see, Jeffrey Batt, 'Reputational Risk and the GDPR: What's at Stake and How To Handle It' (*Economy*, 23 May 2018) <<https://www.brinknews.com/reputational-risk-and-the-gdpr-whats-at-stake-and-how-to-handle-it/>>.

'Reputational damage will be a core consequence of any GDPR-related fine or penalty, similar to the aftermath of a privacy or cyber-related security incident.'

⁴⁶ Retained EU law is defined in s 6(7) of the European Union (Withdrawal) Act 2018 as 'anything which, on or after [31 December 2020], continues to be, or forms part of, domestic law by virtue of section 2, 3, 4 or 6(3) & 6(6) of the European Union (Withdrawal) Act 2018 (as that body of law is added to or otherwise modified by or under this Act or by other domestic law from time to time).'

⁴⁷ The UK GDPR is the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (EU GDPR) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (SI 2019/419).

⁴⁸ Data Protection Act 2018 c.12.

⁴⁹ It includes the provisions that were previously in effect (EU GDPR), unless the context otherwise requires.

purposes of this work, the UK GDPR is considered equivalent to the EU GDPR in terms of its implementation approach, particularly with regard to PbDD implementation. Several notes and guidance produced by the UK supervisory authority, the Information Commissioner's Office (ICO), are presented throughout the thesis, which are deemed relevant to this study.

1.1. Context and scope of the study

As a result of the incorporation into the GDPR, specifically in its Article 25, which refers to the principle of "Data Protection by Design and by Default," which mandates that appropriate measures should be incorporated into the design of systems, processes, and technologies from the outset, PbD has been elevated from a theoretical concept to a legal obligation,⁵⁰ which translates into the implementation of organisational and technological measures to protect personal data into businesses' systems and data processing activities.

Essentially, this operationalisation of data protection law means that, at the time of determining the means for processing (design stage, including systems design) and at the time of the processing itself, organisations must implement appropriate measures to ensure that, by default: (i) only the necessary personal data for each specific purpose of the processing are processed,⁵¹ (ii) personal data is made available to an indefinite number of natural persons only through the intervention of the individual,⁵² and (iii) the security of

⁵⁰ In its guidance notes on data protection by design and by default, the ICO states that '[T]his concept is not new. Previously known as 'privacy by design', it has always been part of data protection law. The key change with the GDPR is that it is now a legal requirement.' ICO, 'Accountability and Governance' (*Guide to the General Data Protection Regulation (GDPR)*) <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/>>.

⁵¹ GDPR, Article 25(2).

⁵² *ibid.*

the processing.⁵³ Specifically, this obligation concerns: (a) the volume of personal data that are collected, (b) the extent to which they are processed, and (c) their storage and accessibility.⁵⁴

The operationalisation of GDPR calls thus for organisations to consider ‘data protection’ and ‘privacy’ at the design stage and throughout the lifecycle of new products, processes, systems, or services involving the processing of personal data. It is mandatory that organisations implement mechanisms to properly inform individuals about the processing, before the processing begins, and to only process the data that is necessary for the purpose for which it was originally collected. As part of this process, the default settings should always be the most secure and privacy-friendly options available.

The UK regulator, Information Commissioner’s Office (ICO), offers the following non-exhaustive checklist to help organisations comply with the principles of PbDD:⁵⁵ Organisations must design and implement systems, services, products, and business practices with data protection in mind from the outset. In the pursuit of PbDD, organisations must anticipate risks and potential privacy-invasive events proactively. By doing so, they can take preventive measures to safeguard individuals and prevent any harm before it occurs. An essential principle of PbDD is the limited processing of personal data to only what is necessary for the intended purpose(s). Organisations should ensure that the data is used solely for those specific purposes, promoting privacy by minimising unnecessary data processing.

⁵³ *ibid.* Article 32.

⁵⁴ *ibid.* Article 25(2).

⁵⁵ ICO, ‘Data Protection by Design and Default’ (*Accountability and Governance*, n.d.) <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/>>.

Furthermore, organisations must ensure that personal data is automatically protected within all IT systems, services, products, and business practices. This approach removes the burden from individuals, ensuring that they do not have to take any specific actions to protect their privacy. Transparency is key to PbDD, and organisations should provide clear and accessible identity and contact information of those responsible for data protection. This information should be made available both within the organisation and to individuals, facilitating communication and accountability. In addition, organisations should adopt a 'plain language' policy for public documents, making it easier for individuals to understand how their personal data is being handled. Empowering individuals is crucial, and organisations should provide tools that allow individuals to determine how their personal data is being used. They should also ensure that their policies are effectively enforced, allowing individuals to verify the compliance and integrity of data processing practices.

Respecting user preferences is a fundamental aspect of PbDD. Organisations should offer strong privacy defaults, user-friendly options, controls, and mechanisms that align with individual privacy preferences. When engaging data processors, organisations must select those that provide sufficient guarantees of TOMs for data protection by design. This ensures that all parties involved in data processing adhere to privacy-centric principles. Moreover, when utilising other systems, services, or products in their processing activities, organisations must choose those that consider data protection issues. Collaboration with designers and manufacturers who prioritise privacy reinforces the commitment to PbDD. Lastly, the use of privacy-enhancing technologies (PETs) can significantly assist organisations in complying with their data protection by design obligations. By leveraging

PETs, organisations can enhance privacy safeguards and promote responsible data handling practices.⁵⁶

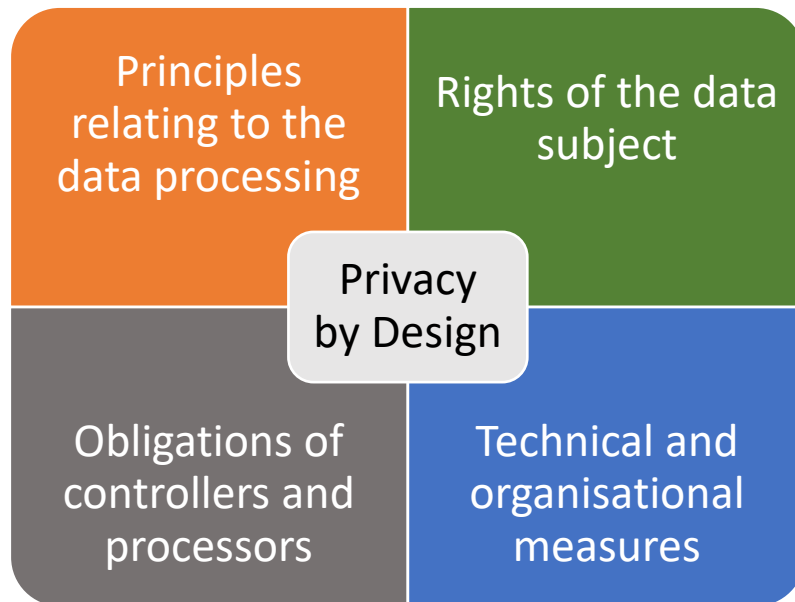


Figure 1 - PbDD and GDPR lineages

A careful reading of the ICO list confirms the significance that the GDPR places on PbDD and underscores its broad scope, ranging from information requirements to the protection of IT systems and corporate policies. In addition, PbDD provides basic insurance mechanisms for the application of the risk-based approach outlined in the GDPR.⁵⁷ Specifically, it does this by designing the conduct of specific data protection assessments,

⁵⁶ This guidance was created by the UK Supervisory authority, the Information Commissioner’s Office (ICO), as general guidance provided to organisations in relation to the EU GDPR. Following Brexit, the GDPR was retained in domestic law as the UK GDPR, sitting alongside an amended version of the Data Protection Act 2018. This means that the key principles rights and obligations, including data protection by design and by default, remain the same.

⁵⁷ For many, this risk-based approach to GDPR is crucial for achieving compliance. See Gellert (n 28). See also, ‘GDPR One Year Anniversary: A Risk-Based Approach to GDPR Is Key for Achieving Compliance’ *ENP Newswire* (15 July 2019) <<https://link.gale.com/apps/doc/A593354902/ITOF?u=rdg&sid=summon&xid=877ee309>>.

known as Data Protection Impact Assessments, or "DPIAs." DPIAs make it possible for organisations to anticipate data protection risks before they occur and inform their decisions regarding the TOMs that need to be implemented. Therefore, data protection needs to be built into the technology as part of a user-centric approach to meet the legislator's expectations for data protection and privacy.

Article 25 and Recital 78 of the GDPR offer practical examples of how PbDD can be implemented. These examples include data minimisation, anonymisation and pseudonymisation, encryption, and conduction of DPIAs. Despite these examples, previous research⁵⁸ and empirical evidence, including the analysis of fines levied by supervisory authorities,⁵⁹ demonstrate that organisations have yet to attain an adequate level of data protection maturity that ensures a more secure data environment and fewer privacy concerns.

Since the implementation of GDPR on May 25, 2018, fines have been imposed for a variety of violations.⁶⁰ In many cases, organisations have incurred fines for their failure to implement appropriate measures to ensure information security, thus resulting in a failure

⁵⁸ See e.g., 'Experian Data Breach Resolution and Ponemon Institute Find Organisations Are Not Ready for Global Security Risks and Regulations: Only 9 Percent of Companies Are Prepared for the Global Data Protection Regulation (GDPR) Half Don't Know Where to Begin' *PR Newswire* (New York, 27 June 2017) <<https://www.proquest.com/wire-feeds/experian-data-breach-resolution-ponemon-institute/docview/1913638074/se-2?accountid=13460>>. 'The study found that more than half (51 percent) of companies surveyed had experienced a global data breach, with nearly 56 percent experiencing more than one breach in the past five years. Yet, despite these major security intrusions, 32 percent of respondents noted that their respective companies still don't have a response plan in place.'; 'Companies aren't adequately prepared to respond to a global data breach.'

⁵⁹ Please see Annex 1 for a visualisation of GDPR fine statistics utilised in this work.

⁶⁰ See Jukka Ruohonen and Kalle Hjerpe, 'The GDPR Enforcement Fines at Glance' (2022) 106 *Information Systems* 101876.

to implement PbDD.⁶¹ This type of violation has resulted in fines totalling over €375,780,219.00.⁶²

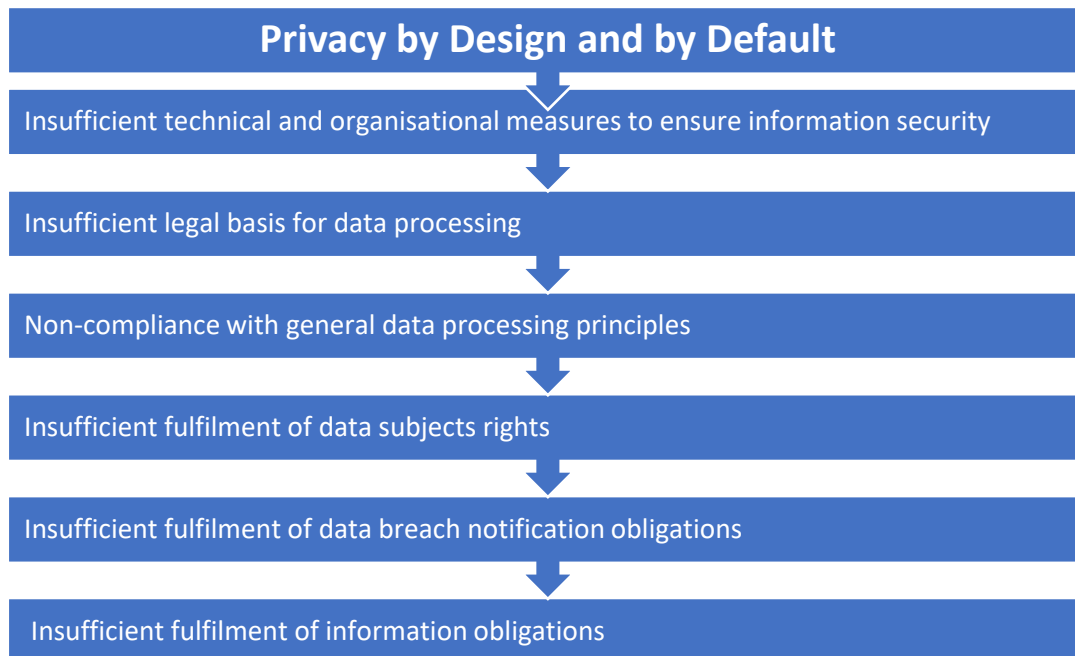


Figure 2 - An illustration of the GDPR fines imposed by the EU supervisory authorities, based on the type of violation.

Additionally, as I shall note, numerous academics and privacy practitioners have pointed out the existence of limitations, both inside and outside the GDPR, that make compliance with the Regulation difficult, or in some cases impossible.⁶³

⁶¹ The predominant portion of fines was allocated to processing activities lacking a sufficient legal basis. The subsequent most prevalent grounds for imposing fines encompassed data processing activities that failed to adhere to general data processing principles. Following closely were fines imposed for inadequate implementation of technical and organisational measures aimed at ensuring information security, insufficient fulfilment of information obligations, and inadequate fulfilment of data subject rights. It is worth noting that only a limited number of fines have thus far been levied for non-cooperation with Supervisory authorities, violations of obligations related to data breaches, inadequate involvement of a data protection officer, or the absence of data processing agreements. For an up-to-date breakdown of fines issues by EU Supervisory authorities, See CMS enforcement tracker, <<https://www.enforcementtracker.com/>>.

⁶² As of January 2023. See Annex 1 for a visualisation of GDPR fines.

⁶³ See e.g., Jimmie Franklin, 'In-House Counsel: 100% Compliance with GDPR Almost Impossible' [2020] *International Financial Law Review* <<https://www.proquest.com/trade-journals/house-counsel-100-compliance-with-gdpr-almost/docview/2373953912/se-2?accountid=13460>>. 'Don't trust anyone who says

Therefore, the ensuing sections aim to scrutinise various organisational practices and external factors that could hinder the effective application of the GDPR's requirements, particularly those pertaining to PbDD, and ultimately culminating in a personal data breach. For instance, organisations frequently encounter difficulties in establishing suitable systems and processes for managing the enormous volumes of data collected, tracking it from inception to disposal, and efficiently storing it based on certain criteria in between.⁶⁴

I would like to emphasise that the European Court of Human Rights (ECtHR) has already used sibling principles of PbDD. For instance, in *Case of I v Finland*,⁶⁵ (2008), the Court conclusions pointed to a violation of Finland's positive obligations under Article 8 ECHR, as a result of the lack of TOMs to protect patient privacy. According to the ECtHR, in order to comply with Article 8 ECHR, Finland would have to provide more than mere data protection *de jure*: '[T]he data controller had to make sure that data were protected *de facto*'.⁶⁶ In addition, while not directly addressing PbDD in the context of Article 25 GDPR, the CJEU has emphasised the importance of adequate TOMs to enable organisations to ensure data privacy and protection in the same way as the ECtHR has done.⁶⁷ A good example of this reasoning can be found in the *Scarlet*⁶⁸ case, when the Court rejected

that they are 100% compliant,' said the data protection counsel for a global corporation. 'The business will take a risk-based approach. If we were unfortunate enough to have a security breach, we would want to ensure that decisions has [sic] been made at the right level and had been well-documented – but absolute compliance isn't feasible.'

⁶⁴ Based on the results of EY's Data Analytics Survey in 2018, it was revealed that a considerable proportion of businesses were unprepared for GDPR compliance following the regulation's effective date on May 25th, 2018. See 'Third Biennial Ernst & Young 2018 Global Forensic Data Analytics Survey' (*GDPR compliance — from planning to action*, 2018) <https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/assurance/assurance-pdfs/ey-forensics-gdpr-compliance-from-planning-to-action.pdf>.

⁶⁵ *I v Finland*, App no 20511/03, (ECtHR, 17 July 2008).

⁶⁶ *Ibid.*, para. 47.

⁶⁷ Lee A Bygrave, 'Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements' (2017) 1 Oslo Law Review 105.

⁶⁸ *Scarlet* [2011] (n 39).

proposals to introduce privacy-invading technologies, such as deep packet inspection algorithms, to counter digital piracy, and in the case of *Google Spain*,⁶⁹ when the CJEU ordered Google to redesign the systems and algorithms in their web search operations in a way that would be more privacy-friendly.

It is important to note that, in the context of Cavoukian's PbD, information systems managers were identified as the operational force responsible for converting the legal framework and associated concepts into functional privacy tools,⁷⁰ capable of ensuring both data security as well as operational efficiency.⁷¹ PbD, as a stand-alone concept, was thus developed as a way of thinking about systems engineering,⁷² and as demand for the consideration of privacy throughout each and every step of the engineering process, directed towards systems engineers rather than towards lawyers.⁷³

Article 25 GDPR outlines the obligations concerning data protection by design and by default, and reads as follows:

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall,

⁶⁹ *Case C-131/12 Google Spain SL, Google Inc v Agencia Española de Protección de Datos, Mario Costeja González EU:C:2014:317* 12.

⁷⁰ Ann Cavoukian, 'Understanding How to Implement Privacy by Design, One Step at a Time' (2020) 9 IEEE consumer electronics magazine 78.

⁷¹ *ibid.*

⁷² See Bednar, Spiekermann and Langheinrich (n 43). (*Privacy by Design* 'requires the guts and ingenuity of engineers') (emphasis added). See also Sarah Spiekermann, 'The Challenges of Privacy by Design' (2012) 55 Communications of The ACM - CACM 38. ('[A]s it is the systems engineers (i.e., software architects, information architects, interaction designers, product designers, and related specialities) who have to find a competent and creative way to realize privacy protection implementations.').

⁷³ *Ibid.* 'Taken together, our theoretical and empirical insights suggest that *there may be an underlying conflict between the legal world and the engineering world*, with lawyers imputing responsibility on engineers that the engineers do not want to embrace.' (emphasis added).

both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate TOMs, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

2. The controller shall implement appropriate TOMs for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.
3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.⁷⁴

Since the concept of "data protection by design and by default" partly parallels the concept better known as "privacy by design" the two terms are often used interchangeably (the concept of "privacy by design" has been kept and given a home in the GDPR, which does not use the term "privacy by design," but rather "data protection by design and by default."),⁷⁵ for the sake of clarity, I shall henceforth refer to PbDD when addressing "data

⁷⁴ GDPR, Article 25.

⁷⁵ Matjaž Drev and Boštjan Delak, 'Conceptual Model of Privacy by Design' (2022) 62 The Journal of Computer Information Systems 888.

protection by design and by default" in the context of GDPR, and to PbD when discussing Cavoukian's "privacy by design" concept.

1.2. Description of the research problem and research question

'In *The Morality of Law*, Lon Fuller tells a tale of a young ruler who undertakes to reform the law of the land. After a few attempts at it, all met by public discontent, the ruler wants to teach his subjects a lesson and makes it a crime 'to cough, sneeze, hiccough, faint or fall down in the presence of the king ... [and] not to understand, believe in, and correctly profess the doctrine of evolutionary, democratic redemption. Unsurprisingly, the citizens threaten to disregard the new law, since '[t]o command what cannot be done is not to make law; it is to unmake law, for a command that cannot be obeyed serves no end but confusion, fear and chaos.'⁷⁶

An important legal principle of EU law is legal certainty, 'based on the fundamental premise in which those subject to the law must be able to ascertain what the law is so as to be able to plan their actions accordingly.'⁷⁷ However, many scholars from the legal, technological and business management fields have already stated that, due to the lack of clarity and certainty in the Regulation, it is becoming increasingly difficult for organisations to

⁷⁶ Nadezhda Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10 *Law, Innovation and Technology* 40.

⁷⁷ Tatiana Eleni Synodinou, 'Lawfulness for Users in European Copyright Law: Acquis and Perspectives' (2019) 10 *JIPITEC* 20.

understand how the GDPR requirements can be put in practice, in particular those related to Data Protection “by design” and “by default” (PbDD).⁷⁸

It is thus clear from previous research that bridging and incorporating legal requirements into information systems and modern business processes through the implementation of PbDD might be an extremely difficult or impossible undertaking, namely, because Article 25 GDPR, which refers to the principle of PbDD, suffers from ‘multiple flaws, in particular, a lack of clarity over the parameters and methodologies for achieving its goals, and a failure to communicate clearly and directly with those engaged in the engineering of information systems.’⁷⁹ This lack of clarity and certainty in the GDPR makes it challenging for organisations to understand how PbDD can be put in practice. I argue that this discrepancy is at odds with the position adopted by the CJEU, which asserts that ‘[T]he principles of legitimate expectation and assurance of legal certainty are part of the legal order of the Community’.⁸⁰ The CJEU highlights the correlation between legal certainty and legitimate expectation; if the law is certain, citizens (and data controllers) know what to expect.

Furthermore, the GDPR underscores the fact that PbDD is closely intertwined with abstract considerations, including but not limited to the “state of the art,” “cost of implementation,” “nature, scope, context, and purpose of processing,” and “risks of varying likelihood and severity for the rights and freedoms of natural persons posed by the

⁷⁸ For a discussion of the challenges posed to the practical implementation of GDPR, see Jeroen van Rest and others, ‘Designing Privacy-by-Design’ in Bart Preneel and Demosthenes Ikononou (eds), *Privacy Technologies and Policy* (Springer Berlin Heidelberg 2014). See also, Bednar, Spiekermann and Langheinrich (n 43).

⁷⁹ Bygrave (n 67).

⁸⁰ *Joined Cases 205-215/82 Deutsche Milchkontor GmbH and others v Federal Republic of Germany* EU:C:1983:233, [1993] ECR 1983-02633.

processing.” These factors form the basis of a "balancing exercise" that must be undertaken before implementing TOMs.⁸¹

The extent of GDPR compliance is contingent on the thorough evaluation and mitigation of risks of varying likelihood. However, this approach may not always be compatible with PbDD, which necessitates a certain degree of “tangibility” from a practical and operational standpoint. Given the technological features that the law aims to regulate, specifically the situations that lead to the control of personal data,⁸² PbDD becomes a functional concept rather than a merely formal one.⁸³ Consequently, PbDD requires a tangible framework that can be implemented in a practical sense, rather than solely relying on theoretical considerations. Moreover, many technical practicalities involving the electronic processing of personal data⁸⁴ not always appear to be compatible with the PbDD measures prescribed by the Regulation, such is the case of management of organisations’ legacy data in a way that ensures compliance with the storage limitation requirements⁸⁵ imposed by the GDPR.⁸⁶ For example, unless a great deal of human effort and money is

⁸¹ GDPR, Article 25(1).

⁸² Tzanou (n 6). “[D]ata protection seems to fall into the aspect of privacy that is known as control over personal information.”

⁸³ A similar approach is adopted by the AG Mengozzi in its Opinion delivered on 1 February 2018 on *Case C-25/17, Jehovan todistajat (AG Opinion) (2018) ECLI:EU:C:2018:57* 14. para. 68. ‘[I]t is necessary to rely upon a more factual than formal analysis in order to assess whether the religious community plays an effective role in determining the objectives and practical means of processing.’

⁸⁴ To gain insight into some of these practical considerations in the context of software development, see M. Colesky, J. Hoepman, and C. Hillen, ‘A Critical Analysis of Privacy Design Strategies’, *2016 IEEE Security and Privacy Workshops (SPW)* (2016).

⁸⁵ In contrast, Article 9(2) of Convention 108 permits derogations from the data protection requirements, subject to the condition that such derogations are enshrined in law, maintain the essence of fundamental rights and freedoms, and are necessary and proportionate in pursuit of legitimate objectives, such as national security, data protection, and criminal prosecution. It is pertinent to note that this exception is not present in the GDPR.

⁸⁶ For instance, Article 5(1)(e) of the GDPR stipulates that data must not be retained for any longer than necessary. However, the regulation does not provide a specific timeframe for data retention, potentially leading to ambiguity in one crucial aspect of business operations: How long can an organisation legitimately retain personal data for?

applied,⁸⁷ the existence of pre-GDPR data silos poses a barrier on the feasibility of implementation of the PbDD principles into businesses' operations: the stash of substantial volumes of business legacy data, sometimes inseparable from large structured⁸⁸ and unstructured⁸⁹ data sets, and frequently widespread across an organisation's data ecosystems, becomes a major factor for non-compliance. Although many of those data sets were lawfully and fairly collected and processed under the DPD,⁹⁰ the GDPR makes its further processing unfair⁹¹ under the new data subject's consent for processing requirements.⁹²

Since the DPD, the requirement of maintaining an appropriate schedule of data retention and deletion has been an enormous challenge for organisations. For example, in *Rijkeboer (2009)*,⁹³ a citizen of the Netherlands submitted a request to the local administration for information regarding the recipients of their personal data in the preceding two years. The administration accepted the request but constrained the

⁸⁷ See e.g., an economic impact analysis of GDPR on a specific sector (IoT), considering aspects such as legal costs, preventative costs, reputational effect (before and after GDPR), demonstrates that the impact of GDPR have heightened the tension and concerns of companies. Junwoo Seo and others, 'An Analysis of Economic Impact on IoT Industry under GDPR' (2018) 2018 Mobile Information Systems 6792028.

⁸⁸ Structured data pertains to data that is typically associated with relational databases, such as flight reservation systems, inventory control systems, customer relationship management databases, sales transaction records, and automated teller machines (ATMs), among others. See e.g., 'Understanding Structured Data: A Comprehensive Guide 101' (28 June 2021) <<https://hevodata.com/learn/understanding-structured-data/>>.

⁸⁹ Unstructured data refers to data that lacks a specific format or structure and is often comprised of files such as text files, photos, video files, audio files, and spreadsheets. See, Bernard Marr, 'What Is Unstructured Data And Why Is It So Important To Businesses? An Easy Explanation For Anyone' (*Forbes*) <<https://www.forbes.com/sites/bernardmarr/2019/10/16/what-is-unstructured-data-and-why-is-it-so-important-to-businesses-an-easy-explanation-for-anyone/>>.

⁹⁰ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23/11/1995 P. 0031 - 0050 1995 31.

⁹¹ The concept of unfair processing refers to the way in which personal data are obtained or processed through deception or concealment of the data subject as defined in *KH and Others v Slovakia, App no 32881/04, (ECtHR, 28 April 2009)*.

⁹² Olly Jackson, 'GDPR: Companies at Risk over Unstructured Data' [2018] International financial law review.

⁹³ *Case C-553/07 College van burgemeester en wethouders van Rotterdam v MEE Rijkeboer EU:C:2009:293*.

timeframe to one year, explaining that personal data older than one year would be automatically erased from their systems. The Court of Justice declared that a balance between the accuracy principle and the principle of storage limitation must be established. The right to privacy implies that the data subject has the assurance that their personal data is being lawfully and accurately processed, specifically that the basic data pertaining to him are accurate and disclosed to authorised recipients; 'In the present case, limiting storage of information on recipients and content to one year, while the basic data is stored much longer, does not constitute a fair balance, unless it can be shown that longer storage would constitute an excessive burden.'⁹⁴

The interplay between storage limitation and individual rights requires a thorough examination through the lens of PbDD, specifically to achieve a balance between the need for business data retention and the protection of individuals' rights and control over their personal information. This work aims to undertake such an examination. This demands the identification and implementation of specific measures to ensure that appropriate mechanisms are integrated into processing operations for embedding relevant data retention schedules. Neglecting to implement such measures would inevitably result in detrimental consequences for data subjects' fundamental rights and freedoms. This was particularly the case in *S. and Marper (2008)*,⁹⁵ where the ECtHR had already taken a similar approach when the indefinite retention of genetic and biometric data (fingerprints, cell

⁹⁴ *ibid.*, paras. 51-57, 64-66

⁹⁵ *S and Marper v the United Kingdom (2008) ECHR 1581* (n 30).

samples, DNA profiles) of individuals after the criminal proceedings had been terminated was deemed unlawful.⁹⁶

Owing to the inherent presence of "varying conditions," developing automatic mechanisms for identifying, analysing, and deleting data is a highly challenging task. Consequently, imposing strict timelines for personal data retention and erasure within the scope of PbDD would be a formidable undertaking, as highlighted by the CJEU's decision to invalidate the Data Retention Directive (DRD).⁹⁷ In *Digital Rights Ireland*,⁹⁸ the CJEU concluded that the DRD failed to differentiate between data categories based on their relevance in achieving the objectives and lacked any objective justification for determining the exact duration of data retention.⁹⁹ The Court noted that the EU legislature enacted a broad and general Regulation that applied to all people¹⁰⁰ and all electronic communication

⁹⁶ The Court placed significant emphasis on the sensitive nature of the information contained in cellular samples, including the individual's health information, as well as the unique genetic code present in each sample, which holds considerable importance to the individual and their family. Given the substantial amount of personal information involved, the retention of cellular samples was deemed to represent an infringement upon the individual's right to privacy. The Court decided that the keeping of both cellular samples and DNA profiles amounted to an interference with the applicants' right to privacy under Article 8(1) of the Convention.

⁹⁷ European Union, Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC, 2006 24.

⁹⁸ *Joined cases C-293/12 and C-594/12 (GC) Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others (C-594/12) EU:C:2014:238.*

⁹⁹ The Directive mandated member states to enact legislation requiring communications service providers to retain specific types of traffic, subscriber, and geo-location data generated by their users for a duration ranging from six to 24 months. It is worth noting that member states were allowed to impose longer retention periods in cases where special circumstances justified a limited extension.

¹⁰⁰ The EU legislature has exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter.

devices, without making any distinction, limitation, or exception¹⁰¹ based on its crime-fighting objective.¹⁰²

While it may be impractical to incorporate all these variables into a data retention algorithm, the Court's ruling provides vital guidance to data controllers responsible for implementing data retention procedures under a PbDD programme. Specifically, the Court underscores the need to adhere to the principle of proportionality and emphasises the importance of incorporating safeguards (TOMs) to protect fundamental rights, such as the right to privacy and the protection of personal data, even when pursuing legitimate objectives, such as combating crime and ensuring public safety. The complexities of adopting rules, policies, and processes to lawfully implement data retention and destruction schedules using PbDD are discussed further in Chapter six.

The GDPR was developed by the EC as an essential step towards strengthening citizens' fundamental rights in the digital age and simplifying business rules in the digital single market.¹⁰³ Nevertheless, it is proving to be extremely complex to comply with when it comes to integrating and harmonising with crucial business processes, systems and activities,¹⁰⁴ as well as meeting certain criteria imposed by EU or MS domestic legislation,¹⁰⁵

¹⁰¹ The CJEU ruled that the data retention requirements imposed by Articles 3 and 6 of the Data Retention Directive violate the rights protected by Article 7 of the Charter.

¹⁰² Retained data could be made available for the purposes of severe crime investigation, detection, and prosecution.

¹⁰³ To obtain a comprehensive understanding of the objectives underpinning the GDPR, see European Commission, 'Questions and Answers - Data Protection Reform Package' (*Press corner*, 24 May 2017) <https://ec.europa.eu/commission/presscorner/detail/en/MEMO_17_1441>.

¹⁰⁴ For a high-level discussion of the real challenges faced by organisations in engaging with the GDPR, see Sean Sirur, Jason Nurse and Helena Webb, 'Are We There Yet?: Understanding the Challenges Faced in Complying with the General Data Protection Regulation (GDPR)', *Proceedings of the 2nd International Workshop on multimedia privacy and security* (ACM 2018).

¹⁰⁵ See, Lynskey (n 20). 'Therefore, national law must give effect to the Regulation's provisions, subject to the principle of national procedural autonomy.' p.72.

including in areas where processing of special categories of personal data¹⁰⁶ is required, for example, for fraud prevention, scientific research, or automated decision making.¹⁰⁷

Hence, rather than simplifying rules for companies, I argue that some aspects of the law, including the PbDD requirement, have become too blurry and at times overly complex, making it nearly impossible to implement in practice. However, in stark contrast to Koop's perspective, I do not believe that 'the trouble with the [data protection] law, as with Hitchcock's Harry, is that it is dead.'¹⁰⁸ I acknowledge that data protection law within the EU is exerting a substantial global influence, thereby having a significant impact worldwide.

Notwithstanding, specific elements of Koop's discourse merit scrutiny in this study, as my aim is to assist data controllers in attaining the goals of the GDPR, which Koop contends are predicated upon three misconceptions, or fallacies: 1) The delusion that data protection law can give individuals control over their data, which it cannot; 2) The misconception that the reform simplifies the law, while in fact it makes compliance even more complex; and 3) The assumption that data protection law should be comprehensive, which stretches data protection to the point of breaking and makes it meaningless law in the books.¹⁰⁹

¹⁰⁶ The scope of "special categories of data" is provided by Article 9, GDPR. '[D]ata revealing *racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, [...] genetic data, biometric data* for the purpose of uniquely identifying a natural person, *data concerning health or data concerning a natural person's sex life or sexual orientation* [..]' (emphasis added).

¹⁰⁷ For an examination of the discrepancies present across several provisions within the GDPR, see Lokke Moerel, 'GDPR Conundrums: The GDPR Applicability Regime — Part 1: Controllers' (*IAPP Privacy tracker*, 29 January 2018) <<https://iapp.org/news/a/gdpr-conundrums-the-gdpr-applicability-regime-part-1-controllers/>>. See also '11 Drafting Flaws for the European Commission to Address in Its Upcoming GDPR Review' <<https://iapp.org/news/a/11-drafting-flaws-for-the-ec-to-address-in-its-upcoming-gdpr-review/>>.

¹⁰⁸ Bert-Jaap Koops, 'The Trouble with European Data Protection Law' (2014) 4 *International Data Privacy Law* 250. (emphasis added).

¹⁰⁹ *ibid.*

Therefore, I will examine the validity of claims that a number of GDPR requirements impose additional hardship on organisations by requiring the implementation of costly and disruptive changes¹¹⁰ that make compliance more difficult than it has to be, or outright impossible in some instances. In that regard, I will focus on areas where significant challenges arise in implementing and developing suitable internal systems and processes to handle the administration, oversight, and maintenance of substantial volumes of personal information, all while ensuring compliance with legal requirements,¹¹¹ and with the application of PbDD¹¹² as a continual activity across business departments.¹¹³

Although it has been established that Article 25 GDPR creates a general duty on data controllers and processors to implement 'data protection by design and by default,' the principles of PbDD tend to be incompatible with technological advances such as Blockchain, Internet of things (IoT) and Artificial intelligence (AI) and, to some extent, with methods of privacy management based solely on organisational "accountability." Among the criticisms of Article 25 GDPR, some flaws include: it lacks scope, it fails to provide sufficient examples of TOMs - other than pseudonymisation and encryption - and it employs vague language.¹¹⁴ Organisations find it difficult to translate the principles of Article 25 GDPR into concrete actions during the development of products or services.

¹¹⁰ As per Article 25 of the GDPR, the data controller is required to take into account the cost of implementation when determining and implementing the appropriate technical and organisational measures, as well as the requisite security safeguards, to ensure the effective implementation of data protection principles and uphold the rights of data subjects. This encompasses the consideration of both time and personnel resources.

¹¹¹ Seo and others (n 87).

¹¹² See Mireille Hildebrandt and Laura Tielemans, 'Data Protection by Design and Technology Neutral Law' (2013) 29 Computer Law & Security Review 509. 'The legal obligation of data protection by design (DPbD) is a provocative concept and a challenging obligation.'

¹¹³ For an overview of practical GDPR compliance requirements, including aspects of e-discovery of personal data, data retention management, PbD, in a large or medium-sized organisation, see Murty Vedula, 'GDPR Compliance: The IT Role' (2019) 61 ITNOW 44.

¹¹⁴ Purtova (n 76).

Determining what constitutes "privacy-friendly" design or "default settings" can be a complex task, and there may be uncertainty about whether certain measures are sufficient to meet the GDPR requirements. Moreover, Article 25 GDPR employs broad and somewhat abstract language, such as the requirement to implement "appropriate technical and organisational measures" for data protection. The concept of "data protection by design and by default" itself is somewhat subjective, and different stakeholders may interpret it differently. The lack of specific guidelines or a detailed framework, such as the proposed DPPA, makes it challenging for organisations to determine what measures are considered appropriate for their specific context. It is also noteworthy that the swift evolution of technology can outstrip the formulation of precise requirements for compliance. With the emergence of new technologies, ensuring the incorporation of data protection measures into the design and default settings of innovative systems may pose increased challenges.

Since the research question that I present below focuses primarily on the feasibility of the practical application of PbDD and its importance in ensuring the efficacy of the GDPR legal framework, particularly due to its contemporaneity in the context of emerging technologies, another criticism that I will address is the claim that the Regulation does not provide sufficient discussion about the practical application of PbDD, therefore increasing uncertainty as to what Article 25 GDPR intends to achieve, rendering PbDD in this circumstance a "command that cannot be obeyed."

In order to evaluate the efficacy of GDPR, namely with regard to its application in emerging technologies, it is imperative to first consider the feasibility of implementing PbDD principles within organisational practices. This aspect assumes significant importance as it pertains to safeguarding individuals' fundamental rights, while also ensuring the establishment of adequate standards for business data security, privacy, and information

governance. Since the GDPR leaves open what exact measures should be taken in order to protect personal data, I believe legal uncertainty has become endemic to PbDD.¹¹⁵ Therefore, in an effort to bridge the existing gaps between law and data security,¹¹⁶ the research question presented in the study primarily focuses on the feasibility of practical application of the PbDD principles ('effectiveness'), and on the realisation of the personal data security principle ('integrity and confidentiality').¹¹⁷

To undertake a comprehensive exploration of the intricate nature of PbDD, as defined by the GDPR, this analysis will leverage my substantial experience and personal challenges as a data protection practitioner, particularly in relation to businesses' endeavours to safeguard personal data (organisational perspective), the impact of technological advancements on its efficacy (technological perspective), and the present legal status in the EU (legal perspective). The practicability of the regulatory structure proposed by the GDPR will be assessed based on the following research question:

Can organisations successfully implement Data Protection by Design and Default as stipulated by the GDPR, or does it represent a 'command that cannot be obeyed'?

Therefore, the primary aim of my research is to investigate the effectiveness of implementing PbDD within organisations, in alignment with the requirements specified by

¹¹⁵ One of the goals of this thesis is to pave new paths for GDPR compliance, thereby improving legal certainty without jeopardising the legal protections already provided to data subjects by the GDPR.

¹¹⁶ GDPR, Recital 78. 'The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met.'

¹¹⁷ GDPR, Article 5(1)(f).

the GDPR. The study will primarily focus on exploring the insights derived from fines issued by supervisory authorities in the EU and UK, upon which I will offer a meticulous examination and provide a detailed explanation in Chapter two. Moreover, in Chapter two, I will delve into the methodologies employed for analysing GDPR fines data. By conducting this comprehensive analysis, a profound understanding of the practical implications and challenges associated with the implementation of PbDD will be attained.

1.3. Contribution of this thesis

According to the GDPR, organisations acting as data controllers and processors must implement appropriate measures to effectively uphold data protection principles and safeguard individual rights. This necessitates organisations to integrate data protection into all stages of their processing activities and operations, beginning from the design phase and continuing throughout the entire lifecycle. Termed "Data Protection by Design and by Default" (PbDD), this approach's stipulations are outlined in Articles 25(1) and 25(2) of the GDPR, representing the apex of GDPR compliance.

To the best of my knowledge, no academic has conducted a comprehensive examination of the emergence and progression of compliance issues with PbDD in the context of GDPR for organisations, nor have they presented potential solutions.

In this thesis, my objective is to address the gap in the literature by delivering a comprehensive analysis of the legal issues surrounding PbDD and their implications for its practical implementation, therefore, the analysis of fines imposed by supervisory authorities under the GDPR serves a crucial purpose within this research. It enables a thorough examination of the challenges and difficulties faced by organisations when

striving to achieve compliance with the GDPR. By scrutinising the fines, it becomes possible to identify recurring patterns, common violations, and specific areas where organisations encounter the most significant obstacles in adhering to the regulatory requirements. Moreover, the study of these fines offers valuable insights into the specific aspects of PbDD implementation that have proven deficient or problematic. It aids in the identification of gaps in organisational comprehension, implementation strategies, and internal systems that have contributed to instances of non-compliance. Understanding these challenges and shortcomings establishes a foundation for developing comprehensive recommendations and strategies aimed at effectively addressing them.

The insights derived from the analysis of supervisory authorities' fines greatly contribute to the focus and trajectory of this study. By examining patterns, trends, and specific instances of non-compliance, my research could narrow its scope and identify key areas of concern. This analytical approach directed the investigation towards a comprehensive exploration of the practical implications and challenges associated with achieving successful PbDD implementation. Furthermore, it has facilitated a targeted and well-informed approach to comprehending the factors that impede compliance and devising effective strategies to enhance organisational adherence to the GDPR requirements. This has culminated in the development of a practical framework that clarifies and streamlines the compliance process for organisations, incorporating a crucial element of "operationalisation" of the law within the business context, which has long been awaited.

By offering a practical framework for compliance, this work provides guidance for organisations struggling with PbDD implementation, allowing them to streamline their data protection efforts and reduce the risk of GDPR fines.

This study intends thus to mitigate, to the fullest extent possible, the internal inconsistencies and external limitations of the GDPR regarding the implementation of PbDD. By doing so, it contributes to a more comprehensive understanding of the issues affecting the current regulatory regime in the field of EU data protection law and to propose solutions that can improve the current state of affairs. As a result, significant progress is expected to be made towards the operationalisation of PbDD in businesses, thereby enhancing the present situation. This study can serve as a pilot for future research projects, benefiting academics, data protection practitioners, and policymakers by providing a better understanding of the practical aspects associated with the incorporation of PbDD principles into business operations, while highlighting the key vulnerabilities of PbDD and the inconsistencies in the Regulation that limit its practical application. Rather than merely creating a roadmap for GDPR compliance, this research makes a significant contribution to the field of data protection law by expanding and elaborating upon the theory of PbDD. Despite the fact that this study's innovative compliance model does not resolve the issues pertaining to the compatibility of technology with the law, it emerges as a stand-alone framework that provides a practical model for effectively managing personal data protection to a standard very close to that required by the GDPR when combined with PbDD.

Unveiling the Data Protection Principles Approach (DPPA)

The creation of the DPPA framework represents a significant step forward in facilitating organisations' compliance with the GDPR, as it offers a practical “roadmap” for managing personal data protection with a high degree of precision. This framework will help organisations address the challenges posed by PbDD implementation and enhance

their overall data protection measures. In my opinion, the DPPA framework's creation marks a milestone in the domain of GDPR compliance, as it holds the potential to advance the practical application of PbDD principles and contribute to the GDPR's overall effectiveness.

While the GDPR has been in force for some time, it is noteworthy that certain aspects of this regulatory framework, particularly as they relate to emerging technologies remain underdeveloped. Notwithstanding my diligent research efforts, I encountered a dearth of specific guidance and authoritative case law pertaining to certain aspects of the GDPR, particularly as they relate to the burgeoning fields of IoT, Blockchain, and AI.¹¹⁸

Therefore, this study undertakes a rigorous analysis to examine the interpretation of PbDD in *de lege ferenda*, with a particular emphasis on the context of emerging technologies, which is widely acknowledged as the sphere where the future lies. The aim is to clarify the challenges and inconsistencies inherent in the current GDPR framework by presenting case studies that exemplify areas where PbDD exhibits limitations and presents substantial difficulties in aligning with GDPR requirements. The intention is to provide “tangible examples” that highlight the current deficiencies of PbDD, thereby demonstrating the intricate complexities involved in consolidating its implementation within the existing regulatory framework. The inclusion of these case studies assumes a critical role within the research methodology, providing compelling illustrations of the practical obstacles and limitations currently encountered during the implementation of PbDD. Furthermore, by

¹¹⁸ Advocate General Sharpston had previously noted a lack of legislative will to consider emerging technologies (in this case AI). See AG’s Opinion delivered on 15 October 2009, *Bavarian Lager [2010]* (n 38). ‘I deliberately leave aside the question whether it would be possible, by the application of artificial intelligence (‘AI’), to replace any/some/most/all of the functions currently performed manually. [...] Furthermore, it seems a little unlikely that the Community legislator had AI potential in mind when framing Regulation No 1049/2001.’ para. 64. (emphasis added).

examining these case studies, researchers can gain a deeper understanding of the intricate relationship between emerging technologies and the GDPR. This knowledge is crucial for staying abreast of the evolving digital landscape and effectively addressing the challenges posed by new technologies. By scrutinising these real-world scenarios, alternative approaches will be proposed to effectively address the identified challenges and bridge the existing gaps. The ultimate objective is to offer practical guidance to businesses and provide policymakers with valuable insights that can inform future amendments to the GDPR, ensuring its ongoing relevance, effectiveness, and adaptability in the face of emerging technologies. Through the implementation of these proposed amendments, the GDPR can be strengthened to safeguard individuals' rights and empower them with control over their personal data, enhancing its suitability and future-proof nature more effectively.

The DPPA compliance model represents a significant advancement towards effective implementation of the GDPR, offering a range of advantages, including a) Improved compliance: The DPPA offers a practical roadmap for managing personal data protection that closely adheres to the GDPR's requirements. By facilitating the resolution of the challenges posed by PbDD implementation, this framework enhances overall data protection measures, thereby improving compliance with the GDPR; b) Cost-effectiveness: The streamlined approach to personal data management adopted by the DPPA compliance model enables organisations to implement the GDPR's requirements at reduced costs. By providing a clear and concise framework for managing personal data, the DPPA helps organisations avoid costly compliance errors; c) Enhanced Data Protection: The DPPA compliance model prioritises data protection, ensuring that organisations adopt best practices for safeguarding personal data. This approach results in better data protection outcomes, which are crucial for maintaining data subject's trust and avoiding reputational

damage; d) Scalability: The DPPA is designed to be scalable, making it applicable to organisations of varying sizes and complexities. This framework can be customised to meet the unique needs of different businesses, ensuring that it remains relevant and effective in diverse contexts; e) Future-proof: The DPPA is adaptable to emerging technologies and changing regulatory environments, making it future-proof. As new technologies and Regulations emerge, the DPPA framework can be updated to ensure ongoing compliance with the GDPR's requirements, thus offering a sustainable and reliable compliance solution. In summary, the DPPA compliance model offers several benefits that are instrumental in enhancing compliance with the GDPR, safeguarding personal data, and maintaining individual's trust.

This research successfully uncovered critical areas of GDPR compliance that pose significant challenges to organisations by tracking the grounds for violation from which most fines originated. Through the analysis of this information, vital edge issues and substantial challenges currently confronting organisations were identified. These findings played a central role in shaping the proposed compliance framework, with the aim of supporting improved compliance and effectively addressing the identified challenges. One such challenge is the integration of data protection principles and the establishment of effective mechanisms for addressing data subjects' rights into modern technologies.¹¹⁹ This accomplishment was achieved through the utilisation of a correlational analysis methodology, applied to publicly available data provided by the EU supervisory

¹¹⁹ As an illustration, with respect to the right to be forgotten, expunging personal data in a blockchain environment is unfeasible from a technical standpoint, as the system is inherently designed to preclude it.

authorities.¹²⁰ In addition, a thorough examination of pertinent technical literature was conducted to further enhance the understanding of the subject matter.

I believe that, at this stage, it is crucial to provide an explanation regarding the territorial approach adopted in this thesis, which takes a "no-borders" perspective by acknowledging the universal applicability of the GDPR to all EU member states. Consequently, no specific jurisdiction within the EU was exclusively the focus of this study. This signals that the study adopts a broad and inclusive view, recognising the universal applicability of the GDPR. This perspective aligns with the GDPR's intent to establish a unified framework for data protection and helps orient readers to the scope and perspective of the study. Instead of narrowing the scope to a particular jurisdiction, this research encompasses the collective impact and implications of the GDPR on the EU as a whole. In the context of this study, the aim is to investigate the broader applicability and ramifications of the GDPR within the integrated entity of the EU. Additionally, the study is mindful of the effects on third countries that process data of individuals in the EU. Therefore, my research delves into the harmonisation of data protection practices and the common challenges faced by organisations operating within the EU or processing data of individuals in the EU, transcending the limitations of any singular jurisdiction. By embracing this approach, the thesis takes a holistic perspective, acknowledging the shared responsibilities and obligations imposed by the GDPR on all EU countries and third countries processing data of individuals in the EU.

This study also offers valuable insights into the practical challenges that worldwide organisations encounter when striving to achieve PbDD compliance. Article 3 GDPR

¹²⁰ In this thesis, the term "EU Supervisory authorities" refers to regulatory bodies in both the EU and the UK.

establishes the territorial scope of the GDPR, which has both territorial and extraterritorial effects. In accordance with the principle of the place of performance, *lex loci solutionis*, the GDPR also applies if personal data of a data subject located in the EU is processed by an organisation located outside European borders, and the processing is related to the provision of goods or services.¹²¹ To protect personal data, the GDPR also mandates the monitoring of data that is exported outside the EU. To illustrate the global impact of GDPR, according to a PwC survey, 92 percent of US companies consider GDPR to be their top data protection priority.¹²² GDPR compliance is thus an issue affecting millions of organisations worldwide.

In this regard, this study also serves as a convergence point of interests, notably by presenting a comprehensive case study on the intricate relationship between the European Union (EU) and the United States (US) regarding the transfer of personal data and the challenges that arise within this realm of data processing. The study aims to address this issue by proposing appropriate measures for transfers of personal data between the EU and third countries, which will be included as a reference in the DPPA. The case study highlights the contrasting approaches to data protection between the United States (US) and the European Union (EU), which have resulted in notable tensions between the two regions. The US government has expressed concerns that the GDPR's strict requirements may impede cross-border data flows and hinder economic growth. To address the concerns raised regarding data transfers between the EU and the US, and to ensure that these transfers are legal and compliant with the GDPR, ongoing discussions are taking place

¹²¹ Annegret Bendiek and Magnus Römer, 'Externalizing Europe: The Global Effects of European Data Protection' (2019) 21 Digital Policy, Regulation and Governance 32.

¹²² 'Pulse Survey: US Companies Ramping up General Data Protection Regulation (GDPR) Budgets' 3.

between the two regions. The primary objective of these discussions is to establish a framework that facilitates the smooth transfer of personal data while maintaining robust data protection standards. Chapter six of this study will delve deeper into this topic.

Moreover, as a practitioner with extensive experience in the field of information privacy, I successfully employed a methodological approach that relied on my practical knowledge and the challenges encountered to navigate effectively between the aspects of *lex lata* and *lex ferenda*. As a result, a PbDD-based conceptual framework (DPPA) was developed, offering a practical approach to attaining global GDPR compliance. This framework is firmly grounded in the real-world challenges faced by organisations, making it a notable and practical contribution to the field. As a matter of reflection, it is worth noting, however, that any proposals for incorporating this framework into business operations are subject to acceptance or rejection by business leaders, similar to how policymakers may accept or reject proposed legislative changes. Nevertheless, the proposed framework offers a valuable tool that can assist in guiding decision-making and work practices by providing evidence and an informed evaluation of policy change options. As such, this work holds significant importance for both academics and practitioners in the field of information privacy, as it contributes to the development of practical solutions for achieving PbDD-based GDPR compliance.

Contributions of this thesis include thus the provision of a novel, adequate, holistic and pragmatic framework-based approach to GDPR implementation, titled Data Protection Principles Approach ('DPPA'). The DPPA aims to (i) provide the most effective means of incorporating the GDPR legal framework into current business operations, and (ii) provide organisations with additional tools to supplement PbDD-based privacy management approaches in order to demonstrate legal compliance conclusively.

1.4. Difficulties encountered throughout the research

At the outset of the study, the aim was to conduct a comprehensive exploration of the issues surrounding the implementation of PbDD across all areas of personal data security and protection. However, it was soon evident that this undertaking was too vast and complex to be addressed by a single study. Subsequently, the focus of the research shifted to identifying the primary motivators for regulators to impose fines. Through a reverse engineering approach, fines were analysed to uncover underlying issues leading to violations and following a review of the literature, it became apparent that the initial focus of the study should instead be on issues such as the lack of clarity, complexity, and high costs associated with implementing the Regulation. Data breaches were used as a motivator for implementing technological and organisational measures aimed at protecting personal data. Despite these challenges, the study's results provide valuable insights into the issues surrounding the implementation of PbDD in organisations' personal data processing operations and provide practical solutions for addressing these real-world obstacles through the development of the DPPA compliance framework.

The results of my research uncovered several inconsistencies between the GDPR and emerging technologies, as well as organisational data protection limitations that impede the practical application of PbDD. These constraints, when combined with data pertaining to the penalties levied by EU/UK supervisory authorities, proved to be critical data points for the development of the DPPA framework.

However, the outbreak of Covid-19 and subsequent national lockdowns hindered the ability of some EU regulators to provide timely access to their enforcement records. As a result, reliance had to be placed on data gathered by global privacy non-governmental

organisations such as Noyb, as well as data obtained from publicly available databases like the CMS Enforcement Tracker, which may not have been as comprehensive or reliable as official data. These challenges may have limited the scope of the study and its ability to access critical data points.

Furthermore, a critical component of the study was the assessment of theoretical concepts in relation to their practical application. Regrettably, the COVID-19 pandemic created obstacles for conducting face-to-face meetings with industry experts in the field of business privacy, thereby adding a layer of complexity to the evaluation process. The outbreak of Covid-19 also posed additional challenges to the research process, including the difficulties associated with conducting research remotely. Furthermore, the Covid-19 pandemic precluded the ability to deploy, examine, and assess the efficacy of the DPPA in a genuine business environment. This inability to fully test the DPPA in a real-world setting limits the study's ability to draw definitive conclusions about its effectiveness and may call for further testing in the future.

1.5. Limitations

The DPPA offers a comprehensive set of TOMs for data protection, meticulously curated through a thorough analysis of relevant technical literature. In addition, the DPPA outlines the steps necessary to establish a data protection program that relies on successful implementation of data protection principles and mechanisms to uphold data subject rights through PbDD. These measures have been selected based on their prevalence and prominence in contemporary discussions on data protection, with the intention of demonstrating the effectiveness of the model for the implementation of PbDD and the

operationalisation of the GDPR. It should be noted that while the selected list of TOMs included in the DPPA is not intended to be exhaustive, it serves as a valuable resource for organisations seeking to enhance their data protection practices.

My research focused on the challenges related to the actual implementation of PbDD, namely the operational procedure, to outline how a PbDD implementation model needs to function in practice. However, it is essential to note that any tensions and conflicts that may arise regarding specific technological and legal functional requirements have not been fully explored. To demonstrate the importance of a legal-technical interoperability framework, the study examines data protection trends in ever-changing processing business systems and operations and correlates them with existent industry security standards. Therefore, the successful application of the DPPA in a real-world scenario requires the intervention of technology experts who can determine the most appropriate technical measures in relation to each processing activity.

My research aimed to identify the most significant barriers to PbDD implementation by using publicly available data on fines issued by EU supervisory authorities and "reverse-engineering" the decisions, classifying them in proportion to their importance to PbDD. The findings reveal that the most common obstacles to GDPR compliance are as follows: a) insufficient TOMs to comply with general data processing principles; b) insufficient or no legal basis for personal data processing; c) insufficient TOMs for fulfilment of information obligations; d) insufficient TOMs to ensure information security; and e) insufficient TOMs to fulfil data subjects' rights. While this work provides essential insights into the most significant obstacles to GDPR compliance, I am mindful of the following limitations:

Limited scope: My research focuses primarily on the findings of fines imposed by EU/UK regulators and may not reflect the full range of obstacles to GDPR compliance. For

example, many organisations may have difficulty implementing PbDD, even if they have not yet received a fine.

Publicly available data: My research relies on publicly available data, which may not provide a complete picture of the reasons for GDPR fines. Some fines may have been settled through private negotiations, and the details of the violations may not have been disclosed. There may have been many violations that did not result in a fine or enforcement action.

Reverse-engineering approach: My research relies on "reverse-engineering" the decisions made by supervisory authorities to classify violations in proportion to their importance to PbDD. While this approach may be useful, it may not accurately reflect the actual importance of each violation to PbDD.

Lack of context: My research does not consider the specific circumstances and context of each violation. Some violations may be more significant than others depending on factors such as the type of data involved, the size of the organisation, and the potential harm to data subjects.

The present research undertakes an analysis of penalties levied by all EU Member States and the United Kingdom, focusing solely on fines that have been made publicly accessible. However, it must be acknowledged that the differences in policies among supervisory authorities regarding the publication of fines create an inherent limitation in the data provided by the Enforcement Tracker, which serves as primary data source for this study. Nonetheless, to mitigate this limitation, extensive efforts have been made to

supplement and correlate this dataset with information obtained directly from supervisory authorities^{123,124} and gathered from Noyb's GDPRhub Decision database.¹²⁵

By all the above, the findings should be viewed within the context of these limitations, and further research is necessary to gain a more comprehensive understanding of the obstacles to PbDD implementation.

1.6. Outline of the chapters

This thesis represents a comprehensive and meticulously structured analysis that contributes to a deeper understanding of the complex issues surrounding the protection of personal data within the context of the General Data Protection Regulation (GDPR) and Data Protection by Design and Default (PbDD). The ten chapters of this work build upon one another in a systematic and in-depth manner to provide a comprehensive overview of the hurdles faced by organisations seeking to comply with the GDPR while adhering to the principles of PbDD.

The focal point of this study is the introduction of the DPPA compliance framework. The DPPA is specifically tailored to aid organisations in their efforts to comply with the GDPR and surmount the challenges associated with it. This compliance model presents a practical guide that simplifies the GDPR implementation process and assists in identifying

¹²³ In this thesis, the term "Supervisory authorities" refers to regulatory bodies in both the EU and the UK.

¹²⁴ Annex 3 contains a list of the Supervisory authorities that were invited to contribute data for this thesis. While not all of them provided the requested information, any gaps were filled by consulting their official websites. These sites typically include public pages with comprehensive information about the authorities' decisions and the fines they have imposed.

¹²⁵ The GDPRhub Decision database, collects and summarises decisions from Data Protection Authorities and courts across Europe. < https://gdprhub.eu/index.php?title=Welcome_to_GDPRhub>.

appropriate measures for each relevant GDPR Article and processing activity. The introduction of the DPPA framework thus constitutes a notable contribution to the field of data protection law.

Overall, this thesis represents a valuable resource for scholars and practitioners seeking a more nuanced understanding of personal data protection and its relationship to PbDD. Chapter one serves as an introduction to the research, providing an overview of the background and objectives of the study, highlighting the contribution of the thesis for this field of knowledge. The chapter also discusses the challenges faced during the research, such as those brought about by the global COVID-19 pandemic, identifies the limitations of the study and provides an outline of the Chapters forming it.

Chapter two provides a detailed account of the methodology applied in this study. It clarifies the approach taken for the literature review and outlines the distinctive method employed for the analysis of both quantitative and qualitative data, linked by correlation techniques. This approach is considered one of the innovative aspects of this work.

Chapter three elucidates the theoretical framework underpinning the Data Protection Principles Approach (DPPA) and contextualises its applicability within the context of GDPR, with a specific focus on aspects of Legal Certainty.

Chapter four presents a conceptual analysis of PbDD, delving into the core principles of the GDPR and the rights of data subjects, and examining the feasibility of implementing PbDD in practice. This chapter scrutinises the theoretical aspects of PbDD, including its benefits and limitations, and proposes alternative approaches to address the challenges posed by the GDPR. Additionally, it highlights the potential advantages of integrating PbDD into organisational practices.

Chapter five highlights the importance of PbDD as a foundational concept for GDPR compliance and examines the challenges associated with the applicability of the GDPR in the context of technological advancements. By focusing on emerging technologies such as Blockchain, IoT, and AI, the chapter underscores the need for effective data protection measures to keep pace with technological advancements.

Chapter six examines aspects of the applicability of PbDD in an organisation's technological context. The chapter also addresses important issues of data quality and security, including potential hurdles such as the processing of legacy personal data. By examining the technical aspects of GDPR compliance, this chapter offers practical solutions for organisations seeking to implement PbDD.

Chapter seven focuses on the implications of the lack of clarity and guidance provided by the Regulation and examines the challenges faced by organisations attempting to conform to PbDD principles. The economic implications of implementing the GDPR are also discussed at length, highlighting the potential costs and benefits of compliance.

Chapters eight and nine provide an in-depth exploration of my compliance framework, known as the Data Protection Principles Approach (DPPA). Within the context of the EU GDPR, I consider this framework to be the most versatile and adaptable strategy for implementing PbDD. This framework serves as an operational guide for simplifying the GDPR implementation process and identifying appropriate measures for each GDPR Article and processing case. By offering a practical framework for implementing PbDD, these chapters provide organisations with a roadmap for effective GDPR compliance.

Chapter ten presents the research findings and contributions made by the thesis to the field of data protection law. The chapter also suggests areas for future research and provides recommendations for controllers and lawmakers to ensure effective

implementation of PbDD principles within the GDPR framework. Through its systematic and consistent approach, this work offers valuable insights into the complex issues of data protection law and shows practical solutions to overcome these challenges.

1.7. Concluding remarks

In concluding this introductory chapter, I have endeavoured to establish the contextual framework for the study, providing insights into the scope and significance of my research. The identification of the research problem and the formulation of a pertinent research question serve as a roadmap guiding subsequent chapters.

The contributions of this thesis are twofold: addressing the identified research gap and contributing to the broader discourse on the operationalisation of PbDD. By examining the challenges faced by organisations operating within the EU and those processing data of individuals in the EU, my study aims to illuminate the harmonisation of data protection practices. This overarching goal aligns with the ongoing efforts to establish a cohesive and effective data protection framework in the European context.

Throughout the research process, I have encountered various difficulties inherent in the complex nature of bridging theoretical legal concepts into business data processing operations. These challenges have been integral in shaping the methodology employed in the subsequent chapters. While I acknowledge these obstacles, they have provided valuable insights into the intricacies of my research domain.

However, I found it essential to acknowledge the limitations of this study. These constraints, whether inherent or environmental (such as the impact of the COVID-19 global

lockdown), are crucial in understanding the boundaries within which my findings should be interpreted.

As I transition to the literature review and methodology chapter, the groundwork laid in this introductory section provides a solid foundation for the ensuing analytical exploration. The literature review will further delve into existing scholarship and case law, setting the stage for my methodology, which was meticulously crafted to address the identified research question.

Chapter 2 – Literature review and methodology

Introductory notes

The study commences with an evaluation of Cavoukian's framework of 'Privacy by Design' and addresses key preparatory inquiries such as: 'What is the GDPR?', 'What is the significance of the terms 'privacy' and 'data protection'?', 'What do the terms 'data protection by design' and 'by default' mean in relation to GDPR?', and 'How does the legal definition of personal data influence its processing?'. This line of enquiry tries to disentangle key concepts buried in the Regulation and to elucidate the challenges and potential compliance issues that may arise from the implementation of PbDD.

The thesis is constructed upon three primary areas of investigation: (i) the uncertainty that surrounds the GDPR (specifically, the lack of clarity and definitive guidance within the Regulation, which can hinder organisations' ability to implement PbDD requirements effectively); (ii) the applicability of the GDPR (whether the GDPR has become excessively intricate and has failed to keep pace with technological developments, making it challenging to implement in practice); and (iii) the complexity and expense of implementing the GDPR (which aspects of the GDPR make it complex, and how can these challenges be addressed?; a cost and benefit analysis, considering the economic implications and whether the implementation cost is a barrier for organisations).

The study is also aimed at identifying the adverse outcomes resulting from non-compliance with data protection principles and individual's rights. This will be achieved by conducting both quantitative and qualitative analyses and evaluations of penalties imposed by EU supervisory authorities within the first four years of GDPR enforcement.

The primary objective is to determine whether the violations of GDPR that prompted regulatory action were due to inadequate implementation of PbDD.

The inclusion of a separate chapter dedicated to the literature review and methodology in this thesis serves several important purposes, namely, it serves to maintain clarity and organisation in the thesis. By having a separate chapter for the literature review and methodology, the thesis can delve deeper into each aspect without overwhelming the introduction with excessive details. Moreover, separating these chapters facilitates a logical flow of information, as this sequential arrangement helps the reader better understand the progression of the research process and the rationale behind the chosen approach.

2.1. Literature review and methodology

The literature review can be defined as a 'summary of a subject field that supports the identification of specific research questions.'¹²⁶ The inclusion of arguments from the literature review throughout this thesis (there is no specific chapter dedicated to it), which looks at the implementation of EU data protection law into businesses sectors and operations, intends to facilitate the fundamental interdisciplinary conversation between professional disciplines such as information systems management, cyber-security, and legal scholarship. The latter, due to its nature - anchored predominantly on theoretical reasoning - evolves by taking a more critical approach to the legal concepts enshrined in

¹²⁶ Jennifer Rowley and Frances Slack, 'Conducting a Literature Review' (2004) 27 *Management research news* 31.

the GDPR and by convening and bringing in contemporary academic views on data protection to better underpin the feasibility study of PbDD practical implementation (or, on the 'operationalisation of the law').

Although my methodological approach cannot be considered, *de facto*, as interdisciplinary, I understand that, to a certain extent, interdisciplinarity becomes a requirement when materialising EU data protection law into businesses' operations. This is due to GDPR requirements compelling organisations, inter alia, to 'implement appropriate TOMs to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation.'¹²⁷ and '(...) for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.'¹²⁸ I believe that such important dialogue between technology and law, which is rooted in the concept of PbDD,¹²⁹ and expected in the context of the activities related to the implementation of PbDD, is invoked in the GDPR in a veiled way. I maintain that there is a lack of clarity regarding the practical application of PbDD in day-to-day business operations, and it appears that the GDPR does not effectively communicate its objectives to those responsible for ensuring its implementation, maintaining information systems, and ensuring corporate governance. This has an impact on organisations' compliance efforts.

The idea of interdisciplinarity, or at least collaboration between technology and law, or between engineers and lawyers, was influenced by the principle of PbD and

¹²⁷ GDPR, Article 24.

¹²⁸ GDPR, Article 25.

¹²⁹ It is noteworthy to emphasise that PbDD encapsulates the "fundamentally technological" tenets of Cavoukian's PbD, elevating them to a legal requirement and thereby establishing an interdisciplinary nexus between law and technology (e.g., in areas such as information systems management and cybersecurity).

embedded in the concept of PbDD provided by the European Commission (EC) in its final 2012 proposal for GDPR:

‘The principle of ‘Privacy by Design’ means that privacy and data protection are embedded throughout the entire life cycle of technologies, from the early design stage to their deployment, use and ultimate disposal.’¹³⁰

Some academics and practitioners consider the above initial definition of PbDD to be vague, meaningless and insufficiently expanded by the legislation enacted - in my opinion, it remains vague as to its full meaning and, more importantly, its practical application in business systems, processes and operations. Consequently, a thorough literature review is deemed essential not only to contextualise the thesis but also to identify relevant issues and trends that may otherwise go unnoticed if viewed solely through the lens of a legal scholar. In addition to references to primary and secondary law, legal research, and scholarly Articles, this work's literature review will consider select reports, opinions, and journal Articles presented by information security professionals and privacy practitioners in relevant technological areas. This will undoubtedly aid in identifying and better comprehending recent developments in context.

The study presents some methodological challenges in that it endeavours to map contemporary data protection issues against business practices and existing "soft" and "hard" law. This is done in order to construct answers to several legal issues, many of which

¹³⁰ European Commission, ‘Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 25.01.2012, COM(2012) 11 Final’.

are practically emergent, in the sphere of PbDD. Furthermore, the study aims to apply these answers to the constantly evolving organisational and technological business processes, facilitating organisations' compliance with GDPR. The applied methodology is primarily doctrinal, relying on the study of legislation and case law, as well as literature focused on the theories of privacy and data protection law.¹³¹ Duly reference is made to judicial decisions, regulatory guidance provided by supervisory authorities and doctrine on relevant aspects or sub-aspects of the practical application of the GDPR, particularly in relation to concepts such as personal data, privacy by design, and data protection by design and default. Salter and Mason¹³² describe legal doctrinal research as an in-depth and highly technical commentary on the context of legal doctrine and systematic exposition of it. This statement holds true for data protection law since it is a subject area heavily shaped by statutes and cases and exposed to socio-political factors. This initial internal methodological approach allows the selection of the relevant aspects of the law through a critical analysis of the literature with the aim of identifying the main problems of practical emergence.¹³³

The chosen method seeks thus to facilitate the discussion on the feasibility of the implementation of PbDD and GDPR beyond the "law of books" which occasionally requires

¹³¹ See Vijay M Gawas, 'Doctrinal Legal Research Method a Guiding Principle in Reforming the Law and Legal System towards the Research Development' (2017) Volume 3 International Journal of Law 128. 'Most of the doctrinal research sources are text books, periodicals, and commentaries but they do not possess as much authority as the original sources like enactment and case published by authorized publisher. Similarly, the acts passed by state legislatures and parliament fall under the category of precedents. But all case laws decided by Supreme Court and high courts which are binding on lower courts are also part of doctrinal research sources.'

¹³² Michael Salter and Julie Mason, *Writing Law Dissertations : An Introduction and Guide to the Conduct of Legal Research : An Introduction and Guide to the Conduct of Legal Research* (Pearson Education UK 2007) <<http://ebookcentral.proquest.com/lib/reading/detail.action?docID=5136574>>.

¹³³ See Richard L Schwartz, 'Internal and External Method in the Study of Law' (1992) 11 Law and Philosophy 179.

an inter-disciplinary dialogue between legal scholarship and other disciplines, namely, information systems management and cyber security. In addition, it aims to provide better and more informed outcomes, particularly, by allowing the use of statistics and correlational data analysis, in a legal area where limiting factors emerge from organisational or technological spheres that are outside the remit of the legal scholarship.

In order to determine the “appropriateness” of TOMs in the context of PbDD, as well as the feasibility of implementing PbDD in practise, I investigate and analyse data requirements against the current state of the art (empirical research) to draw normative conclusions. With this, I hope to create a collection of theorems that, when combined with the GDPR’s PbDD framework in a functional context, will facilitate its operationalisation.

To provide a more comprehensive understanding of the practical considerations involved in implementing GDPR standards, this thesis looks at the various data protection management activities required. One such activity is the GAP analysis, a core element of the DPPA, which involves identifying the gaps between an organisation's current practices and the GDPR's obligations. This analysis provides a foundation for determining the necessary changes that need to be implemented to comply with the Regulation. Another important activity is risk analysis. This assessment helps organisations determine the level of risk associated with their data processing activities and implement appropriate measures to mitigate those risks. Resourcing and budget planning is also an essential aspect of GDPR compliance.

In addition to the above activities, this thesis also examines the data protection structure and systems necessary to ensure GDPR compliance. This includes mechanisms that cover the rights of data subjects and principles of data protection, such as access, correction, and deletion of personal data. Demonstrating compliance with GDPR

requirements also necessitates proper documentation. This involves implementing measures to show that an organisation is adhering to GDPR obligations, such as the application of the 'accountability' principle. Finally, this thesis examines the importance of third-party relationships in GDPR compliance. Data processing agreements that data controllers are required to enter into with data processors, joint data controllers, and international transfers of personal data are critical components of the GDPR's regulatory framework. By examining these data protection management activities, this thesis aims to provide a more practical understanding of GDPR compliance and assist organisations in implementing the necessary measures to achieve compliance.

Moreover, this study aims to identify broader issues related to the practical implementation of GDPR by evaluating whether it is feasible to incorporate PbDD into modern business systems and processes, including emerging technologies, in accordance with GDPR provisions. While privacy concerns can arise from both governmental access to personal data and private companies' processing of personal data, this study focuses on the latter, which is primarily regulated by GDPR in the EU. Additionally, it highlights potential policy options and approaches that can be integrated into future legislation.¹³⁴

To address the research question, a mixed-methods approach is deemed necessary, incorporating both empirical and doctrinal approaches to legal research and integrating quantitative and qualitative data collection and analysis.¹³⁵ In this work, the integration of

¹³⁴ To explore the topic pertaining research focused on policy change, see Lucie Cerna, 'The Nature of Policy Change and Implementation: A Review of Different Theoretical Approaches' (OECD 2013) <<https://www.oecd.org/education/ceri/The%20Nature%20of%20Policy%20Change%20and%20Implementation.pdf>>.

¹³⁵ Mixed methods refer to a methodology that advances the systematic integration of quantitative and qualitative data within a single investigation or program of enquiry. The primary premise is that such integration permits a more complete utilisation of data than do separate quantitative and qualitative data collection and analysis.

both quantitative and qualitative methods can provide a more holistic approach to studying complex legal issues. For example, a quantitative study can provide statistical evidence of the effectiveness of PbDD in achieving GDPR compliance, while qualitative research can offer insights into the practical challenges and barriers to implementing PbDD in organisational settings.

Being a data protection practitioner myself, I fully support the statement that ‘the complementarity of doctrinal legal research (internal perspective),¹³⁶ and empirical legal research methods (external perspective),¹³⁷ translates as the law in the books and the law in action’.¹³⁸ I occasionally turn to primary empirical research,¹³⁹ since it is true that ‘empirical research can inform how the law is applied in practice’.¹⁴⁰

Tom Tyler,¹⁴¹ advocates the empirical method, stating that ‘actuarial risk calculations, can predict human behaviour better than intuitive hunches, and can inform law’. By focusing on establishing relationships between empirical findings and normative law, Tyler advocates for evidence-informed law; ‘better facts and better law lead to more

¹³⁶ Schwartz (n 133). ‘As applied to law, internal method reflects the viewpoint of the participant in a legal system and the traditional method of studying law, doctrinal analysis. The participant accepts the authority of legal texts and manipulates them, employing prescribed interpretive canons, for practical purposes. He also accepts and works within restrictions on the range of meanings which may permissibly be ascribed to such texts. Respected professional opinion, the product of continual discussion among lawyers and other members of the legal community, is the medium within which such restrictions take shape.’

¹³⁷ *ibid.* ‘External method is not bound by the limitations which define internal method. It does not acknowledge the authority of canonical texts and need not adhere, as does internal method, donor recruitment to approved interpretive approaches. Nor are the meanings it may ascribe to canonical texts limited by the conventional restraints which guide internal method. External readings of authoritative legal texts are therefore free to ascribe meanings to them which reflect the concepts and explanatory resources of extra-legal disciplines.’

¹³⁸ A Argyrou, ‘Making the Case for Case Studies in Empirical Legal Research’ (2017) 13 *Utrecht law review* 95.

¹³⁹ See M Gawas (n 131). ‘[T]he legal researchers are concerned with empirical investigation *but the analysis and manipulation based on the theoretical concepts.*’ (emphasis added).

¹⁴⁰ Argyrou (n 138).

¹⁴¹ Tom R Tyler, ‘Methodology in Legal Research’ (2017) 13 *Utrecht law review* 130.

justice'.¹⁴² Accordingly, research must show which factors influence human behaviour in organisations and in particular the adherence to norms and values.^{143,144}

In the scientific research method, two hypotheses have been formulated, which will be addressed based on the predictions of possible relationships between the variables emerging from the study data.

The first hypothesis (H1) posits that ineffective implementation of PbDD renders GDPR compliance impossible, leaving organisations vulnerable to data breaches. The second hypothesis (H2) proposes that integrating PbDD into a more stringent Data Protection Principles Approach (DPPA) model will result in higher levels of GDPR compliance and a greater number of data breaches being prevented.

These hypotheses will be rigorously tested using a mixed-methods approach, incorporating both empirical and legal doctrinal research techniques and the integration of quantitative and qualitative data collection and analysis. The findings of this study have the potential to inform policymakers and practitioners about the effectiveness of PbDD in achieving GDPR compliance and preventing data breaches, thereby contributing to the advancement of data protection practices and the protection of individual rights and freedoms.

In the following section, I will elucidate the empirical methodology employed in this study to gather and analyse data for a comprehensive understanding of the research topic.

¹⁴² *ibid.*

¹⁴³ PM Langbroek and others, 'Methodology of Legal Research: Challenges and Opportunities' (2017) 13 *Utrecht law review* 1.

¹⁴⁴ For a discussion of the relationship between Empirical Legal Studies and Doctrinal Legal Research see, Gareth Davies, 'The Relationship between Empirical Legal Studies and Doctrinal Legal Research' (2020) 2020 *Erasmus law review* 1.

2.2. Data sources

From the outset, the subject of this study is diverse as it consists of legislative data, technology-oriented material and quantitative secondary data originating from EU institutions, Statista,¹⁴⁵ CMS Enforcement Tracker^{146,147} and privacy NGO Noyb,^{148,149} often rendering the choice of methods somewhat challenging. In certain circumstances - particularly, when investigating the myriad of technological challenges emerging from the application of PbDD into businesses' systems (software and hardware), and the occasional incompatibilities between some business needs and GDPR requirements - the study calls for a bottom-up approach,¹⁵⁰ which includes not only a review of legal provisions, but also a summary of case studies¹⁵¹ from technological fields that are relevant to understanding

¹⁴⁵ Statista is a leading provider of market and consumer data. < <https://www.statista.com/>>.

¹⁴⁶ The CMS.Law GDPR Enforcement Tracker provides an overview of fines and penalties which data protection authorities within the EU have imposed under the EU GDPR. < <https://www.enforcementtracker.com/>>.

¹⁴⁷ Copyright notice: The 'enforcementtracker' database is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License. 'enforcementtracker.com' is provided by CMS Law.Tax. CMS Law.Tax granted all the required permissions for using the data provided in this study.

¹⁴⁸ The NGO Noyb offers the GDPRhub, an open wiki that allows anyone to find, edit and share GDPR insights, including Supervisory Authorities and Court decisions. < <https://noyb.eu/en/gdprhub>>.

¹⁴⁹ The data sets were obtained directly from EU supervisory authorities, either electronically transferred via email or extracted from their websites, complemented with data obtained from the Privacy NGO Noyb and the CMS Law (enforcement tracker) websites.

¹⁵⁰ The technique adopted is inductive, which suggests that, on the basis of the data obtained, a theory or a "search for a pattern of meaning" is established. This entails a change from the specific to the general and is often referred to as a bottom-up approach.

¹⁵¹ See, Micah Altman and others, 'Practical Approaches to Big Data Privacy over Time' (2018) 8 International Data Privacy Law 29. (with relevance to the study of data retention and big data). See also, Dominique Machetes and Rainer Böhme, 'Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR' (2019) 2020 Proceedings on Privacy Enhancing Technologies 481. (with relevance to the study of consent mechanisms under GDPR). Ze Shi Li and others, 'GDPR Compliance in the Context of Continuous Integration'. (with relevance to the study of GDPR compliance challenges to SMEs). Christos Kalloniatis and others, 'Applying Soft Computing Technologies for Implementing Privacy-Aware Systems' in Marko Bajec and Johann Eder (eds), *Advanced Information Systems Engineering Workshops* (Springer Berlin Heidelberg 2012). (with relevance to the study of PETs). S. Cimato and others, 'Privacy-Aware Biometrics: Design and Implementation of a Multimodal Verification System', *2008 Annual Computer Security Applications Conference (ACSAC)* (2008). S. Cimato and others, 'Privacy-Aware Biometrics: Design and Implementation of

the practical application of the law in business operations, thus complementing theoretical constructions with empirical results.

2.3. Data analysis (GDPR fines)

By applying computational techniques to manipulate pre-existing statistical data,¹⁵² I will employ a quantitative methodology in my research. Through a process of “deconstructing fines” imposed by the supervisory authorities and analysing their decisions, it was possible to identify, with a high level of scientific rigour, emerging issues related to the non-implementation, or defective implementation of PbDD. Additionally, several internal and external inconsistencies and constraints of the GDPR, resulting in the impracticability of PbDD, could be identified.

The use of these datasets is critical to the study since the results of the analysis shed light on fundamental issues of GDPR implementation and PbDD in particular.¹⁵³ To provide practical guidance for controllers, this research undertakes the task of categorising fines into non-compliance groups based on real-world challenges faced by organisations. This process involved the creation of a table of TOMs applicable to specific scenarios,¹⁵⁴ which could be integrated into the DPPA. By categorising fines, an attempt will be made to

a Multimodal Verification System’, 2008 Annual Computer Security Applications Conference (ACSAC) (2008). (with relevance to the study of biometric authentication). Martin Horák, Václav Stupka and Martin Husák, ‘GDPR Compliance in Cybersecurity Software: A Case Study of DPIA in Information Sharing Platform’, *Proceedings of the 14th International Conference on availability, reliability and security* (ACM 2019). (with relevance to the study of PbDD in the context of cyber security).

¹⁵² A variety of computational techniques were employed to manipulate pre-existing statistical data, specifically data cleaning and pre-processing, data visualisation, statistical modelling, and machine learning.

¹⁵³ A major issue of PbDD implementation is identified, e.g., by allocating the percentage of fines issued by supervisory authorities to a failure to implement technical and organisational measures.

¹⁵⁴ Please see Table 5 for a list of GDPR Articles requiring the adoption of a PbDD measure.

identify the specific Articles in the Regulation that mandate the implementation of TOMs or require action on the part of the controller.

It is important to note that while the categorisation process provided a framework for identifying common non-compliance issues, the specific measures required to achieve compliance may vary depending on the context of the processing activities. Therefore, the measures presented in the DPPA should be viewed as a starting point for controllers to develop a comprehensive strategy for GDPR compliance. Additionally, it is worth noting that the measures indicated in the DPPA may need to be updated periodically to reflect changes in the regulatory landscape and technological developments.

To achieve its research objectives, this study employs a mixed-methods research methodology that included the collection and analysis of both quantitative and qualitative data. The quantitative data was obtained from sources such as EU supervisory authorities, CMS Enforcement Tracker, Statista, and Noyb, and was analysed using statistical methods to identify patterns and relationships.

The qualitative data, on the other hand, was obtained from an examination of relevant case law and legal, technology, and information security literature, which served to provide context and delimit the research parameters.

Through this approach, the study aimed to achieve a comprehensive and nuanced understanding of the research topic. To augment the research process, a correlation analysis was conducted, utilising the well-established Braun and Clarke thematic

framework.^{155,156} This analysis was undertaken by scrutinising a dataset consisting of decisions made by the EU supervisory authorities between the period of May 2018 (when the GDPR was implemented) and January 2023. Specifically, the analysis was focused on the GDPR Articles that pertain to the implementation of PbDD, which were subsequently aggregated into pre-determined themes, as is illustrated in Annex 2.

The quantitative (statistical) data was also subjected to qualitative interpretations.¹⁵⁷ This interpretive approach aimed to establish a connection between each theme and the hypotheses included in the scientific research method to assess their validity. The results of this analysis enabled the identification of appropriate measures to rectify, or at least mitigate, the violations that led to the levying of fines, which were subsequently incorporated into the DPPA. Moreover, the adoption of both quantitative and qualitative data analysis techniques has facilitated a more thorough comprehension of the complexities associated with the implementation of PbDD. This integrated approach has further facilitated the identification of the practical obstacles that organisations currently face when striving to comply with the GDPR.

¹⁵⁵ Virginia Braun and Victoria Clarke, 'Using Thematic Analysis in Psychology' (2006) 3 *Qualitative Research in Psychology* 77.

¹⁵⁶ The Braun and Clarke thematic framework is a qualitative data analysis approach that involves identifying and organising patterns, themes, and categories within qualitative data. It comprises several key steps, namely, familiarisation with the data, generating initial codes, searching for themes, reviewing, refining and naming themes, creating a thematic map and writing the outcomes.

¹⁵⁷ For a discussion on qualitative interpretations of quantitative data see, Saul McLeod, 'What's the Difference between Qualitative and Quantitative Research?' (*Simply Psychology*, 2019) <<https://www.simplypsychology.org/qualitative-quantitative.html>>.

The following software tools were utilised in my research:

REDCap

Study data were collected and managed using REDCap electronic data capture tools hosted at University of Reading.^{158,159} REDCap (Research Electronic Data Capture) is the University's secure, web-based system designed to support data capture for research studies, providing 1) an intuitive interface for validated data capture; 2) audit trails for tracking data manipulation and export procedures; 3) automated export procedures for seamless data downloads to common statistical packages; and 4) procedures for data integration and interoperability with external sources.

Tableau Software

The raw data for this research project was extracted from REDCap using the Web Data Connector and subjected to a rigorous cleansing and analysis process in Tableau. The data underwent segmentation into various subsets¹⁶⁰ and was analysed over a span of 57 months.

To explore the relationships between two or more quantitative variables, a correlation analysis is conducted also in Tableau. For example, as the fines categorized under *{Art_32}* increased, so did *{violation_1}* in a systematic manner. With an adequate

¹⁵⁸ PA Harris, R Taylor, R Thielke, J Payne, N Gonzalez, JG. Conde, Research electronic data capture (REDCap) – A metadata-driven methodology and workflow process for providing translational research informatics support, *J Biomed Inform.* 2009 Apr;42(2):377-81.

¹⁵⁹ PA Harris, R Taylor, BL Minor, V Elliott, M Fernandez, L O'Neal, L McLeod, G Delacqua, F Delacqua, J Kirby, SN Duda, REDCap Consortium, The REDCap consortium: Building an international community of software partners, *J Biomed Inform.* 2019 May 9 [doi: 10.1016/j.jbi.2019.103208].

¹⁶⁰ Subsets included in the method: Country, Supervisory authority, Date of issue, Amount, Responsibility (Controller/Processor), Economic Sector, Violated Article, Violation Type, URL to decision.

amount of data, it was possible to draw meaningful conclusions regarding the importance of the violation [*Insufficient TOMs to ensure information security*] in relation to the secondary variable {violation_1} which corresponded to {*non-implementation or defective implementation of PbDD*}.¹⁶¹

Moreover, the software's visualisation capabilities allowed me to create visual representations of the data that facilitated the identification of patterns and trends that might have gone unnoticed through purely numerical analysis.

By leveraging the correlation method in Tableau, I was able to identify the patterns and interrelationships present in the data, leading to meaningful and actionable conclusions. Overall, Tableau's comprehensive suite of tools and features played a pivotal role in the successful completion of this research project, enabling me to derive valuable insights from the data.

Data analysis results

The following results are of significance for the development of the DPPA:

As of January 2023, the Enforcement Tracker has recorded a total of 1,551 fines. The total amount of the fines exceeds €2.777 billion. Over the 2018-2023 period, the average fine across all countries was circa €1,889,781.

Notably, the highest GDPR fine ever imposed to date amounts to €746 million and was issued by the supervisory authority in Luxembourg in July 2021 for non-compliance with general data processing principles. This significant fine was preceded by a fine of approximately €405 million imposed by the Irish supervisory authority and a fine of

¹⁶¹ See Annex 3 for the table of variables used in this research.

approximately €90 million levied by the French supervisory authority in December 2021. It is noteworthy that in the summer of 2021, the total amount of one billion euros in GDPR fines was exceeded for the first time, indicating the increasing enforcement of GDPR.

Non-compliance with general data processing principles, averaging €1.651 billion, tops the list of GDPR violations in terms of both the number of fines issued and the average sum of fines. Fines levied for insufficient legal basis for data processing averaged €450 million. The next row in the table is occupied by insufficient TOMs to ensure information security, averaging €375 million followed by insufficient fulfilment of data subject's rights, averaging €277 million.

The DPPA framework provides organisations with a practical approach to meeting GDPR requirements by mapping GDPR Articles to appropriate TOMs. In this study, I aimed to identify the most relevant GDPR Articles for deeper investigation and implementation of PbDD measures. To achieve this, I examine various decisions issued by EU supervisory authorities and classified the Articles that appeared most frequently, cross-referencing them with the type of violation. This analysis generated valuable insights into areas that require greater attention and prioritisation of PbDD efforts. The reasoning behind this approach is based on the notion that by focusing on the Articles that are most frequently cited in supervisory authority decisions and that have attracted the heaviest fines, controllers can address the weaknesses in their own organisation's implementation approach and prevent future penalties.

The statistical data presented herewith is of significant relevance, as it pertains to the fines that have been issued by the supervisory authorities within the European Union and United Kingdom. The fines are in reference to the provisions of GDPR Article, and the data covers the period spanning from May 2018 to January 2023.

It is worth emphasising that a single supervisory authority decision may address multiple violations, which can lead to multiple GDPR Articles being addressed (correlated) within that decision. Hence, a fine may correspond to two or more themes, depending on the number of violations that were taken into account within that decision. To establish the correlation between fines and the themes to which they relate, the study employed a methodology that is illustrated in the correlation table, presented in Annex 2.

The findings of this study are presented in a clear and concise manner. Specifically, Figure 3 displays the frequency with which the GDPR Articles are referenced in the decisions made by EU supervisory authorities.

Annex 1.A provides a precise accounting of the number of occurrences of these references within the sample used for this research.

Given the significance of understanding the factors that impact the imposition of fines under the GDPR, the subsequent section will describe the implementation of correlational methodology to explore potential relationships between different variables. By scrutinising the statistical data on fines, alongside additional contextual information including the nature of the violations and the implicated organisations, this correlational approach aims to unveil patterns and associations that can offer valuable insights into the enforcement practices and outcomes associated with the GDPR.

2.4. Correlational methodology

Correlational research represents a non-experimental research method that involves the measurement of two variables, offering insights into the statistical relationship between them, without the researcher exerting control over either variable. In the following

illustration, two variables are scrutinised, namely (i) the nature of the GDPR breach, and (ii) the frequency of its occurrence. As ‘research for causal explanations must first clarify what effects need causal explanation and then try to discover what their causes are,’¹⁶² the application of a correlation method enabled the generation of derived data to provide further insight into the hypotheses presented for investigation. This data helped in understanding not only the frequency and trends of specific violations, such as the number of fines imposed and their variation over a defined period of time, but also to comprehend and interpret the cause of such violations, which may relate to issues with the law or its application. By employing this correlation method, a deeper understanding of the causal relationships between violations and the relevant GDPR requirements or obligations was achieved.

The correlation coefficient is a crucial statistical tool utilised in diverse fields such as social science, economics, and healthcare, to determine the association between two variables. The coefficient quantifies the degree of the relationship between the two variables and measures how changes in one variable affect the other. The range of values for the correlation coefficient varies from -1 to +1, where values closer to +1 signify a strong positive correlation between the variables, indicating that they increase or decrease in tandem. On the other hand, values closer to -1 suggest a strong negative correlation, which means that the variables move in opposite directions. A correlation coefficient close to zero, indicates no discernible relationship between the two variables, suggesting that any variation in one variable has no effect on the other. The interpretation of the correlation

¹⁶² Merton S Krause, ‘Associational versus Correlational Research Study Design and Data Analysis’ (2018) 52 *Quality and Quantity* 2691.

coefficient is critical in making informed decisions in various domains, ranging from business operations to public policy. The study integrates correlational analysis as a fundamental statistical tool to investigate the nature and existence of the correlation between the number of fines levied by the EU/UK supervisory authorities and issues associated with the application of PbDD. The primary objective is to ascertain the nature of the correlation between the two variables, namely whether a positive correlation exists, indicating that as the number of fines increases, issues related to PbDD also increase (i.e., the two variables change in the same direction); a negative correlation, implying that as the number of fines increases, issues related to PbDD decrease (i.e., the two variables change in opposite directions); or a zero correlation, signifying that the number of fines issued by EU/UK supervisory authorities is unrelated to the application of PbDD. The integration of correlational analysis in this study offers a comprehensive understanding of the relationship between the variables, thereby allowing for more informed decisions in addressing issues related to PbDD.

The quantitative (statistical) analysis of the data was thus conducted with the specific objective of determining the existence of a relationship between two variables, as opposed to establishing a causal relationship between them. The data collected was systematically arranged and managed using the University of Reading's 'RedCap' database, and subsequently, refined and structured through an advanced visualisation tool, Tableau. Specifically, the following information was meticulously organised: (i) the country where the fine was issued; (ii) the date of issuance; (iii) the amount; (iv) the name and business sector of the controller or processor; (v) the specific type of violation (e.g. pertaining to non-compliance with data processing principles); (vi) the Articles of GDPR contravened; and (vii) a hyperlink to the supervisory authority's decision.

The dataset encompasses all (published) GDPR fines imposed in the EU/UK between May 2018 and January 2023. Annex 1 provides a comprehensive visualisation of the GDPR fine statistics utilised in this study, while Annex 3 contains a list of supervisory authorities, and Annex 4 contains the URLs of the corresponding decisions.

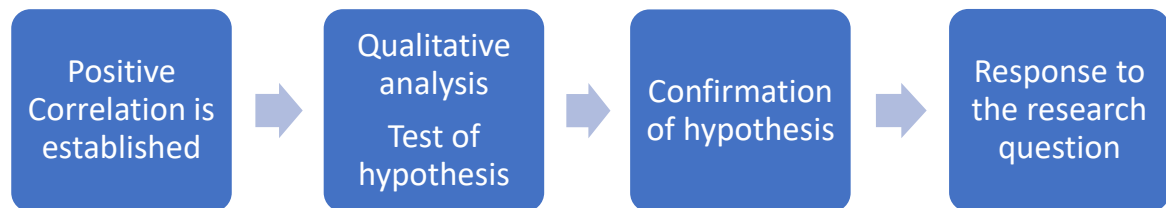


Figure 3 - Correlational methodology

The study is centred on examining the enforcement of the GDPR by the EU/UK supervisory authorities, with a focus on investigating the correlation between the number of fines and penalties imposed and issues related to the application of PbDD. To ensure a representative sample, a targeted sampling strategy was adopted, selecting a predetermined number of fines and penalties levied by the EU/UK supervisory authorities. The chosen sample size of over 100 was deemed sufficient to provide the study with the necessary statistical power to detect meaningful correlations. The selected fines and penalties were then recorded in self-completion spreadsheets and analysed using Tableau, a powerful data visualisation and exploration tool. Correlational research methods were employed to establish the presence and strength of relationships between the two variables, enabling a comprehensive understanding of the effectiveness of GDPR enforcement and highlighting areas that require improvement. This approach provides an evidence-based foundation for developing strategies and policies that enhance GDPR compliance, thereby safeguarding the privacy rights of individuals.

Qualitative analysis was employed to establish the causal relationship between the two variables under consideration.¹⁶³ This approach involved an in-depth examination of several factors, including: (a) the content of the supervisory authority decision (e.g., ‘failure to take appropriate TOMs to ensure the ability to ensure the continuity of confidentiality of processing services, failure to test and assess the effectiveness of TOMs to ensure the security of personal data’); (b) the aspects of the law considered (e.g., ‘insufficient TOMs to ensure information security’ refers to a violation of Art. 25 GDPR (PbDD) and Art. 32 GDPR (security of processing), or ‘entrusting the processing of personal data without the contractual obligation of the processor to process personal data solely on the documented instructions of the controller refers to a violation of Article 28(3) of GDPR); (c) business practices involved in the data processing activity leading to the violation (e.g., managing a copy of the database of the training platform of the National School of Judiciary and Public Prosecution); and (d) the technical or technological context in which the violation occurred (e.g., personal data breach).¹⁶⁴

¹⁶³ The use of qualitative data to explore quantitative findings.

¹⁶⁴ For coherence of thought the examples provided relate to the fine levied by the Polish Supervisory authority to the National School of Judiciary and Public Prosecution (Decision DKN.5130.2024.2020) in the amount of PLN 100 000 (one hundred thousand zlotys), on 11 February 2021. This specific example was included in Annex 2 to illustrate the correlation analysis process. <<https://www.uodo.gov.pl/decyzje/DKN.5130.2024.2020>>.

2.5. Steps carried out in the analytical process

My primary objective was to ascertain the underlying motivators prompting the violations resulting in penalties, specifically discerning the actions or inactions undertaken by organisations that may lead to infringement of the GDPR.

The first step in my analysis was thus to identify patterns in the data relevant to the main topics of the study: (a) the harmonisation and integration of the legal requirements into the businesses' practices and operations, (b) the complexities surrounding PbDD, and (c) the constraints towards the realisation of PbDD. Secondly, I created correlational tables for the dataset of fines as described above. The third step of the analysis involved aggregating the fines and developing thematic statements to further examine the patterns observed in the data. The themes used for the data analysis were carefully selected based on their relevance to the research objectives and the significant legal requirements outlined in the GDPR. The identified themes included non-compliance with general data processing principles, insufficient legal basis for data processing, inadequate TOMs to ensure information security, insufficient fulfilment of information obligations, inadequate fulfilment of data subjects' rights, inadequate fulfilment of data breach notification obligations, insufficient data processing agreements, insufficient involvement of the data protection officer, insufficient cooperation with the supervisory authority, and insufficient fulfilment of data subject rights. The adoption of these themes enabled the identification of common patterns and underlying factors that contributed to GDPR violations, thereby enabling the development of targeted strategies for improving GDPR compliance and data protection practices.

Finally, the results obtained from the correlation tables were synthesised to comprehensively address the research question, by asking: What is the underlying message conveyed by the themes? Are there discernible links between the identified themes and the implementation of PbDD?

By adopting this approach, the study was able to generate insights that shed light on the challenges and issues associated with the implementation of PbDD and provided a more comprehensive understanding of the factors that contribute to GDPR violations.

To refine and direct the focus of this analysis towards addressing the research question effectively, several additional key inquiries were explored. These inquiries included investigating the most frequent GDPR violations that result in fines, exploring any potential links between these violations and the ineffective implementation of GDPR requirements, particularly PbDD, in business operations. Furthermore, the study also examined whether there were discernible patterns of non-compliance over time, and whether these violations arose from inadequate data processing practices, including information security, or a lack of comprehension of the Regulation from controllers.

Furthermore, an inquiry was undertaken to ascertain whether the difficulties highlighted in the literature regarding the integration of data protection principles and GDPR requirements into business systems, processes, and operations have a role to play in contributing to these violations. The insights gleaned from addressing these questions enabled the validation of the response to the overarching research question. In other words, by analysing the quantitative data based on qualitative interpretations, I was able to identify the main issues beyond the practical application of PbDD, and more generally, beyond the practical application of GDPR.

The analysis conducted on the fines issued by supervisory authorities within the European Union has revealed a clear pattern in terms of the GDPR provisions that attract a higher number of penalties. Specifically, the GDPR provisions that pertain to principles relating to the processing of personal data, security of processing, information obligations, consent, and data subject rights have been the focal point of enforcement action. To facilitate the development of the DPPA methodology, the aforementioned sets of fines have been grouped into wider themes, including non-compliance with general data processing principles, insufficient legal basis for data processing, insufficient TOMs to ensure information security, insufficient fulfilment of information obligations, and insufficient fulfilment of data subject rights. The resulting findings are visually presented in the following charts.

Figure 4 presents a visual representation of the five most significant themes, based on the total number of fines issued by supervisory authorities within the EU and UK. This information carries significant weight, as it highlights the most prevalent areas of regulatory non-compliance in the context of GDPR enforcement.

Figure 5 offers a visual representation of the five most consequential themes, based on the total sum of fines issued by supervisory authorities within the EU and UK. This information is highly pertinent as it provides insights into the most common areas of regulatory non-compliance that attract the highest value of fines in the context of GDPR enforcement.

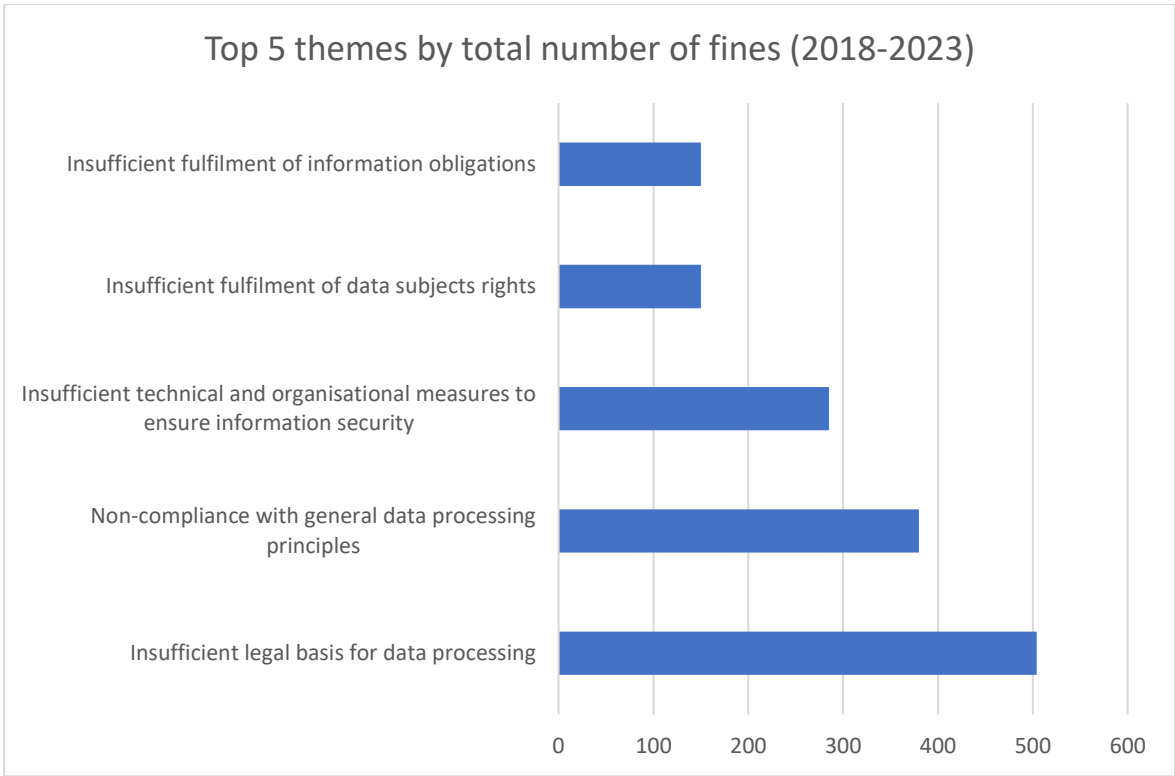


Figure 4 - Top 5 themes by total number of fines (2018-2023)

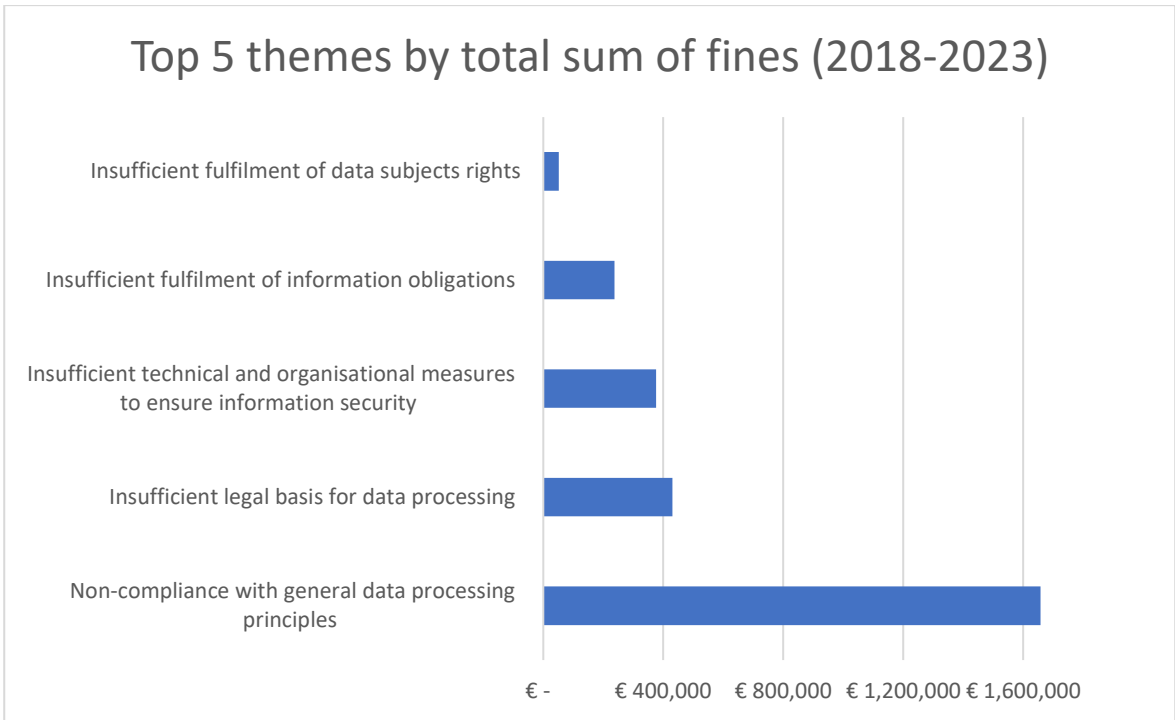


Figure 5 - Top 5 themes by total sum of fines (2018-2023)

Chapter 3 – Theoretical frameworks shaping the DPPA

Introductory notes

The interplay between ambiguous legal requirements on one hand, technological advancements, business interests, and the protection of individual rights on the other, constitutes a critical cornerstone of the proposed Data Protection Principles Approach (DPPA). This chapter aims to address this perspective by exploring and integrating the theoretical frameworks that underpin the DPPA, delving into pertinent theoretical constructs. By emphasising the conceptual roots of the DPPA, I hope to assist the reader in better comprehending and supporting the proposed framework.

The legal concepts presented, with a highlight on legal certainty,¹⁶⁵ which serve as a foundational principle to the DPPA framework, will be subject to further exploration throughout the thesis. The concept of legal certainty pertains, inter alia, to the

¹⁶⁵ The principle of legal certainty has deep roots in the development of the EU and its legal system. While the term "legal certainty" may not have always been explicitly used, the concept has been integral to the evolution of EU law and institutions. The principle of legal certainty finds its foundation in the Treaties establishing the European Communities, which later evolved into the Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU). These treaties lay down the legal framework for the EU and establish principles such as the supremacy of EU law, direct effect, and the obligation of member states to ensure compliance with EU law. The ECJ, through its case law, has played a crucial role in shaping the principle of legal certainty within the EU legal system. Landmark cases such as *Van Gend en Loos* (Case 26/62), *Costa v ENEL* (Case 6/64), and *Internationale Handelsgesellschaft mbH v Einfuhr- und Vorratsstelle für Getreide und Futtermittel* (Case 11/70) have established fundamental principles like the supremacy of EU law, direct effect, and proportionality, which contribute to legal certainty by providing clarity and predictability in the application of EU law. Over time, the principle of legal certainty has been codified in various EU legal instruments and incorporated into the institutional framework of the EU. For example, the Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU) explicitly recognise the principle of legal certainty as a fundamental value of the EU. Additionally, the establishment of institutions such as the European Commission, the European Parliament, and the European Court of Justice (ECJ) further strengthens legal certainty by ensuring the consistent application and interpretation of EU law. Legal certainty is essential for ensuring the rule of law, protecting fundamental rights, promoting trust in the EU legal system and is deeply embedded in the legal and institutional framework of the European Union. It serves as a foundational principle that underpins the coherence, predictability, and effectiveness of EU law and institutions.

predictability¹⁶⁶ and coherence¹⁶⁷ of legal rules, which are essential for ensuring the enforceability and compliance of data protection regulations.

These principles are embedded in EU law and justify the creation of the DPPA as a tool that contributes to ensuring certainty in the application of legal requirements to practical scenarios and business activities by providing a structured framework for implementing and interpreting data protection regulations. Importantly, the DPPA establishes clear guidelines and principles that organisations can follow to achieve compliance with legal standards, thus reducing ambiguity and uncertainty in their data processing practices. Moreover, the DPPA helps bridge the gap between abstract legal principles and their practical implementation by offering specific guidelines and best practices tailored to various industries and business contexts. By doing so, it enhances the predictability of outcomes and ensures consistent application of data protection rules across different scenarios.¹⁶⁸

¹⁶⁶ See, Isabel Lifante-Vidal, 'Is Legal Certainty a Formal Value?' (2020) 11 *Jurisprudence* 456. 'First of all, a legal system (or, better still, a certain sector of a legal system) will be more predictable the more things it allows us to predict and the more accurately it does so. Thus, determining the degree of predictability in this first dimension will depend on whether it is possible to know precisely beforehand which behaviours are prohibited, mandatory or permitted by the law and the legal consequences established for certain behaviours (or for certain situations), as well as the conditions under which those consequences, which may be procedural, temporal, economic, or of any other nature, may be generated.'

¹⁶⁷ *ibid.* 'The same reasons that make it impossible to know the law completely also confer particular importance on a factor that generates legal certainty: the regulatory coherence offered by legal principles.' ; 'However, these dimensions are, in turn, complex, and what, for example, generates predictability for one kind of subject (e.g., businesses) may destroy it for other kinds of subject (workers, consumers), or a very precise wording (high content formality) may generate incoherence with other norms, making it necessary to interpret it in a less literal way (reducing interpretive formality).'

¹⁶⁸ Overall, legal certainty justifies the creation of the DPPA by providing a solid theoretical foundation for achieving clarity, predictability, and consistency in data protection regulations and practices. By aligning with the principles of legal certainty, the DPPA offers a practical framework for organisations to navigate the complexities of data protection compliance effectively.

Furthermore, the DPPA serves as a mechanism for promoting transparency¹⁶⁹ and accountability¹⁷⁰ in data processing activities.¹⁷¹ By delineating clear responsibilities and obligations for data controllers and processors, it fosters trust among stakeholders and minimises the risk of non-compliance. It is recognised that while the GDPR's principle of transparency, on its own, does not establish any form of legal presumption – i.e., it will not inherently render a technology trustworthy - it is widely acknowledged that a lack of transparency often characterises emerging technologies, particularly in terms of their potential risks and impacts, a problem that the DPPA also aims to mitigate.¹⁷²

It is also recognised that the practical application of the GDPR is determined by two main streams devised by the European legislator. Firstly, it involves the strengthening and standardisation of data protection rules within the EU.¹⁷³ Secondly, it encompasses the broadening of the territorial scope of such protection, introducing an additional layer of

¹⁶⁹ For a discussion on the principle of transparency in the GDPR, see, e.g., Bernhard Ganglmair, Julia Krämer and Jacopo Gambato, 'Regulatory Compliance with Limited Enforceability: Evidence from Privacy Policies' <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4600876>. 'The General Data Protection Regulation (GDPR) contains a set of cumulative principles that are a prerequisite for any form of processing of personal data and ensure their lawful processing. One of these principles is transparency (in Art. 5(1) lit. a GDPR) which requires any information concerning the processing of personal data to be easily accessible and understandable. The underlying aim behind this principle is that consumers need to understand the information provided to them to be able to make informed decisions about who and how their data are processed.'

¹⁷⁰ For a discussion on the principle of accountability in the GDPR, see, e.g., *Managing Privacy through Accountability* (Daniel Guagnin, Leon Hempel, Carla Ilten, Inga Kroener, Daniel Neyland, Hector Postigo, Palgrave Macmillan London) <<https://doi.org/10.1057/9781137032225>>.

¹⁷¹ Both principles of transparency and accountability will be the subject of deeper discussion in Chapter 4.

¹⁷² Please See, Paul de Hert and Guillermo Lazcoz, 'When GDPR-Principles Blind Each Other: Accountability, Not Transparency, at the Heart of Algorithmic Governance' (2022) 8 *European data protection law review* (Internet) 31.

¹⁷³ While the GDPR provides a unified framework for data protection within the EU, challenges arise in ensuring consistent enforcement and interpretation of these rules across different member states. This has led to discrepancies in implementation and enforcement, affecting the effectiveness of data protection measures—an issue that the DPPA also aims to address.

safeguarding for personal data transferred to third countries.¹⁷⁴ This compels 'countries with lax Regulations to tighten them as EC Regulations are developed.'¹⁷⁵ These streams are also incorporated into the proposed DPPA, with specific mechanisms addressing 'the data protection principles' and 'data subject rights' forming its core. By harmonising data protection practices across jurisdictions against established legal principles outlined in the GDPR, it helps organisations navigate the complexities of global data governance while maintaining compliance with applicable regulations. This harmonisation is crucial in today's interconnected world where data flows freely across borders.

The DPPA provides thus a common framework that organisations can adopt to ensure that their data protection practices meet the standards set forth by various regulatory bodies. This not only simplifies the compliance process but also enhances trust and confidence among citizens, knowing that their data is being handled in accordance with internationally recognised standards, such as the globally recognised ISO 27001.¹⁷⁶

¹⁷⁴ One significant issue arising from the broadening of the territorial scope of the GDPR is ensuring that personal data transferred to third countries receives an adequate level of protection equivalent to that provided within the EU. Following the Schrems II ruling, this involves assessing the data protection standards and practices in the recipient country to ensure compliance with GDPR requirements. Issues such as data breaches, government surveillance, and lack of effective legal remedies in third countries can pose challenges to ensuring adequate protection for transferred data. Another emerging issue is the legal mechanisms for transferring data to third countries, such as Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs). Recent legal developments, such as the Schrems II ruling by the CJEU, have raised concerns about the validity and effectiveness of these mechanisms in ensuring adequate protection for transferred data, particularly in light of government surveillance practices in some third countries. Moreover, it is claimed that the global jurisdictional claim in Article 3(2) of the GDPR is limited by its intrinsic difficulty to be enforced. For a discussion on the extra-territorial enforcement of the GDPR, see, e.g., Benjamin Greze, 'The Extra-Territorial Enforcement of the GDPR: A Genuine Issue and the Quest for Alternatives' (2019) 9 *International Data Privacy Law* 109.

¹⁷⁵ Ernest Braun and David Wield, 'Regulation as a Means for the Social Control of Technology' (1994) 6 *Technology Analysis & Strategic Management* 259.

¹⁷⁶ Isabel Maria Lopes, Teresa Guarda and Pedro Oliveira, 'Implementation of ISO 27001 Standards as GDPR Compliance Facilitator' (2019) 4 *Journal of information systems engineering & management* <<https://go.exlibris.link/g0s9scjZ>>.

Moreover, the alignment with GDPR principles ensures that organisations are equipped to address the specific requirements and challenges associated with international data transfers, such as data subject rights, lawful basis for processing, and security measures. By adhering to these principles, organisations can mitigate the risks associated with cross-border data transfers and demonstrate their commitment to protecting personal data regardless of geographical boundaries. Therefore, the harmonisation facilitated by the DPPA framework promotes consistency and coherence in data protection practices, reducing the regulatory burden on organisations operating in multiple jurisdictions and contributing to legal certainty. This not only streamlines compliance efforts but also fosters a level playing field for businesses, ensuring fair competition in the global marketplace.

Other concepts presented in this chapter, while not necessarily warranting a detailed theoretical underpinning, will function as an engine for the practical application of the DPPA. This is evident in the reference to the Collingridge Dilemma, named after David Collingridge,¹⁷⁷ which pertains to the difficulty of predicting and controlling the societal impacts of technology, particularly in its early stages of development. This dilemma directly affects legislators' capability to enact precise laws aimed at regulating technological aspects of data protection, thereby limiting the achievement of legal certainty.¹⁷⁸

¹⁷⁷ For contextualisation, See, e.g., Audley Genus and Andy Stirling, 'Collingridge and the Dilemma of Control: Towards Responsible and Accountable Innovation' (2018) 47 Research Policy 61. See also, Jenifer A Buckley, Paul B Thompson and Kyle Powys Whyte, 'Collingridge's Dilemma and the Early Ethical Assessment of Emerging Technology: The Case of Nanotechnology Enabled Biosensors' (2017) 48 Technology in Society 54.

¹⁷⁸ On one hand, legislators must balance the need to address emerging threats to data privacy and security with the imperative to foster innovation and technological advancement. On the other hand, they face the challenge of crafting precise and effective laws without complete knowledge of the future implications of evolving technologies. In the context of data protection, the Collingridge Dilemma directly affects legislators' capability to enact precise laws aimed at regulating technological aspects such as data collection, processing, and storage. The rapidly evolving nature of technology, coupled with its unpredictable societal impacts,

Within the context of this thesis, a crucial aspect of the practical application of PbDD that the DPPA aspires to effectively address is the alignment of legal requirements imposed by the GDPR with the challenges presented by emerging technologies. These include the Internet of Things (IoT), Blockchain, and Artificial Intelligence (AI), sometimes referred to as Big Data Processing, or the “three V’s processing” (volume, velocity, and variety).¹⁷⁹ These technologies are also associated with issues of “Data Power,” as Lynskey suggests that it is ‘exercised by technology companies occupying strategic positions in the digital ecosystem.’¹⁸⁰

Notably, the DPPA endeavours to navigate and integrate the complexities associated with these cutting-edge technologies into the compliance framework. The ambition is also to harmonise the regulatory framework with the dynamic landscape of these technologies, ensuring that data protection principles remain robust and adaptable in the face of evolving digital paradigms. In this regard, it is crucial to emphasise the perspectives of several scholars who share my own beliefs and argue that the underpinnings of the AI revolution and corresponding legislation are yet to be fully unveiled. This is particularly pertinent regarding how to safeguard the vast amount of data shared and processed by these technologies.¹⁸¹

complicates the task of drafting legislation that can effectively safeguard individuals' privacy rights while allowing for innovation and economic growth.

¹⁷⁹ Omer Tene, ‘Privacy in the Age of Big Data: A Time for Big Decisions’ <https://www.researchgate.net/publication/259892061_Privacy_in_the_Age_of_Big_Data_A_Time_for_Big_Decisions/>.

¹⁸⁰ Orla Lynskey, ‘Grappling with “Data Power”: Normative Nudges from Data Protection and Privacy’ (2019) 20 *Theoretical inquiries in law* 189.

¹⁸¹ Ben Rossi, ‘Why Businesses Should Be More Concerned with G DPR and AI than Brexit’ (*Information Age*, 21 March 2017) <<https://www.information-age.com/businesses-concerned-gdpr-ai-brexite-4910/>>.

Braun and Wield argue that technology policy encompasses more than just regulation; it also involves various measures to support technology development.¹⁸² I fully agree with this perspective, which is why I carefully considered the Collingridge Dilemma when developing the DPPA, especially in the context of conducting Data Protection Impact Assessments (DPIAs).¹⁸³ This dilemma highlights the challenge of controlling and regulating emerging technologies,¹⁸⁴ with significant implications for how we apply Articles 24, 25, and 32 of the GDPR within the framework of the DPPA, namely, during the later stages of data processing.¹⁸⁵

The Collingridge Dilemma suggests that there is a paradoxical relationship between information and control: when we have little information about a technology's potential consequences, it is challenging to control it effectively, and by the time we have sufficient information, control may be more difficult due to the established nature of the technology.¹⁸⁶ This highlights the importance of adapting and responding to technological advancements and regulations in data protection. It prompts questions about the legal

¹⁸² Braun and Wield (n 174).

¹⁸³ Article 35 of the GDPR does not explicitly define the Data Protection Impact Assessment (DPIA). However, the guidelines on DPIA provided by the Article 29 Working Party offer the following definition: "A DPIA is a process designed to describe the processing, assess its necessity and proportionality, and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data."

¹⁸⁴ For contextualisation, See, e.g., Genus and Stirling (n 176). The dilemma is characterised by a dual problem related to the control of technology at different stages of its development, which the legislator seems unable to anticipate and predict its impacts on the legal system. For example, in the early stages of technological development, particularly when data protection by design is meant to be applied, and when a technology is not yet fully mature or widely adopted, it is challenging to accurately predict its potential impacts on society. It is argued that at this stage, attempts to control the technology may be premature or ineffective due to insufficient information about its long-term consequences.

¹⁸⁵ Once a technology is well-established and its societal impacts become clearer, it may already be deeply embedded in the social and economic fabric. Therefore, attempts to control or modify the technology at this point may be challenging due to entrenched interests, dependencies, and resistance to change. These factors may make the application of TOMs designed to address data protection by default even more difficult.

¹⁸⁶ For a discussion on the Collingridge's dilemma of control and on the cross disciplinary interconnection of law and IT, namely, how digital dimensions and technology are addressed in the law, See e.g., Mirko Pečarič and others, 'Digitalisation and Law: The More Things Change – The More They Stay the Same' (2022) 20 *Lex Localis* 411.

certainty provided by the GDPR.¹⁸⁷ Moreover, it highlights the inherent difficulties faced by legislators, especially in the realm of new technology governed by the GDPR. The evolving nature of technology necessitates a dynamic and adaptive regulatory framework capable of navigating challenges posed by both early-stage uncertainties and late-stage entrenched practices. Continuous review and updates to legislation, along with collaboration between regulators, practitioners, engineers, businesses and other stakeholders, are crucial to addressing these complexities. In this respect, the DPPA adopts Collingridge's view that 'keeping future options open facilitates the social control of technology by enhancing the flexibility of decisions.'¹⁸⁸

The GDPR was enacted with the intention of providing individuals with control over their personal data. However, in practical terms, particularly in the early stages of technological development, legislators may struggle to foresee all possible uses and misuses of data. This can make it challenging to formulate specific and comprehensive regulations, as well as to anticipate appropriate TOMs to be applied to the use of personal data. This, in turn, opens the door to legal uncertainty.

On the other hand, as technologies mature, their impact on privacy and data protection becomes clearer, and devising TOMs may become easier. I contend that the GDPR needs adjustments to effectively address new challenges that were not initially anticipated. This gap is largely filled by the DPPA. The DPPA provides tools for businesses by introducing stringent TOMs for data controllers and processors. These include the

¹⁸⁷ Li and others (n 151).

¹⁸⁸ D. Collingridge, cited in Genus and Stirling (n 176).

collective DPIA and ongoing revision of interdependencies between various technologies to address potential gaps in regulatory coverage, as we will now explore.

3.1. The strategy towards risk and the concept of "Collective DPIA" within the context of the DPPA

A Data Protection Impact Assessment (DPIA) is a process designed to systematically analyse and assess the potential risks that a particular data processing activity may pose to individuals' privacy and data protection.¹⁸⁹ A collective DPIA involves collaboration among different stakeholders, such as data controllers, processors, and possibly regulators, to collectively evaluate the impact of a specific data processing initiative.¹⁹⁰ The use of a collective DPIA is based on several key premises; In the early stages of technological development, a collective DPIA allows for a thorough examination of the potential risks associated with a new technology or data processing activity. By identifying risks early on, stakeholders can proactively address privacy concerns and implement measures to mitigate these risks before the technology becomes entrenched. By implementing measures to mitigate risks at the outset, potential negative impacts on individuals' privacy can be minimised, promoting responsible data processing practices. Moreover, the collaborative nature of a collective DPIA brings together diverse perspectives, including those of data protection experts, engineers, legal professionals, and other relevant

¹⁸⁹ For a discussion on DPIA under GDPR, See, e.g., Marija Boban, 'GDPR AND DATA PROTECTION IMPACT ASSESSMENT (DPIA)', *Economic and Social Development: Book of Proceedings* (Varazdin Development and Entrepreneurship Agency (VADEA) 2020) <<https://go.exlibris.link/9ZqTv5Yh>>.

¹⁹⁰ The concept of a collective DPIA, as suggested in the DPPA, serves various purposes, including identifying and mitigating risks posed to the processing of personal data. This approach is particularly relevant in addressing challenges such as the Collingridge Dilemma and the lack of legal certainty.

stakeholders. This diversity of expertise helps in capturing a more holistic view of the potential risks and benefits associated with the technology. By involving various stakeholders in the DPIA process, critical aspects are less likely to be overlooked, leading to more informed decision-making.¹⁹¹

The Collingridge Dilemma highlights the challenge of adapting regulations and controls as technology evolves, especially within a risk-based approach. The core of risk-based regulation lies in offering a framework to attain a proportionate and adaptable strategy for regulatory enforcement.¹⁹² In this case, a collective DPIA allows stakeholders to continually assess and adapt measures in response to changing circumstances. In terms of risk mitigation, a collective DPIA facilitates collaborative efforts in developing and implementing effective privacy risk mitigation strategies.¹⁹³ Stakeholders can collectively design and enforce TOMs that address the identified risks, fostering a cooperative approach to data protection. Stakeholders can also opt for a risk eradication approach. While risk mitigation seeks to minimise the impact of risks, risk eradication aims to eliminate them entirely by addressing their root causes.

¹⁹¹ However, enforcing collective Data Protection Impact Assessments (DPIAs) poses several challenges for organisations. Coordinating multiple stakeholders with varying priorities and expertise can lead to difficulties in achieving consensus on risk identification and mitigation strategies. Additionally, conducting a collective DPIA requires substantial time, expertise, and financial resources, which may not always be readily available. Regulatory compliance adds another layer of complexity, especially when dealing with differing requirements across jurisdictions. Issues related to data sharing and confidentiality also arise, as sharing sensitive information among stakeholders raises concerns about data security. Establishing protocols to protect confidential information while enabling collaboration is crucial but challenging. Furthermore, defining roles, responsibilities, and decision-making authority among stakeholders is essential for effective risk assessment and mitigation but can be complex.

¹⁹² Milda MACENAITE, 'The "Riskification" of European Data Protection Law through a Two-Fold Shift' (2017) 8 *European journal of risk regulation* 506.

¹⁹³ For an overview of privacy risk mitigation strategies applied to IoT, See, e.g., Anna Lenhart and others, "'You Shouldn't Need to Share Your Data": Perceived Privacy Risks and Mitigation Strategies Among Privacy-Conscious Smart Home Power Users' (2023) 7 *Proc. ACM Hum.-Comput. Interact.* <<https://doi.org/10.1145/3610038>>.

One must note that risk eradication is an organisational prerogative instead of a regulatory requirement. Although the GDPR requires organisations to identify and mitigate risks, it does not advocate a risk eradication avenue. However, it is my belief that this approach might prove extremely helpful, especially when the object of the DPIA is new technologies.¹⁹⁴ Moreover, a collective DPIA fosters transparency in the assessment of risk, contributing to public trust in the technology and the organisations involved. Of course, establishing trust is crucial in addressing data protection compliance, especially when dealing with uncertainties in the early stages of technological development and in the context of technologies such as Blockchain where traditional privacy solutions are not applicable.¹⁹⁵ These technologies lack scope for the application of several concepts, such as the concept of the "data controller," and the implementation of technical measures aiming to ensure the data subject's rights, such as the right to erasure. I will delve into these aspects in more depth later in this thesis.

In summary, a collaborative DPIA within the framework of the DPPA presents a proactive, collaborative, and comprehensive approach to tackling the challenges stemming from the implementation of PbDD and GDPR requirements. This approach is rooted in the concept of "Collaborative Governance" as proposed by Kaminski and Malgieri.¹⁹⁶

This approach is especially pertinent to the challenges highlighted by the Collingridge Dilemma in the context of IoT, AI, and Blockchain, and in addressing the issue

¹⁹⁴ The primary goal of risk mitigation is to reduce the impact or likelihood of a risk, while risk eradication aims to eliminate the risk altogether. Thus, mitigation focuses on managing risks that cannot be entirely eliminated, whereas eradication targets risks that can be completely removed.

¹⁹⁵ Li Peng and others, 'Privacy Preservation in Permissionless Blockchain: A Survey' (2021) 7 *Digital Communications and Networks* 295.

¹⁹⁶ Margot E Kaminski and Gianclaudio Malgieri, 'Multi-Layered Explanations from Algorithmic Impact Assessments in the GDPR', *FAT 2020 - Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency* (2020) <<https://go.exlibris.link/t94NBbLD>>.

of legal clarity within the Regulation. By systematically identifying, assessing, and mitigating risks in a collaborative manner, stakeholders can navigate the complexities of technology development, striking a balance between innovation and effective data protection. Therefore, in my opinion, future revisions of the Regulation should introduce the concept of a "Collective DPIA" as a requirement, particularly when personal data processing involves these new technologies.

3.2. Tackling the operational challenges posed by new technologies

The DPPA provides a method for implementing the core data protection principles in the context of emerging technologies such as IoT, Blockchain, and AI. While it is true that the GDPR has led to more harmonised rules across the single market, and an increasing number of organisations are integrating its concepts into the development of their privacy policies, there is an argument that ensuring the effectiveness of the GDPR in the application of AI and IoT devices remains challenging.¹⁹⁷ This challenge is sometimes attributed to difficulties faced by users of such technology in accessing and erasing their personal data. Additionally, there has been a lack of clear methods for users to provide or withhold consent.¹⁹⁸ Other identified problems include, for example, the notion that these long-term data activities generally heighten identifiability and broaden the scope of harms to which

¹⁹⁷ Varda Mone and CLV Sivakumar, 'An Analysis of the GDPR Compliance Issues Posed by New Emerging Technologies' (2022) 22 *Legal Information Management* 166.

¹⁹⁸ P. Cheng and others, 'Smart Speaker Privacy Control - Acoustic Tagging for Personal Voice Assistants', 2019 *IEEE Security and Privacy Workshops (SPW)* (2019).

individuals are exposed. Key characteristics contributing to these concerns include age, period, and frequency.¹⁹⁹

Hence, in relation to IoT, the DPPA approach is grounded in the implementation of TOMs, as outlined in Chapters 8 and 9 of this thesis. The emphasis is on two crucial data protection principles: Data minimisation and Purpose limitation.²⁰⁰ Regarding data minimisation, IoT devices often accumulate extensive amounts of data. The DPPA, aligned with the data minimisation principle, advocates for the collection of only necessary data. This approach aims to reduce the risk of excessive and unnecessary data processing. In addressing Purpose limitation, the DPPA underscores the importance of clearly defining and communicating the purposes for which IoT data is collected and for how long is retained, addressing thus aspects such as the right to erasure and algorithmic discrimination.²⁰¹ This ensures that data is not used for unintended or undisclosed purposes. This focus on Data minimisation and Purpose limitation within the context of IoT aligns with the imperative to strike a balance between technological innovation and responsible data handling practices. As Macenaite posits, ‘this development cannot come at the expense of fundamental rights and freedoms.’²⁰²

¹⁹⁹ Altman and others (n 151).

²⁰⁰ Data minimisation and purpose limitation emerge as cornerstone principles in the GDPR, gaining heightened significance in the dynamic landscape of new technologies. They serve as protectors of individuals' privacy, fortifiers of data security, cultivators of user trust, and guardians of legal compliance, all the while presenting the challenge of harmonising innovation with regulatory adherence. The principles of data minimisation and purpose limitation will undergo further discussion in Chapter 4.

²⁰¹ Algorithmic discrimination refers to the biased or unfair treatment of individuals or groups based on the use of algorithms in decision-making processes. Algorithms are sets of instructions or rules followed by a computer program to perform a specific task. When these algorithms exhibit biased behaviour, it can lead to discriminatory outcomes.

²⁰² MACENAITE (n 191).

Regarding Blockchain, its immutability feature aligns with the principles of data integrity and accuracy. Once data is recorded on the Blockchain, it remains unalterable, ensuring the information's integrity. However, in my opinion, this creates a significant challenge, resulting in a paradox: the immutability of data hinders the exercise of crucial data subject rights, such as the right to erasure (right to be forgotten), rectification, and objection to processing. In response to this challenge, the DPPA emphasises the application of TOMs based on these principles of data integrity and accuracy. These measures are integrated with heavily pseudonymised data formats that include separate keys logged in a different system (data separation). Upon a data subject's request, these keys can be deleted, effectively rendering the associated data anonymised. Despite this approach posing a potential conflict with the "decentralised" characteristic of Blockchain technology²⁰³ (as it would necessitate some form of data centralisation for pseudonymisation keys), it appears, given the current state of the art, to be the most viable option for the DPPA to address the selection of technical measures aiming at achieving compliance with GDPR requirements concerning the rights of data subjects.

In the effort to regulate the use of AI within the EU, the European Commission has recently introduced the AI Act,²⁰⁴ marking the first EU Regulation on artificial intelligence and the world's first comprehensive AI law. This legislative framework is intended to establish overarching principles governing the development, commodification, and utilisation of products, services, and systems driven by AI within the territorial jurisdiction

²⁰³ Matthias Berberich and Malgorzata Steiner, 'Blockchain Technology and the GDPR - How to Reconcile Privacy and Distributed Ledgers Reports: Practitioner's Corner' (2016) 2 European Data Protection Law Review (EDPL) 422.

²⁰⁴ Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS, COM/2021/206 final.

of the EU. The aim is to reach an agreement among the EU countries in the Council on the final form of the law by the end of 2023. An important premise thus arises in EU law regarding AI, stipulating that the priority is to ensure the safety, transparency, traceability, non-discrimination, and environmental friendliness of AI systems used in the EU. Oversight of AI systems should be conducted by humans rather than automation to prevent harmful outcomes.²⁰⁵

The new Regulations, which will undoubtedly be crafted as *lex specialis* to the GDPR, delineate obligations for both providers and users, contingent upon the level of risk associated with AI. Despite many AI systems presenting minimal risk, they are still required to undergo assessment. It is crucial to note that, in its risk analysis threshold, the EU legislator introduces the concept of "unacceptable risk," a regulatory notion similar to that proposed by the DPPA in situations where the processing is identified as high-risk for the rights and freedoms of data subjects, emphasising the elimination (eradication) of risk rather than risk mitigation. AI systems classified as presenting unacceptable risk, considered a threat to individuals, will be prohibited. These encompass cognitive behavioural manipulation of people or specific vulnerable groups, such as voice-activated toys encouraging dangerous behaviour in children; social scoring, involving the classification of individuals based on behaviour, socio-economic status, or personal characteristics; and real-time and remote biometric identification systems, like facial recognition. Nevertheless, some exceptions may be permitted. For example, "post" remote

²⁰⁵ 'EU AI Act: First Regulation on Artificial Intelligence | News | European Parliament' (8 June 2023) <<https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence>>.

biometric identification systems, where identification occurs after a significant delay, will be allowed to prosecute serious crimes, but only with court approval.²⁰⁶

Regarding AI, the DPPA underscores the significance of fairness and transparency in AI algorithms, eliminating algorithmic discrimination and ensuring that decision-making processes are understandable and unbiased.²⁰⁷ For that end, the EDPB emphasised the importance of “Regularly assessing whether algorithms are functioning in line with the purposes and adjust the algorithms to mitigate uncovered biases and ensure fairness in the processing. Data subjects should be informed about the functioning of the processing of personal data based on algorithms that analyse or make predictions about them, such as work performance, economic situation, health, personal preferences, reliability or behaviour, location or movements”.²⁰⁸

The right to information²⁰⁹ must, therefore, be incorporated in the early stages of developments through appropriate TOMs, most of which are further identified in Chapters 8 and 9 of the thesis. Additionally, AI systems often handle sensitive information and special category data. In this regard, the DPPA mandates the implementation of robust security measures to safeguard the confidentiality and security of the data processed by AI, achieved through the application of effective enhanced privacy controls.

²⁰⁶ *ibid.*

²⁰⁷ Alessandra Calvi and Dimitris Kotzinos, ‘Enhancing AI Fairness through Impact Assessment in the European Union: A Legal and Computer Science Perspective’, *ACM International Conference Proceeding Series* (2023) <<https://go.exlibris.link/NYcLPcYz>>.

²⁰⁸ European Data Protection Board (EDPB), ‘Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0’ (EDPB 2020) <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en>.

²⁰⁹ For a discussion around the challenges of implementing the right to information in AI technology, See e.g., Iakovina Kindylidi and Inês Antas de Barros, ‘AI Training Datasets & Article 14 GDPR: A Risk Assessment for the Proportionality Exemption of the Obligation to Provide Information’ (2021) 13 *Revista de direito, estado e telecomunicações* 1.

Throughout various new technologies, the DPPA advocates for the application of cross-cutting principles, with accountability deemed crucial in holding organisations responsible for complying with data protection requirements. Additionally, given the potential intrusiveness of these technologies, the DPPA underscores the importance of applying TOMs directed towards user control and obtaining consent for processing.

Given the challenge posed by the complexity and interconnected nature of these technologies, including the contemporary ground where they operate—Cloud environments—the DPPA addresses the intricate relationships and dependencies between IoT, Blockchain, and AI in an adaptable manner to the evolving technological landscape. Regular updates and revisions to the GDPR will be essential to address emerging challenges and changes in technology, including updates to the law as technology evolves. Until then, the DPPA suggests that organisations incorporate mechanisms, such as codes of conduct and collective DPIAs, as part of their PbDD programme. This aims to demonstrate their commitment to developing services or products designed in a privacy-friendly way and that safeguard the data of the data subjects.²¹⁰

²¹⁰ In its recent guidance on AI, the ICO states: ‘You cannot delegate these issues to data scientists or engineering teams. Your senior management, including DPOs, are also accountable for understanding and addressing them appropriately and promptly (although overall accountability for data protection compliance lies with the controller, ie your organisation). To do so, in addition to their own upskilling, your senior management will need diverse, well-resourced teams to support them in carrying out their responsibilities. You also need to align your internal structures, roles and responsibilities maps, training requirements, policies and incentives to your overall AI governance and risk management strategy. It is important that you do not underestimate the initial and ongoing level of investment of resources and effort that is required. You must be able to demonstrate, on an ongoing basis, how you have addressed data protection by design and default obligations. Your governance and risk management capabilities need to be proportionate to your use of AI. This is particularly true now while AI adoption is still in its initial stages, and the technology itself, as well as the associated laws, regulations, governance and risk management best practices are developing quickly.’ ‘What Are the Accountability and Governance Implications of AI?’ (19 May 2023) <<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/what-are-the-accountability-and-governance-implications-of-ai/>>.

3.3. Securing Legal Certainty through the DPPA

The main objective of this section is to examine how legal uncertainties impede the successful implementation of PbDD and to elucidate how the DPPA tackles this challenge by offering solutions to overcome them. Legal certainty, as discussed in the introductory note of this chapter, is regarded as the core theoretical framework applied to this thesis. It not only informs the rationale behind the DPPA but also crucially justifies the necessity for its elaboration. Importantly, from a data protection perspective, 'legal certainty requires that decisions (*and actions*) are consistent with the framework of the existing legal system.'²¹¹ Moreover, as noted by Elina Paunio, 'in ECJ case law, considerations of legal certainty (i.e. predictability) are sometimes weighed against other principles such as that of effectiveness and uniformity in particular.'²¹² This viewpoint is particularly relevant in the scope of contemporary data protection law, in which the ECJ plays an important role in ensuring such legal certainty. An illustrative demonstration of this role is exemplified by the landmark cases *Schrems I*²¹³ and *Schrems II*,²¹⁴ wherein the ECJ deliberates on matters concerning international data transfers. Through these cases, the ECJ not only provides crucial guidance to businesses grappling with the complexities of cross-border data transfers but also delves into pivotal legal intricacies linked to such transfers.²¹⁵ In doing

²¹¹ Elina Paunio, 'Beyond Predictability - Reflections on Legal Certainty and the Discourse Theory of Law in the EU Legal Order' (2009) 10 German Law Journal 1469. Emphasis Added.

²¹² *ibid.*

²¹³ *Case C-362/14 Maximilian Schrems v Data Protection Commissioner EU:C:2015:650.*

²¹⁴ *Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems (Request for a preliminary ruling from the High Court (Ireland)) EU:C:2020:559.*

²¹⁵ Some cases illustrate the ECJ's role in interpreting and clarifying data protection laws within the EU, emphasising the significance of legal certainty in safeguarding individuals' privacy rights and regulating cross-border data flows, such is the case, for example, of *Schrems II (Case C-311/18)*: This case addressed the legality of transferring personal data from the EU to the United States under the Privacy Shield framework.

so, the ECJ seeks to bring about legal certainty to the international arena, thereby contributing to a more transparent and predictable legal framework for data protection in the global context. Among these complexities, the ECJ addresses, for example, issues of effective redress and remedy, which are fundamental to ensuring robust protection of individuals' rights in the context of international data transfers. However, the rulings of the ECJ do not always result in complete clarification of all legal matters. For example, despite the Court's best efforts, 'there still remains significant uncertainty as to the substantive requirements of effective redress in the context of international data transfers.'²¹⁶ This uncertainty underscores the ongoing challenges in achieving comprehensive clarity and consistency in data protection law, particularly considering that, for example, in relation to the above example, 'the European Data Protection Board's (EDBP's) guidelines is incomplete and ad hoc, [...], failing to lay down a comprehensive set of clear standards and expectations.'²¹⁷

The ECJ's decision invalidated the Privacy Shield agreement due to concerns about the adequacy of data protection standards in the US, highlighting the importance of legal certainty in cross-border data transfers; *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (Case C-131/12)*: Commonly known as the "Right to be Forgotten" case, this ruling established an individual's right to request the removal of search engine links containing personal information deemed inadequate, irrelevant, or excessive, thus emphasising the need for legal certainty in determining the scope of personal data protection rights; *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (Case C-362/14)*: Often referred to as Schrems I, this case questioned the legality of transferring personal data from the EU to the US under the Safe Harbor framework. The ECJ's decision invalidated the Safe Harbor agreement, citing concerns about US surveillance practices and underscoring the importance of legal certainty in international data transfers; *Wirtschaftsakademie Schleswig-Holstein GmbH v Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (Case C-210/16)*: This case clarified the scope of consent for the use of cookies under the EU ePrivacy Directive and the GDPR. The ECJ ruled that obtaining valid consent requires active user action, providing legal certainty on the interpretation of consent requirements for online tracking technologies.

²¹⁶ Maria Tzanou and Plixavra Vogiatzoglou, 'In Search of Legal Certainty Regarding "Effective Redress" in International Data Transfers: Unpacking the Conceptual Complexities and Clarifying the Substantive Requirements' [2023] *Review of European Administrative Law*, Forthcoming <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4325287>.

²¹⁷ *ibid.*

Therefore, these concerns are highly relevant to the elaboration of the DPPA, as they provide the groundwork for establishing a framework that manages personal data through procedural²¹⁸ (in sensu lato) and a structured and systematic approach to compliance. To achieve this objective, the DPPA focus on bridging the sometimes-blurred legal requirements into data operations. This framework encompasses policies, procedures, and codes of conduct related to data protection, data processing, data subject rights, data breaches, and other relevant aspects. Additionally, it is able to fill in the gaps in legislation, ensuring comprehensive coverage and effective implementation of data protection measures.

By addressing legal certainty, the DPPA ensures that organisations can establish an effective PbDD programme that operates with a high degree of accuracy. Undoubtedly, addressing legal gaps and uncertainty in the DPPA is vital for the sustained success of organisations operating in today's heavily regulated, data-driven landscape. To commence this endeavour, it is essential to provide an overview of the concept of 'legal certainty' within the context of EU law and correlate it with DPPA actions. This initial step will establish the foundation for the rest of the discourse and set the tone for a more comprehensive discussion.

²¹⁸ See, Paunio (n 209). 'Defining legal certainty as encompassing substantive legal certainty that may be enhanced through communication between relevant legal actors in a given legal community comes close to Habermas' understanding of legal certainty. [...] Importantly, the fact that both laws and contexts of interpretation change means that something is needed to guarantee at least some level of stability. In this sense what remains stable and predictable is the procedure itself.'

3.3.1. Achieving Clarity and Consistency: Exploring the Impact of the EU Principle of Legal Certainty on Data Protection Law

Legal certainty is a fundamental principle of EU law that aims to ensure that legal rules are clear, predictable, and consistent.²¹⁹ It allows individuals and organisations to understand their rights and obligations, thus facilitating compliance with the law. Legal certainty also enables effective judicial protection, as it enables courts to interpret and apply the law consistently. As such, the principle of legal certainty plays a critical role in upholding the rule of law in the EU.

It is evident from the literature review conducted²²⁰ that legal certainty and legitimate expectations are features embedded in the general principles of EU law, including the GDPR.²²¹ These principles necessitate 'that rule of law be clear, precise, and

²¹⁹ See, e.g., Aurelien Portuese, Orla Gough and Joseph Tanega, 'The Principle of Legal Certainty as a Principle of Economic Efficiency' (2017) 44 *European Journal of Law and Economics* 131. 'Recognised expressly for the first time in *Bosch*, the principle of legal certainty has a structural role in the case-law of the ECJ as "fundamental principle" of EU law. Thus, the principle of legal certainty is said to be 'one of the most important general principles recognised by the European Court'. [...], 'The EU principle of legal certainty is a "guiding" and "multi-faceted principle" that while "underpinning any legal system" encompasses both notions of legitimate expectations and of non-retroactivity (or nonretrospectivity) of the law.[...], 'Recognised for the first time by the ECJ in *Firma August Toepfer*, the principle of legitimate expectations (or "principe de confiance legitime") is said to be essential to the EU legal order as part of the general principle of EU law of legal certainty. This important nature of the principle of legitimate expectations renders it applicable both to national acts and EU legal acts, be they of general scope or not.' [...], 'The notion of the predictability of the law partakes to its certainty. The principle of legal certainty entails that the "Community legislation must be unequivocal and its application must be predictable for those who are subject to it"'.

²²⁰ See, e.g., Mark Fenwick and Stefan Wrba, 'The Shifting Meaning of Legal Certainty' in Mark Fenwick and Stefan Wrba (eds), *Legal Certainty in a Contemporary Context: Private and Criminal Law Perspectives* (Springer Singapore 2016) <https://doi.org/10.1007/978-981-10-0114-7_1>.

²²¹ One EU legal certainty theory applied to data protection law is the principle of legal predictability. This principle suggests that individuals and organisations should be able to foresee the legal consequences of their actions, particularly in the context of data protection compliance. Legal predictability entails clear and accessible laws, regulations, and guidelines that provide stakeholders with a clear understanding of their rights and obligations regarding the processing of personal data. Another theory is the principle of legal consistency, which emphasises the need for uniform interpretation and application of data protection laws across EU member states. Consistent application ensures that individuals and businesses are treated similarly regardless of their location within the EU, fostering trust and confidence in the legal system and promoting compliance with data protection regulations. Additionally, the principle of legal transparency is relevant to data protection law. This principle advocates for transparency in the formulation, interpretation, and

predictable in their effect, so that interested parties can ascertain their position in situations and legal relationships governed by EU law'.²²²

Martin Rodriguez²²³ underscores that, according to the CJEU, EU law arms individuals with the following tools: (i) as a condition to the validity and/or enforceability of legal norms, individuals may bring an action to overturn a rule that fails to meet some formal requirements such as clarity, precision²²⁴ or official publication; (ii) as protecting predictability, the principle of legal certainty may not override a substantive legal choice, but it may prevent its subjective application for reasons such as retrospective effect or against individuals' legitimate expectations; (iii) legal certainty, as part of the legal system, applies not only to direct rules but also to indirect legislation, allowing individuals to challenge a prejudicial application, even at the interpretive level;²²⁵ (iv) legal certainty also concerns the right to an effective judicial remedy and a fair trial, as it requires a prior clear determination by the competent court or may preclude changes in the law that either shorten the time for bringing an action or affect ongoing legal proceedings.²²⁶ Therefore, when the rule of law and other fundamental principles in EU law deteriorate, an approach

application of data protection laws and regulations. Transparent laws and processes enable stakeholders to understand the rationale behind legal requirements and decisions, facilitating compliance and accountability in data processing activities.

²²² CJEU 12 February 2015, Case C-48/14, Parliament v Council, para. 45.

²²³ Pablo Martín Rodríguez, "A Missing Piece of European Emergency Law: Legal Certainty and Individuals' Expectations in the EU Response to the Crisis" (2016) 12 European Constitutional Law Review 265.

²²⁴ See, *Joined cases C-201/10 and C-202/10 Ze Fu Fleischhandel GmbH (C-201/10) and Vion Trading GmbH (C-202/10) v Hauptzollamt Hamburg-Jonas* EU:C:2011:282, [2011] ECR I-03545. paras. 35 and 52.

²²⁵ See, *Case C-91/92, Paola Faccini Dori v Recreb Srl* EU:C:1994:292, [1994] ECR I-03325., para. 27. See also, *Fleischhandel [2010]* (n 222), para 27.; *Case C-80/86 Criminal proceedings against Kolpinghuis Nijmegen BV* EU:C:1987:431, [1987] ECR 1987-03969. paras. 13-14. See also, *Case C-7/11 Fabio Caronna Reference for a preliminary ruling from the Tribunale di Palermo [2012]* EU:C:2012:396. paras. 52-56; and *Case C-105/03 Criminal proceedings against Maria Pupino (Reference for a preliminary ruling: Tribunale di Firenze)* EU:C:2005:386, [2005] ECR I-05285. paras. 44-45.

²²⁶ *Stefanetti and Others v Italy, Apps nos 21838/10, 21849/10, 21852/10, 21855/10, 21860/10, 21863/10, 21869/10 and 21870/10 (ECtHR, 15 April 2014).*

based on the general principles of legal certainty and legitimate expectations may be appropriate.²²⁷

Comprehending the significance and roles of legal certainty as a constitutional principle of EU law, and its correlation with EU data protection law, is crucial, as there is a clear need to clarify ambiguous concepts and fill in gaps in GDPR. An appropriate interpretation of the principle of legal certainty in the EU can help address the shortcomings of GDPR by balancing the legal requirements and the efforts of controllers to comply; in the case of PbDD, legal certainty is achieved through a balance between clear and precise legal rules and the flexibility needed to accommodate the technical complexities involved.²²⁸ As noted by Elina Paunio, legal certainty demands a balance between stability and flexibility. Paunio also makes a distinction between formal and substantive legal certainty:

[F]ormal legal certainty implies that laws and, in particular, adjudication must be predictable: laws must satisfy requirements of clarity, stability, and intelligibility so that those concerned can with relative accuracy calculate the legal consequences of their actions as well as the outcome of legal proceedings. Substantive legal certainty, then, is related to the rational acceptability of legal decision-making. In this sense, it is not sufficient that laws and adjudication are predictable: they must also be accepted by the legal community in question.²²⁹

²²⁷ Martín Rodríguez (n 221).

²²⁸ See, e.g., Constantin Elena, 'Evolution of the Quality of Regulation Concept in the Context of Ensuring Legal Certainty' (2019) 7 *Academic Journal of Law and Governance (AJLG)* 107. 'Given the amount of legislation, regulatory quality requirements should be rigorous in the sense that law quality standards should come to ensure the accuracy of laws, and thus balance and efficiency. For optimum results in the law-making process, cooperation between stakeholders remains an essential condition. The accuracy and clarity of the text have a particularly important role in the texts of the law.'

²²⁹ Paunio (n 209).

This statement reminds me of the tale of the young ruler undertaking the reform the law of the land, presented in Chapter one, and the lesson this story teaches.

‘[T]o command what cannot be done is not to make law; it is to unmake law, for a command that cannot be obeyed serves no end but confusion, fear and chaos’.^{230,231}

The lack of precision in the GDPR, especially concerning PbDD,²³² is seen as a source of legal uncertainty and may explain why numerous businesses have not fully adopted the Regulation or have only done so to a limited degree.²³³ Judging by the number of fines imposed by EU regulators²³⁴ in the initial four years of GDPR's enforcement, it is reasonable to affirm the validity of this statement.

²³⁰ Purtova (n 76).

²³¹ This statement implies that laws and regulations, including those related to data protection, must be practical and achievable. If a law imposes obligations or requirements that are impossible for individuals or organisations to fulfil, it essentially renders the law ineffective and undermines its purpose. In the context of data protection, this could include regulations that demand unattainable levels of security or impose overly burdensome compliance measures. Furthermore, it suggests that unrealistic or unachievable laws create confusion, fear, and chaos rather than promoting compliance and order. Individuals and organisations may struggle to understand and adhere to unclear or impractical legal requirements, leading to uncertainty and anxiety about potential legal consequences. Therefore, in the context of data protection law, it is crucial for regulations such as the GDPR to be formulated in a way that is clear, practical, and achievable, ensuring that they effectively serve their intended purpose of protecting individuals' privacy rights and promoting responsible data handling practices.

²³² See, e.g., Bygrave (n 67). ‘Whereas data protection by design and by default is an essential part of a state’s positive obligations to secure respect for the right(s) laid down in ECHR Article 8, at least in relation to safeguarding the confidentiality of health data, its precise status under EU law remains somewhat unclear.’; ‘Article 25 suffers from multiple weaknesses. One obvious weakness is the vagueness and complexity of its language. This is augmented by a paucity of authoritative clear guidance on the parameters and methodologies for achieving data protection by design and by default – a problem that also afflicts discourse on PbD.’

²³³ Also, it pertains to the principle of designing data processes with a clear and specific purpose in mind, ensuring that data collection, storage, and further processing align closely with that purpose. The lack of precision in the GDPR, particularly concerning PbDD, contributes to legal uncertainty for businesses. As discussed, this ambiguity may stem from vague language or insufficient guidance on implementing PbDD principles effectively. Consequently, businesses find it challenging to interpret and apply these principles in their data protection management practices, leading to confusion and potential compliance issues.

²³⁴ Annex 1 presents a visualisation of the analysis conducted on fines imposed under GDPR.

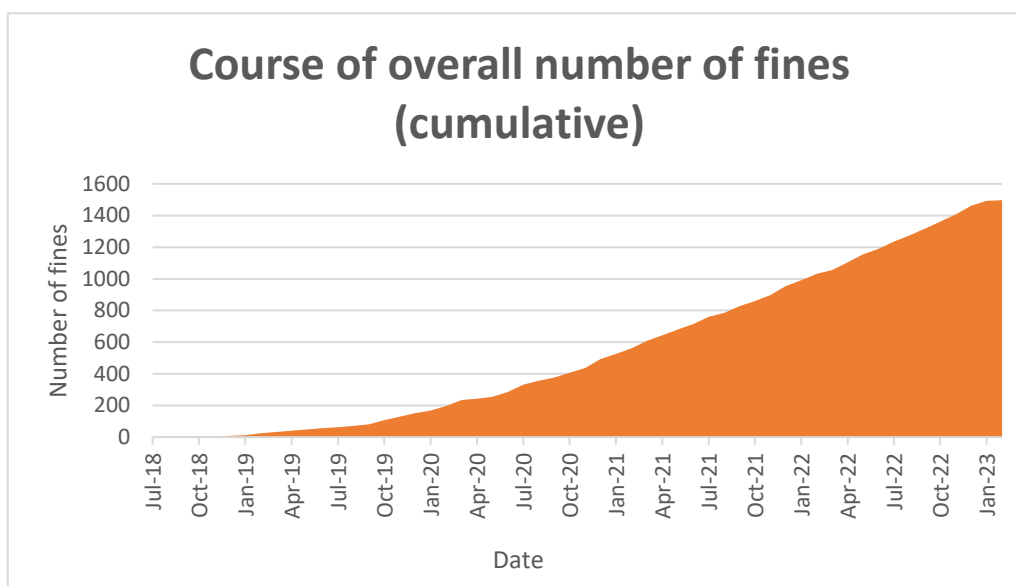


Figure 6 - Course of overall number of GDPR fines (cumulative, May 2018-January 2023)

Keeping this context in mind, we can now proceed to a more detailed examination of the role of the DPPA in the context of legal certainty.

3.3.2. Navigating Legal Uncertainty: Examining How the DPPA Addresses Legal Certainty

Thus far, we have understood that PbDD can assist controllers by integrating the data protection principles into the design and operation of systems and processes, thereby reducing the likelihood of non-compliance with the GDPR. By embedding privacy and data protection principles into the design of systems and processes, PbDD ensures that organisations take a proactive approach to data protection compliance, rather than merely reacting to compliance issues as they arise. Moreover, PbDD can aid in tackling legal uncertainty by offering a structure for evaluating and controlling data protection risk, such as conducting DPIAs and collective DPIAs to detect and mitigate potential risk linked with a particular data processing activity. These evaluations help organisations to pinpoint and

resolve privacy risks before they become compliance problems, ultimately lessening legal uncertainty.²³⁵

The theoretical understandings of legal certainty expressed in this chapter align with the central concept of predictability.²³⁶ Therefore, to mitigate the adverse effects of legal uncertainty on an organisation's compliance efforts, it is essential to implement suitable, tangible TOMs. The DPPA suggests that one of the primary measures is to establish a mechanism for keeping up to date with any changes in data protection laws and Regulations, ensuring that the organisation's policies and procedures are updated accordingly. Regular audits and assessments of the organisation's data processing activities can also help to identify any areas of non-compliance and ensure that corrective measures are taken promptly.²³⁷ Furthermore, organisations can engage with external experts and legal counsel to obtain guidance on data protection compliance matters. This can assist controllers in navigating the complexities of data protection laws and Regulations, ensuring that their practices align with legal requirements. The DPPA effectively incorporates all of these elements.

The DPPA framework advocates a principles-based approach to GDPR compliance. This approach centres on fundamental principles that guide the interpretation and

²³⁵ In my opinion, a DPIA can help to address the issue of legal uncertainty at an internal, organisational level by providing a structured and documented approach to assessing and managing privacy risks associated with processing activities. This approach ensures compliance with the GDPR and provides regulators with evidence of compliance.

²³⁶ Predictability in the context of legal certainty also ensures that individuals and organisations can make informed decisions and plan their actions accordingly, without fear of unexpected legal consequences. This requires laws and regulations to be formulated in a manner that is clear, unambiguous, and capable of consistent interpretation and application across different contexts.

²³⁷ The GDPR underscores the importance of accountability, requiring organisations to demonstrate compliance with its provisions. Regular audits facilitate this by providing a structured mechanism for organisations to assess their data processing practices against GDPR requirements. Through these audits, organisations can identify any areas of non-compliance, potential vulnerabilities, or gaps in data protection measures.

application of the Regulation.²³⁸ Furthermore, the DPPA places a strong emphasis on contextual adaptability and the integration of these principles into the operational fabric of organisations. The core principles outlined by the DPPA include maintaining clear records of data processing activities, conducting regular audits, and ensuring transparent communication with data subjects about how their data is handled (similar to the accountability approach).²³⁹ This involves clearly defining the purpose of data processing, ensuring fairness in data processing practices, and respecting the legal foundations for processing.

In addition, the DPPA underscores the importance of maintaining data integrity and confidentiality, thereby promoting a comprehensive approach to data security. Recognising the potential intrusiveness of data processing,²⁴⁰ the DPPA highlights the importance of implementing TOMs that empower data subjects with control over their personal information. Obtaining explicit consent for processing and facilitating the exercise of data subject rights, such as the right to erasure and rectification, are integral aspects.

To implement the principles-based approach in practice, organisations need to integrate these principles into their fundamental data processing procedures. This may involve various strategies, such as conducting regular impact assessments, incorporating PbDD practices during the development of new systems, and cultivating a culture of data

²³⁸ This approach recognises the dynamic nature of data protection and the diverse contexts in which organisations operate. By centring on principles rather than rigid rules, the DPPA allows for flexibility and adaptability, enabling organisations to tailor their compliance efforts to their unique circumstances while adhering to the overarching principles of the GDPR.

²³⁹ These principles reflect the accountability approach of the GDPR, which emphasises the responsibility of organisations to demonstrate compliance and accountability in their data processing practices.

²⁴⁰ See, Lynskey (n 179). 'Pursuant the case law on Article 8 of the European Convention on Human Rights (ECHR), the mere fact of systematically collecting and storing an individual's publicly available data can constitute an interference with the right to private life.'

protection awareness among employees.²⁴¹ Additionally, organisations are urged to develop and embrace codes of conduct as integral components of their PbDD programmes.²⁴² This signifies a commitment to adopting practices that prioritise privacy. In essence, the DPPA's principles-based approach provides a flexible yet comprehensive framework for achieving GDPR compliance, anchored on clear legal premises. It encourages organisations to adeptly navigate the complexities of data protection, uphold individual rights, and adjust to the ever-evolving technological landscapes.²⁴³

The proposed DPPA framework distinguishes itself from the current GDPR accountability approach in several keyways. In terms of the flexible application of principles, while the GDPR accountability approach outlines principles that organisations must follow, it does not prescribe a specific methodology for their implementation. Conversely, the DPPA places a stronger emphasis on contextual adaptability and the practical implementation of principles. It encourages organisations to integrate these principles into their daily operations, aligning with the specificities of their activities and, most significantly, providing practical tools for application.²⁴⁴

²⁴¹ Cultivating a culture of data protection awareness among employees is essential for implementing the principles-based approach. This involves providing regular training and education on data protection principles and practices, raising awareness about the importance of protecting personal data, and empowering employees to take ownership of data protection responsibilities in their respective roles within the organisation.

²⁴² By establishing codes of conduct, organisations can formalise their commitment to privacy and data protection principles, outlining clear expectations regarding the processing of personal data. These codes of conduct may include provisions for data minimisation, purpose limitation, transparency, and accountability, among other key principles of data protection. Moreover, codes of conduct serve as practical tools for operationalising PbDD within the organisation. They provide concrete guidance on how to integrate privacy and data protection considerations into the design, development, and operation of systems and processes, helping to ensure that PbDD practices are effectively implemented across various departments and functions.

²⁴³ For a discussion on methodology to ensure GDPR compliance integration in an ever-evolving privacy landscape, See, Li and others (n 151).

²⁴⁴ This statement underscores the delicate balance between flexibility and prescriptiveness in regulatory frameworks for data protection and privacy. While the GDPR prioritises flexibility and adaptability, the proposed DPPA framework seeks to provide more structured guidance and support for organisations, potentially offering a clearer path to compliance and accountability.

Regarding the proactive demonstration of compliance, the GDPR requires organisations to be accountable for compliance but does not explicitly mandate proactive measures for demonstrating this accountability other than conducting audits. On the other hand, the DPPA encourages organisations to adopt a proactive stance in demonstrating compliance. This entails, for example, mapping the PbDD activities to the processing activities, maintaining clear records of data processing activities, conducting regular audits, and fostering transparent communication with data subjects. The DPPA clearly presents a simple-to-follow pathway for achieving accountability through actions.

An important aspect of compliance relates to the integration of TOMs and privacy controls. While the GDPR promotes the implementation of TOMs, it does not explicitly emphasise their integration into organisational processes. In contrast, the DPPA identifies such measures and underscores the importance of integrating TOMs directed towards user control and obtaining consent for processing. This ensures that appropriate TOMs are not isolated but are woven into the fabric of data processing operations. Moreover, the GDPR mentions codes of conduct as one of several mechanisms for demonstrating compliance²⁴⁵ but does not specifically highlight their role. The DPPA proposes the incorporation of several mechanisms, such as codes of conduct, SOPs²⁴⁶ and collective DPIAs, as part of organisations' PbDD programme. This underscores the commitment to developing services

²⁴⁵ Codes of conduct are mentioned as one of the mechanisms, alongside certifications, seals, and marks, as well as adherence to approved certification mechanisms (Article 42 of the GDPR). Codes of conduct are voluntary, self-regulatory frameworks that organisations can adopt to demonstrate their commitment to GDPR principles and standards. They provide specific guidelines and standards for data protection practices within a particular industry or sector.

²⁴⁶ SOPs are detailed, step-by-step instructions that outline the processes and protocols for handling personal data within an organisation. By establishing SOPs as part of their PbDD programmes, organisations can ensure consistency and standardisation in data processing activities, helping to mitigate the risk of non-compliance and ensure accountability.

or products in a privacy-friendly manner and promotes public trust in the data processing stakeholders. A significant advantage of the DPPA lies in its adaptability to the technological landscape, whereas the GDPR offers broad principles applicable to various technologies but does not explicitly address the evolving nature of technology. In contrast, the DPPA goes as far as recognising the intricate relationships and dependencies between organisational personal data processing requirements and technologies such as IoT, Blockchain, and AI. It encourages an adaptable approach to the evolving technological landscape and acknowledges the need for regular updates and revisions in procedure and law to address emerging challenges.

Another important aspect that the DPPA addresses relates to the required legal certainty concerning the framing of organisational processing activities within the PbDD requirements.²⁴⁷ In the context of the GDPR, the concept of legal certainty is held as fundamental to providing clear and predictable rules for individuals, businesses, and organisations regarding the processing of personal data. It is, however, essential to acknowledge that environmental events can influence the "level" of legal certainty provided by the Regulation. Within the rapidly evolving landscape of data protection law, as exemplified by the CJEU's invalidation of the EU-US Privacy Shield,²⁴⁸ instances arise wherein a discernible lack of legal certainty might appear to be inherent to the GDPR

²⁴⁷ The PbDD requirements, which encompass principles like purpose limitation and data minimisation, are fundamental aspects of data protection laws aimed at safeguarding individuals' privacy rights. However, without clear and precise guidelines on how organisations should interpret and implement these requirements, legal certainty may be compromised. Uncertainty regarding the application of PbDD principles can lead to inconsistencies in how organisations handle personal data, potentially resulting in violations of data protection laws and infringement of individuals' rights. The DPPA addresses this need for legal certainty by providing a framework that clarifies the requirements and obligations related to PbDD. By outlining specific guidelines and procedures for framing organisational processing activities within the PbDD framework, the DPPA enhances legal certainty for both data controllers and data subjects.

²⁴⁸ 'EU TOP COURT STRIKES DOWN PRIVACY SHIELD, CCIA CALLS FOR URGENT LEGAL CERTAINTY AND SOLUTIONS' *States News Service* (16 July 2020) NA.

itself.²⁴⁹ Therefore, due consideration is given to a common critique of the GDPR: the Regulation falls short in delivering the necessary certainty. Legal certainty within the GDPR must be reflected in the clarity and precision of its provisions. Therefore, the Regulation should articulate the rights and responsibilities of data subjects, controllers, and processors in a manner that aims to be unambiguous and easily comprehensible. The lack of clarity can also manifest, for instance, in matters concerning interpretation, definitions, and terminology used in the GDPR.²⁵⁰ As Gianclaudio Malgieri elucidates in relation to the risks of paternalism in a vulnerability-approach to data protection, 'the lack of clarity about what 'harm' means in the data protection field and the consequent impossibility to perform an objective cost-benefit analysis that could protect individuals from themselves without the risk of undue paternalism.'²⁵¹ Although the Regulation relies on being interpreted and enforced with the guidance of supervisory authorities,²⁵² these authorities should play a more crucial role in ensuring legal certainty by providing prompt guidance and clarification

²⁴⁹ In light of these challenges, organisations may face difficulties in navigating the complex regulatory landscape and ensuring compliance with the GDPR. The lack of legal certainty inherent in certain aspects of the GDPR underscores the need for ongoing guidance, clarification, and interpretation by regulatory authorities, as well as continuous monitoring of developments in data protection law and jurisprudence.

²⁵⁰ Interpretation of the GDPR provisions can be challenging due to the complexity of the legal language used in the regulation. The GDPR contains numerous legal terms and concepts that may be subject to different interpretations by data controllers, data processors, data protection authorities, and legal practitioners. As a result, there may be ambiguity regarding the precise scope and application of certain provisions, leading to uncertainty about compliance requirements. Definitions play a crucial role in determining the scope and application of GDPR provisions. Some GDPR definitions are broad or open to interpretation, which can contribute to uncertainty in their application. For example, terms such as "personal data," "data subject," "processing," and "consent" are central to the GDPR but may be interpreted differently in various contexts, leading to inconsistent application of the regulation.

²⁵¹ Gianclaudio Malgieri, 'The Limitations and the Alternatives of a Vulnerability-Based Interpretation of the GDPR' in Gianclaudio Malgieri (ed), *Vulnerability and Data Protection Law* (Oxford University Press 2023) <<https://doi.org/10.1093/oso/9780192870339.003.0008>>.

²⁵² Supervisory authorities provide this guidance through various means such as guidelines, recommendations, and decisions, helping organisations understand their obligations under the GDPR and ensuring consistent enforcement across different jurisdictions.

on the application of the GDPR in specific cases, without the delays (sometimes of months) that have been observed.²⁵³

It is true that the GDPR incorporates mechanisms to enhance legal certainty across the EU. For example, the consistency mechanism involves cooperation between supervisory authorities in different member states to ensure uniform application of the GDPR. The European Data Protection Board (EDPB) plays a key role in this process, promoting a harmonised interpretation of the Regulation. However, in this respect, there seems to be a deficit of information, particularly concerning the practical aspects of the implementation of GDPR,²⁵⁴ notably in regard to the implementation of PBDD, which this thesis successfully addresses. As previously mentioned, the ECJ also plays a significant role in shaping the interpretation of the GDPR, often leading to major operational impacts. Its decisions on data protection cases contribute to legal certainty by providing authoritative rulings on specific issues, helping to clarify the application of the Regulation in different contexts.²⁵⁵ However, there is clearly a lack of a mechanism that can "translate" those

²⁵³ While supervisory authorities play a crucial role in interpreting and enforcing the GDPR, there is criticism that they should improve their responsiveness and efficiency in providing guidance and clarification to ensure legal certainty for organisations subject to the regulation.

²⁵⁴ While the EDPB issues significant guidelines, recommendations, and opinions to clarify various aspects of the GDPR, there is a lack of detailed guidance on how organisations should practically implement these requirements in their day-to-day operations. This deficit of practical information poses challenges for organisations seeking to comply with the GDPR effectively. Without clear guidance on how to implement specific GDPR provisions in practice, organisations struggle to understand their obligations and may inadvertently fail to meet compliance requirements.

²⁵⁵ For instance, the following cases illustrate the evolving landscape of data protection and the CJEU's role in interpreting and shaping the legal framework: *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González* (2014): Often referred to as the "Right to be Forgotten" case, this ruling by the CJEU clarified the rights of individuals to request the removal of search engine results linked to their personal data under certain conditions. It addressed the balance between privacy rights and the public's right to access information; *Schrems I - Maximilian Schrems v Data Protection Commissioner* (2015): This case led to the invalidation of the EU-US Safe Harbor framework, highlighting concerns about the transfer of personal data from the EU to the US. The CJEU emphasized the importance of ensuring an adequate level of data protection when personal data is transferred outside the EU; *Tele2 Sverige AB v Post- och telestyrelsen, Secretary of State for the Home Department v Tom Watson* (2016): This case addressed data

rulings and "legalese" into practical actions for organisations—an undertaking that the DPPA assumes.²⁵⁶

As previously discussed, legal certainty is also crucial in the context of data subject rights. The GDPR clearly defines the rights of individuals, such as the right to access, rectification, erasure, and the right to object to processing. This clarity empowers data subjects to understand and exercise their rights effectively. However, due to a lack of specific guidance in incorporating addressing mechanisms into businesses' processing activities, there is a risk that these rights may not be upheld as intended by the legislator when drafting the GDPR. For this reason, the DPPA contributes by framing them within a coherent operational framework.²⁵⁷

Elina Paunio, argues that 'Legal certainty requires a balance between stability and flexibility.'²⁵⁸ Following this perspective, it is my belief that the DPPA acts as a 'moderator' in addressing the concept of legal certainty within the operational context of data protection, particularly in response to the points outlined above. Firstly, the DPPA emphasises a principles-based approach, providing clarity and precision in articulating the data protection principles. By explicitly outlining how organisations should implement

retention obligations imposed on electronic communication service providers. The CJEU emphasized the need for a balance between national security interests and the fundamental rights of individuals, emphasizing the principles of necessity and proportionality; *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV* (2019): This case dealt with the joint responsibility of website operators for the collection and transmission of personal data through embedded Facebook "Like" buttons. The CJEU clarified aspects of joint controllership and the need for transparent information to individuals.

²⁵⁶ By analysing ECJ rulings and translating them into actionable guidance, the DPPA helps organisations understand how to apply legal principles in their day-to-day data processing activities. This involves breaking down complex legal concepts into practical steps and providing clear guidance on compliance measures that organisations can adopt to align with ECJ interpretations of the GDPR.

²⁵⁷ By framing these rights within a comprehensive operational context, the DPPA assists organisations in understanding their obligations and implementing effective mechanisms to uphold data subject rights in line with the GDPR's requirements. This ensures that data subjects can confidently exercise their rights and that businesses can navigate the complexities of compliance with certainty.

²⁵⁸ Paunio (n 209).

these principles, the DPPA aims to enhance understanding and compliance, contributing to legal certainty.

Secondly, the DPPA introduces a framework that aligns with GDPR principles, offering guidance on how to implement and adhere to these principles effectively. It also advocates for oversight and engagement with supervisory authorities, reinforcing legal certainty through consistent interpretation and application.

Thirdly, the DPPA encourages the development of codes of conduct, SOPs, standards, and mechanisms beyond those in the GDPR. By promoting the adoption of these standards, the DPPA contributes to consistency and harmonisation in data protection practices, aligning with the EC's efforts to ensure legal certainty across member states. One of the key strengths of the DPPA is its focus on practical, context-specific TOMs. This approach ensures that organisations can translate the principles into concrete actions, promoting legal certainty by offering a clear path for compliance. Moreover, in acknowledging the intricate relationships and dependencies between different processing technologies, including IoT, Blockchain, and AI, the DPPA demonstrates an awareness of the evolving technological landscape. This adaptability is essential for legal certainty in a rapidly changing digital environment.

Finally, the DPPA recognises the necessity for regular updates and revisions in organisational procedures and laws to address emerging challenges. This proactive approach aligns with the concept of legal certainty by ensuring that the framework remains relevant and effective in response to evolving data protection requirements and technological advancements.

3.4. Concluding remarks

In this chapter, we explored the theoretical considerations underpinning the application of the DPPA, specifically delving into the intricate realm of legal certainty within the context of data protection, with a specific focus on the DPPA's role in ensuring its achievement. As we delved into the nuances of both the legal interpretation of GDPR requirements and its practical implementation, the DPPA emerged as a pivotal framework offering innovative solutions to the challenges posed by the GDPR.²⁵⁹

The DPPA's distinctive principles-based approach provides a flexible yet comprehensive guide for organisations grappling with the complexities of data protection. By explicitly outlining how to integrate these principles into daily operations, the framework not only promotes compliance but also empowers organisations to actively demonstrate their commitment to safeguarding user data.

Legal certainty, a cornerstone of EU law and GDPR compliance, finds resonance in the DPPA's emphasis on contextual adaptability and practical implementation. The framework recognises the evolving technological landscape, where legal interpretations must evolve in tandem. Through its encouragement of oversight and engagement with supervisory authorities, the DPPA contributes to a consistent and harmonised application of GDPR principles through PbDD, reinforcing legal certainty in a rapidly changing digital environment. Moreover, the DPPA addresses a critical gap identified in the GDPR - the translation of legal rulings and intricate legal language into practical actions for

²⁵⁹ The theoretical framework underlying the exploration of the DPPA in this chapter revolves around the concept of legal certainty within the context of data protection, particularly concerning its application under the GDPR. The DPPA is positioned as a central framework designed to address the challenges associated with legal certainty and ensure its attainment in data protection practices.

organisations. By offering a clear path for compliance, listing appropriate TOMs, promoting the adoption of codes of conduct, SOPs, and other mechanisms of compliance, the DPPA serves as a beacon for organisations navigating the sometimes-murky waters of data protection law.

As we conclude this contextualisation of the DPPA, which paves the way for the following, more practical-oriented chapters, it is evident that this framework stands at the forefront of the ongoing dialogue surrounding data protection. Its adaptability, practicality, and commitment to user empowerment position the DPPA as a key candidate in shaping the future of data protection governance. In the chapters that follow, we will further dissect the implications of the DPPA, examining its role in specific contexts and its contribution to a more secure and transparent digital landscape.

Chapter 4 – A conceptual analysis of PbDD

‘The GDPR provides for two crucial concepts for future project planning: Data Protection by Design and Data Protection by Default. While long recommended as good practice, both of these principles are enshrined in law under the GDPR (Article 25).

Data Protection by design means embedding data privacy features and data privacy enhancing technologies directly into the design of projects at an early stage. This will help to ensure better and more cost-effective protection for individual data privacy.

Data Protection by default means that the user service settings (e.g., no automatic opt-ins on customer account pages) must be automatically data protection friendly, and that only data which is necessary for each specific purpose of the processing should be gathered at all.’²⁶⁰

Introductory notes

As a privacy concept, Privacy by Design (PbD) was created by Ann Cavoukian in the nineties in response to growing concerns about the privacy rights of individuals arising from advances in data technologies. By the turn of the century, PbD had already been defined as a framework that enabled organisations to include privacy directly in their business practices, physical environments, and network infrastructures - making it the default.²⁶¹ As a result, PbD has evolved into something resembling a "privacy standard" that can be applied to all types of business processes and activities. By introducing PbD into data

²⁶⁰ ‘Data Protection by Design and by Default | Data Protection Commission’ (*Data protection by Design and by Default* | *Data Protection Commission*) <<https://www.dataprotection.ie/organisations/know-your-obligations/data-protection-design-and-default>>.

²⁶¹ Cavoukian, ‘Privacy by Design [Leading Edge]’ (n 25).

protection law, the GDPR forces organisations to operationalise its concepts towards 'building privacy right into system design'²⁶² to enhance the protection of personal data.

Cavoukian explains that one of the jobs of 'engineers and systems architects is to translate the PbD conceptual framework into a set of specific, and operationally feasible tools.' In the context of the GDPR, I contend that the landscape of data protection has shifted in the last two decades. Previously, data protection strategies were primarily the responsibility of internal technology business units. However, contemporary data protection strategies require collaboration from a range of organisational departments, such as cybersecurity, legal, change management, procurement, and finance. The implementation of effective data protection measures is no longer solely dependent on internal technological business units, but also involves external collaborations. Therefore, it is crucial to establish ongoing dialogues between various stakeholders, either informally, with consideration of independent input, or more formally through the establishment of privacy, security, and data protection steering groups.

As society progresses towards the era of big data and AI, organisations are faced with the formidable challenge of safeguarding both personal and confidential information. Striking the right balance between data access and security proves to be a challenging task for several reasons. As demonstrated by the global lockdown imposed by the COVID-19 pandemic, while social networking and collaboration tools offer new opportunities, their improper use can lead to serious risks. In a globalised economy, knowledge workers are more likely to share information, resulting in increased vulnerability to information security

²⁶² Ann Cavoukian, Scott Taylor and Martin E Abrams, 'Privacy by Design: Essential for Organisational Accountability and Strong Business Practices' (2010) 3 *Identity in the Information Society* 405.

breaches. Additionally, organisational boundaries are becoming increasingly fluid, making it difficult to discern how, where, and by whom personal data is stored, managed, and accessed.

PbDD is often perceived as being limited to two domains of business operations, namely, business processes and practices, and physical and networked IT infrastructure (including cloud infrastructure). However, it is worth noting that PbDD can be leveraged to safeguard personal information in any format. Its application is not limited to digital data processing and is particularly critical for the processing of special category data (e.g., health data). In fact, PbDD can be applied to all forms of data processing, including paper-based record systems. Hence, the implementation of PbDD can benefit organisations across different industries and sectors by providing an overarching framework to ensure that privacy and data protection is embedded into all aspects of their operations, regardless of the format of data processing.

In today's business landscape, where maintaining regulatory compliance, avoiding legal liability, and mitigating reputational damage are of utmost importance, providing security and privacy throughout the data lifecycle (from collection to disposal) has become crucial. PbDD has emerged as a valuable tool for organisations seeking to reduce the likelihood of privacy violations and the resulting fines and penalties, as well as financial losses or legal liabilities. By incorporating PbDD into their personal data development workflows, organisations can improve their products, policies, and practices, and foster a culture of privacy throughout the company. This, in turn, can enhance the privacy of data subjects, improve the reputation of the organisation, and reduce the risk of non-compliance.

In this chapter, my aim is to scrutinise the connection between data protection principles and PbDD, a domain that is identified in the literature as having various gaps and deficiencies. Moreover, the analyses of fines issued by supervisory authorities undertaken in this study, revealed that non-compliance with the general data processing principles is the primary cause that prompts supervisory authorities to enforce fines on organisations. Given the significance of this issue, it is crucial to explore and identify effective strategies that organisations can employ to ensure compliance with these principles and to avoid incurring fines. My primary focus is thus to explore the feasibility of integrating these principles into contemporary business processes, while outlining the advantages and drawbacks of PbDD as a mechanism for achieving GDPR operationalisation. Additionally, this chapter seeks to examine the main constraints posed by the Regulation in relation to PbDD implementation.

4.1. An investigation into the (practical) application of the PbDD theory in the context of the GDPR

In contemporary discourse, it is widely accepted that the practical and effective implementation of a GDPR compliance programme relies on an organisation's ability to incorporate PbDD principles into its operations, as well as its technical and organisational capacity to establish robust mechanisms for safeguarding individuals' rights in all aspects of its activities. However, in my opinion, PbDD should not be considered a one-size-fits-all solution for achieving GDPR compliance. The efficacy of PbDD is contingent on additional underlying mechanisms such as privacy management tools (PMTs), which support data protection governance, and privacy enhancement technologies (PETs), which ensure that

optimal privacy and data protection measures are instituted in the context of today's intricate business and technology landscapes.

In light of the foregoing, I argue in favour of the EU legislator who decided to combine 'data protection by design' and 'data protection by default', insofar as Cavoukian's PbD framework, while adequate for the state of technological development in the 1990s, is incapable of meeting the challenges posed by contemporary technology on its own,²⁶³ particularly when one considers the considerable amounts of data being collected, stored or otherwise processed by private and public organisations and the increased (and novel) risks that these new technologies pose to the rights and freedoms of individuals.²⁶⁴ Such risks go far beyond the data security risk that PbD sought to address in the 1990s - such as the early concerns of theft and misuse of personal information online; a concern sometimes referred to as 'the privacy-security dichotomy.'²⁶⁵

I posit that, relying solely on technological means to ensure privacy (such as attempting to prevent data breaches within data infrastructures), does not seem to lead to a model that is suitable for adequately address the data protection concerns of the legislator when drafting the GDPR. A comprehensive data protection compliance framework, translated into a structured strategy for aggregating, harmonising, and

²⁶³ I allude to state-of-the-art and emerging technologies, including but not limited to cryptocurrency, blockchain, autonomous vehicles, unmanned aerial vehicles, biometrics, implanted human chip technology, robotics, IoT technology, targeted advertising, and others.

²⁶⁴ The controller bears the responsibility of evaluating the risk and determining the suitable level of security to be implemented for the processing activity, as stipulated under Article 32(2) of GDPR. The evaluation of an appropriate level of security must be conducted with due consideration to the potential hazards arising from processing, notably those arising from inadvertent, unlawful, or unauthorised (i) destruction; (ii) loss; (iii) modification; (iv) disclosure; and (v) access to personal data.

²⁶⁵ The privacy-security dichotomy demonstrates the importance of striking a balance between the privacy of the individual and the security of data as a whole. See, Don Tapscott, 'False Dichotomy: Privacy Isn't Always at Odds with Security' (2003) 6 *Intelligent enterprise* (San Mateo, Calif.) 12. 'We don't need to trade off privacy to have security. They are two sides of the same coin, and we need both for a just society.'

implementing GDPR requirements and data governance best practise standards, is necessary for a successful implementation of PbDD and thus achieving GDPR compliance.²⁶⁶ The UK's Information Commissioner's Office (ICO) stresses the importance of the implementation of the principles relating to processing of personal data, as follows:

'The principles lie at the heart of the GDPR. They are set out right at the start of the legislation and inform everything that follows. They don't give hard and fast rules, but rather embody the spirit of the general data protection regime - and as such there are very limited exceptions. Compliance with the spirit of these principles is therefore a fundamental building block for good data protection practice. It is also key to effective compliance with the detailed provisions of the GDPR.'²⁶⁷

Therefore, the data protection principles serve as the foundation for operational standards that not only preserve the integrity, confidentiality, and availability of personal data, but also set the tone for processing policies that respect the rights, freedoms, and dignity of the individuals with whom an organisation interacts and whose data it processes.

As there appears to be no previous studies on the "operationalisation" of data protection principles, as well as the critical role played by PbDD in their implementation into organisations' systems and processes, this topic represents a new domain with largely

²⁶⁶ This study provides conclusive evidence that organisations may achieve a reasonable level of compliance maturity by adopting a simple "principles" approach to data security and protection if their efforts are mainly focused on implementing the seven data protection principles via PbDD.

²⁶⁷ Information Commissioner's Office, 'The Principles' (*Guide to the General Data Protection Regulation (GDPR)*) <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/>>.

untapped potential, which I would like to begin paving the way for. As a result, I will now summarise each of the seven data protection principles provided in Article 5 of the GDPR, not only to place the principles in the context of PbDD, but also to help understanding how they may be incorporated into businesses' systems and processes.

4.1.1. Overview of the principles of lawfulness, fairness, and transparency underpinning PbDD

The GDPR is not a Rules-Based Regulation (RBR) but a Principles-Based Regulation (PBR), and data protection law is not the only regulatory field that has had to grapple with this concept; PBR is a regulatory model used, for example, in the financial and communications sectors.²⁶⁸ Under the GDPR, the principles of lawfulness, fairness and transparency apply to any processing activity involving the processing of personal data.²⁶⁹ The Data Protection Directive (DPD),²⁷⁰ already included in Article 6(1)(a) a requirement for data to be processed 'fairly and lawfully', the GDPR adds the transparency requirement; personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject. This change imposes an additional obligation on data controllers, not only by requiring them to take greater care in the design and implementation of their data processing systems and activities, but also by requiring them to implement appropriate measures to ensure the application of those principles "in practice."

²⁶⁸For a synopsis of Principles Based Regulation see, Julia Black, 'Principles Based Regulation: Risks, Challenges and Opportunities' (Sydney, Australia, 28 March 2007) <<http://eprints.lse.ac.uk/62814/>>.

²⁶⁹ GDPR, Article 5(1)(a).

²⁷⁰ Directive 95/46/EC.

I contend that compliance mechanisms must be devised and integrated into the organisation's PbDD programme as operational actions to ensure that the principles of data protection are incorporated at the earliest stage of data processing and upheld throughout the entire life cycle of personal data processing. The significance of organisational transparency in data processing is a key aspect of the GDPR principles,²⁷¹ data controllers must be forthcoming with data subjects about their identity and data processing activities, even when they do not have a direct relationship with the individual.²⁷²

Against this backdrop, I will now undertake an extensive analysis of several critical considerations pertaining to PbDD. Through this exploration, I will delve into the nuances and complexities surrounding each of these issues, providing a rigorous and systematic examination of their importance in upholding the principles of data protection.

²⁷¹ Under the GDPR, transparency is explicitly recognised as a core principle governing the processing of personal data. Article 5(1)(a) requires that personal data be processed lawfully, fairly, and transparently in relation to the data subject. Article 12 mandates that data controllers provide transparent information, communication, and modalities for the exercise of data subject rights. The significance of organisational transparency in data processing has been reinforced through case law from the ECJ. For example, in the case of *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (C-131/12)*, the ECJ ruled that search engine operators are data controllers and must comply with data protection principles, including transparency obligations. The court emphasised the importance of providing transparent information to data subjects about the processing of their personal data, particularly in the context of online data processing activities. Furthermore, in the case of *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV (C-40/17)*, the ECJ clarified the responsibilities of joint controllers in ensuring transparency in data processing. The court held that joint controllers are jointly responsible for providing transparent information to data subjects, including the identity of each controller and the purposes of data processing.

²⁷² This presents a significant PbDD task, as it requires the implementation of both TOMs to effectively integrate these information requirements into an organisation's business-as-usual (BAU) processing operations. In addition, it is important to identify PbDD operational actions. These may include the adoption of DPIAs to identify and mitigate data protection risks, the implementation of privacy-enhancing technologies (PETs) to bolster data security and minimise data breaches, and the development of data retention policies to ensure compliance with storage limitation requirements. Moreover, data controllers must ensure that their PbDD programme is designed to accommodate future technological advancements and evolving regulatory requirements to ensure continued adherence to data protection principles.

4.1.2. Interrelationships of the lawfulness principle: the rights of data subjects

Lawful processing²⁷³ of personal data implies obtaining the consent of the data subject,²⁷⁴ unless such processing can be based on another legal basis listed in GDPR,²⁷⁵ namely, the engagement is based on a contract that requires the processing of personal data; personal data processing is necessary for compliance with a legal obligation of the data controller; vital interests of the data subject or of another person require the processing of their personal data; processing is necessary for the execution of a task in the public interest; the legitimate interests²⁷⁶ of controllers or third parties are the reason for processing (but only if they are not overridden by the data subjects' interests or fundamental rights).²⁷⁷

²⁷³ The principle of lawfulness ensures that individuals possess a clear understanding of the reasons behind the processing of their data, providing a legal framework to protect their rights and privacy. Compliance with this principle is fundamental to the overarching objective of the GDPR – safeguarding the rights and freedoms of individuals concerning the processing of their personal data in a lawful and transparent manner. Organisations must demonstrate accountability not only by complying with the principle of lawfulness but also by maintaining records of their data processing activities and making this information available to relevant authorities.

²⁷⁴ See *Case T-259/03 Kalliopi Nikolaou v Commission of the European Communities EU:T:2007:254* 206. 'Under Article 5 of Regulation 45/2001, the leak constitutes unlawful processing because *it was not authorized by the data subject*, not necessary under the other sub-paragraphs and it did not result from a decision by OLAF. No concrete showing was made of an internal system of control to prevent leaks or that the information in question had been treated in a manner that would guarantee its confidentiality.' 206-209. (emphasis added).

²⁷⁵ See *Joined cases C-465/00, C-138/01 and C-139/01 Österreichischer Rundfunk and Others EU:C:2003:294, [2003] ECR I-04989* para. 65, 00. See also, *Case C-524/06 Heinz Huber v Bundesrepublik Deutschland EU:C:2008:724, [2008] ECR I-09705*. Para. 48.; *Joined cases C-468/10 and C-469/10 Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECMD) v Administración del Estado EU:C:2011:777* para. 26, 10.

²⁷⁶ To be legitimate, the processing must respect the appropriate balance between the interests of the controller and the interests of the data subject. See, Article 29 Working Party, 'Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC' (2014) <<https://ec.europa.eu/newsroom/article29/news-overview.cfm>>.

²⁷⁷ GDPR, Article 6.

Legal Basis for processing	Consent Art. 6(1)(a)	Contract Art. 6(1)(b)	Legal obligation Art. 6(1) €	Vital interests Art. 6(1)(d)	Public interest/functions Art. 6(1)(e)	Legitimate interests Art. 6(1)(f)
Data Subjects Rights						
Access (Art 15 GDPR)	✓	✓	✓	✓	✓	✓
Rectification (Art 16 GDPR)	✓	✓	✓	✓	✓	✓
Erasure (Art 17 GDPR)	✓					✓
Restriction of processing (Art 18 GDPR)	✓	✓	✓	✓	✓	✓
Data portability (Art 20 GDPR)	✓	✓				
Object (Art 21 GDPR)					✓	✓
Automated individual decision making, including profiling (Art 22 GDPR)				✓	✓	✓

Table 1 - Legal Bases for Processing vs. Data Subject's Rights

As evidenced by the correlation table presented above (Table 2), the selection of a specific legal basis may correspond with distinct rights and obligations, which may impact the processing operations undertaken by the organisation. Regarding the processing of special categories of personal data, it is crucial to note that such processing is only lawful if it meets the prerequisites outlined in Article 6 of the GDPR and one of the ten specific conditions enumerated in Article 9 of the GDPR. Additionally, the rights of data subjects are thoroughly elucidated in Chapter III of the GDPR, which spans from Articles 12 to 23 of the GDPR.

The subsequent overview pertaining to the rights of data subjects concisely outlines the duties of data controllers, serving as an essential component of PbDD implementation. It is imperative to grasp the operational intricacies of these rights within the ambit of GDPR conformity. While the practical implementation of these considerations will be discussed

in detail in the DPPA, introducing them at this stage can help contextualise the rights of data subjects within their appropriate framework.

3.1.2.1. The right to be informed

The GDPR outlines the information that must be provided to data subjects by data controllers.²⁷⁸ This requirement can be met in a variety of ways, including by PbDD actions, such as posting a (public) privacy notice on the organisation's website that includes the following information: (i) the identity and contact details of the data controller, and the data protection officer where relevant, (ii) the purpose of the processing and its legal basis, (iii) the recipient of data or categories of recipients, (iv) the existence of the data subject rights, (v) the right to withdraw consent at any time, (vi) the right to lodge a complaint with the supervisory authority, (vii) information about retention periods, (viii) information about the existence of automated decision-making, including profiling and information about how decisions are made, their significance and consequences, and (ix) details of transfers to countries outside the EU and safeguards applied to such transfers. In adherence to GDPR, it is mandatory to implement appropriate measures to ensure that the information provided is transparent, understandable, and easily accessible. Accordingly, the data controller bears the responsibility of presenting the information in clear and concise language, especially when the target audience comprises minors.²⁷⁹

²⁷⁸ Please note that a public entity cannot transmit personal data to another state agency for further processing without the data subject being informed of such processing (transfer of personal data). See, *Case C-201/14 Smaranda Bara and Others v Presedintele Casei Nationale de Asigurari de Sanatate and Others (Third Chamber) EU:C:2015:638*.

²⁷⁹ GDPR, Recital 58.

3.1.2.2. The right of access

The selected PbDD mechanism must guarantee prompt delivery of information to data subjects,²⁸⁰ no later than one month after the request (with a possible extension of two months if the request is complex or voluminous), in line with GDPR. Unless a subject access request ('SAR') is manifestly unreasonable or excessive, data subjects are exempt from any associated fees. Nevertheless, a clear-cut classification of what entails an unreasonable, excessive, or reasonable fee remains absent from GDPR guidance, and it falls on the data controller to discern which category a specific request falls under. Although data controllers may refuse to comply with an unreasonable or unfounded request, they have an obligation to clarify their position to the data subject and notify them of their option to lodge a complaint with the supervisory authority and pursue legal redress if dissatisfied with the outcome.

3.1.2.3. The right of rectification

The right of data subjects to have their incomplete or inaccurate data rectified²⁸¹ is another crucial aspect of PbDD implementation. The protocol employed to handle such inquiries must conform to a transparent decision-making process, wherein data controllers are mandated to respond within a month, which includes the requisite time to inform third parties who may have obtained the data. If the inquiry is intricate, the deadline may be

²⁸⁰ See *Rijkeboer [2009]* (n 93). para. 54. The right of access is necessary to enable the data subject to exercise his other rights (rectification, blocking, erasure, and notify recipients of same; object to processing or request damages). The right must of necessity relate to the past, otherwise the data subject would not be in a position effectively to exercise his right to have data presumed unlawful or incorrect rectified, erased or blocked or to bring legal proceedings and obtain compensation for damages.

²⁸¹ See, *Schrems [2015]* (n 211). para. 95. 'Legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter.'

extended by an additional two months. In the event that the controller declines the rectification request, they must provide the data subject with a detailed explanation and inform them of their entitlement to register a complaint with the supervisory authority or seek judicial remedy.

3.1.2.4. The right of erasure ('right to be forgotten')

If personal data has fulfilled its intended purpose and is no longer necessary, the data subject may initiate a request for its erasure. This right extends to Article 17 of the GDPR, enabling the data subject to request removal from search engines,²⁸² which is also applicable to controllers who have replicated the data on the internet.²⁸³ Nonetheless, a data controller may withhold acceptance with a request for erasure where processing is indispensable for (i) public interest, (ii) health or social care objectives, or (iii) public health purposes in the public interest.²⁸⁴

3.1.2.5. The right to restrict processing

Data subjects are entitled to demand that a data controller halt the processing of their data, in circumstances such as: (i) the data subject contests the accuracy of the data for a period while the controller verifies the accuracy of the data; (ii) the processing is unlawful,

²⁸² The criteria for requesting the removal of personal data from search engine results are contingent upon certain conditions that must be fulfilled in order for the request to be considered valid. These conditions include the following: data being no longer relevant, outdated, or inaccurate; the data subject withdrawing consent; unlawful processing; or the completion of the processing purpose.

²⁸³ This includes the right to request "delisting" in search engines pursuant Article 17 GDPR, therefore, also applies to controllers that replicate the information. See, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González* (2014) (n 69).

²⁸⁴ However, when the disclosure of information is required by law, to ensure legal certainty, the request to delete personal information from a public registry may be denied. See *Case C-398/15 Salavatori Manni v Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce* EU:C:2017:197.

and the data subject requests restriction as opposed to erasure; (iii) the data controller no longer requires the personal data, but the data subject needs it to establish, exercise, or defend legal claims; and (iv) the data subject objects to the data processing necessary for a public interest task or for purposes of legitimate interests, and the controller is considering whether the organisation's legitimate interests override those of the individual (conducting a balancing exercise). Consequently, a PbDD mechanism must be instituted to enable data controllers to retain the personal data without further processing it following a request for restriction of processing. The DPPA, for instance, recommends implementing a mechanism to assist data controllers in retaining personal data without conducting additional processing after receiving a request for processing restriction. This involves proactively integrating privacy measures into the design of systems and processes from the outset. In practical terms, when designing data processing systems, the chosen mechanism must incorporate features that automatically initiate a restriction on further processing when a data subject exercises their right to restrict processing, using automation to enforce these restrictions. Once a request for processing restriction is initiated, the PbDD mechanism employs automated protocols to cease any additional processing of the personal data in question. Essentially, the proposed PbDD mechanism ensures that the right to restrict processing is not an isolated event but an integral aspect of the system's design, promoting a holistic and automated approach to data protection. This aligns with the PbDD philosophy of embedding privacy considerations at the core of technological processes. The PbDD plan should also define procedures for receiving and evaluating

requests for processing restriction and informing the data subject if a decision is made to lift a processing restriction.²⁸⁵

3.1.5.6. The right to object

Despite a data controller's belief that the processing of personal data is lawful, a data subject retains the right to object. Such an objection must be grounded in the data subject's individual circumstances.²⁸⁶ It is noteworthy that the PbDD mechanism employed to address a data subject's request should incorporate the ability to suspend and resume any processing activities associated with their personal data. Unless the controller can establish compelling legitimate grounds that supersede the individual's interests, rights, and freedoms, or the processing is indispensable for the purpose of exercising, establishing, or defending a legal claim, they are obligated to halt the processing of personal data.

3.1.2.7. Rights related to automated decision making and profiling

Individuals have the right not to be subjected to a decision based on automated processing that has a legal effect on them or affects them significantly in some other way.²⁸⁷ It is important to note that automated decisions can be made with or without profiling, and that profiling can also occur in the absence of an automated decision. To ensure effective

²⁸⁵ Under Article 19 GDPR, this obligation does not apply if the controller proves impossible or involves disproportionate effort. Efforts to be disproportionate should be evaluated in terms of time, cost, and manpower. See, *Case C-582/14 Patrick Breyer v Bundesrepublik Deutschland (Request for a preliminary ruling from the Bundesgerichtshof (Germany))* EU:C:2016:779.

²⁸⁶ In general, the rights of the data subject take precedence over the controller's economic interests, depending on the nature of the information and its sensitivity to the data subject's private life, as well as the public's interest in obtaining that information. See, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (2014)* (n 69).

²⁸⁷ The definition of profiling is provided in Article 4(4) of the GDPR.

compliance with the principle of lawfulness, organisations may need to refrain from conducting some data processing activities that involve automated decision making and profiling, for example, in cases where aspects of health data need to be processed.²⁸⁸ In this area the GDPR clearly ‘attempts to draw a line between the spheres of health research and the market’²⁸⁹ by limiting the processing only to cases where the protection of individual’s fundamental rights is adequately guaranteed, and to wider public interests or scientific research.²⁹⁰

My contention is that additional measures ought to be implemented, particularly in software and web development, to detect potentially illicit processing, particularly in scenarios that may result in: (i) a violation of a confidentiality obligation; (ii) infringement of copyright; (iii) a breach of an enforceable contractual obligation; (iv) contravention of sector-specific statutes or Regulations; (v) a breach of human rights; or (vi) the organisation surpasses its legal jurisdiction or exerts that authority in an inappropriate manner. In the event of illicit data processing by an organisation, the GDPR accords the rights of erasure and restriction of processing, thereby necessitating the establishment of PbDD mechanisms to enable individuals to exercise such rights, namely, the right to access personal data,²⁹¹ information,²⁹² rectification, and erasure.²⁹³

²⁸⁸ Tzanou (n 6). “[S]ensitive data, such as data revealing racial or ethnic origin, political and religious beliefs, health and sexual life, should be shielded from certain categories of processing, especially if this is undertaken for the use of the data for different purposes from the ones initially collected.”

²⁸⁹ Giulia Schneider, ‘Disentangling Health Data Networks: A Critical Analysis of Articles 9(2) and 89 GDPR’ (2019) 9 *International Data Privacy Law* 253.

²⁹⁰ GDPR, Recital 40.

²⁹¹ See, *Rijkeboer [2009]* (n 93).

²⁹² See, *Bara [2015]* (n 270).

²⁹³ See, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González* (2014) (n 69).

To conclude this summary of the interrelationships between PbDD, data protection principles and data subjects' rights, I would like to emphasise that any PbDD programme must consider as a first step the implementation of the lawfulness principle across all organisation's processing activities as well as the implementation of mechanisms to identify the lawful bases for collecting, storing, or, otherwise processing personal data, while maintaining compliance with any other areas of law.²⁹⁴ Chapters eight and nine will provide an elaboration on the practical implementation of PbDD, delineating various mechanisms that can be utilised to safeguard individuals' rights. It will also illustrate how organisations can identify the suitable measures in the context of PbDD. When these mechanisms are integrated into an organisation's PbDD plan, they serve not only as a means of enhancing operational efficiency but also as a means of ensuring compliance with the accountability principle as prescribed by Article 5(2) of the GDPR.

4.1.3. PbDD as a guarantor of the fairness principle

The GDPR also mandates that organisations process personal data in a manner that is deemed 'fair.' Essentially, the data controller must evaluate the extent to which its processing activities may impinge upon the rights and freedoms of individuals. If such an impact is likely, the data controller must be able to provide a justifiable rationale for any resultant detrimental effects. However, organisations should limit the processing of personal data to activities that data subjects can reasonably anticipate, or when they can

²⁹⁴ The DPPA serves as a framework that harmonises with data protection principles, respects and promotes data subjects' rights, enhances transparency and user control, and contributes to overall risk reduction and regulatory compliance. The integration of PbDD principles into data processing practices reflects a commitment to a privacy-conscious and ethically sound approach to information management.

explain why an eventual unexpected processing of personal data is necessary and justified. A crucial aspect of upholding 'fairness' pertains to data collection, whereby personal data must not be acquired through deceptive or misleading practices. Controllers should also respect, as far as it is possible, the wishes of the data subject,²⁹⁵ particularly in situations where consent is used as the legal basis for processing.²⁹⁶ Processing personal data should not be conducted surreptitiously, and individuals must be apprised of the potential risks associated with such processing, as well as the safeguards put in place.

In my estimation, this presents one of the most notable inconsistencies in PbDD, as per Cavoukian's full-functionality principle:

'Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Privacy by Design avoids the pretence of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.'²⁹⁷

In my assessment, implementing such a model in the realm of data protection law is impractical. This is largely due to factors such as organisational bias, which is often driven by robust economic considerations, as well as the ostrich effect²⁹⁸ - wherein executives tend to disregard pertinent issues to evade negative impacts on their business. For

²⁹⁵ *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González* (2014) (n 69).

²⁹⁶ *K.H. and Others* (2009) (n 91).

²⁹⁷ Ann Cavoukian, 'Privacy by Design: The 7 Foundational Principles' (Information and Privacy Commissioner of Ontario 2010) 1.

²⁹⁸ See, Dan Galai and Orly Sade, 'The "Ostrich Effect" and the Relationship between the Liquidity and the Yields of Financial Assets' (2006) 79 *The Journal of Business* 2741. 'The ostrich effect is defined as avoiding apparently risky financial situations by pretending they do not exist.'

instance, consider a marketing campaign intended to increase sales by a specific percentage, which persists despite the absence of data subject consent for such processing activity. Moreover, organisations frequently face challenges in reconciling their interests with fundamental rights.²⁹⁹

Gianclaudio Malgieri, suggests that ‘the best interpretation of the fairness principle (taking into account both the notion of procedural fairness and of fair balancing) is the mitigation of data subjects' vulnerabilities through specific safeguards and measures’³⁰⁰ which means, through the implementation of TOMs. Hence, I posit the inclusion of a measure in the PbDD strategy that is not exclusively reliant on risk mitigation to protect the rights and freedoms of data subjects (a safety net). This measure, which may assume the form of an organisational policy or a specific assessment, should be integrated at the initial stages of processing. When one of the parties in a relationship is perceived as a "weak link" (as is frequently the case with the data subject in a commercial relationship), achieving a mutually beneficial outcome (win/win situation)³⁰¹ can be a challenging, if not insurmountable task.³⁰²

Attempting to strike a fair balance when individual rights and freedoms are subject to subjective and economically biased evaluations is fundamentally impossible. To buttress

²⁹⁹ *Case C-275/06 Productores de Música de España (Promusicae) v Telefonica de España* EU:C:2008:54, [2008] ECR I-271. See also, *Case C-557/07 Lsg-Gesellschaft Zur Wahrnehmung Von Leistungsschutzrechten GmbH V Tele2 Telecommunication GmbH* EU:C:2009:107.; *Scarlet* [2011] (n 39).

³⁰⁰ Gianclaudio Malgieri, ‘The Concept of Fairness in the GDPR: A Linguistic and Contextual Interpretation’, *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency* (Association for Computing Machinery 2020) <<https://doi.org/10.1145/3351095.3372868>>.

³⁰¹ The ‘win-win’ proposition here is based on controller’s goals vs. privacy.

³⁰² The ‘full functionality’ paradox implies that evaluating the magnitude of the detrimental effect that a processing activity may have on a data subject is an impossible undertaking that cannot be resolved through risk assessment only. In my perspective, any trade-offs made in relation to privacy matters are merely superfluous tactics designed to surmount barriers to data processing, without serving any discernible purpose in safeguarding the rights and freedoms of data subjects.

my assertion, it is worth noting that when evaluating the interests of the search engine, the CJEU in the *Google Spain* case at para. 81, noted that ‘these are economic interest, which cannot justify the potential seriousness of the interference with the data subject’s rights.’³⁰³ In my perspective, it is of paramount importance to re-evaluate the full-functionality principle (or paradox) enshrined in the PbDD concept, and for the legislature to establish clear boundaries as to the extent to which a risk-based approach can determine the ‘fairness’ of a processing activity that detrimentally impacts the rights and freedoms of the affected individuals.

4.1.4. A lever for PbDD implementation: the purpose limitation principle

The principle of purpose limitation constitutes a fundamental tenet of the GDPR and is inherently intertwined with data protection concepts such as transparency and individuals’ control. Given that ‘the individual must be the one who determines the fate of his or her personal information,’³⁰⁴ the purpose of processing should be established prior to the commencement of personal data processing: ‘if the purpose of processing is sufficiently specific and clear, individuals know what to expect and transparency and legal certainty are enhanced.’³⁰⁵ Furthermore, having a clear understanding of the processing purpose

³⁰³ *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González* (2014) (n 69). para. 81.

³⁰⁴ Ann Cavoukian, ‘Global Privacy and Security, by Design: Turning the “Privacy vs. Security” Paradigm on Its Head’ (2017) 7 *Health and technology* 329.

³⁰⁵ European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law* (2018 Edn, Publications Office of the European Union). 122.

facilitates data subjects in more effectively exercising their data protection rights, particularly the right to object to processing.³⁰⁶

The purpose limitation principle represents a crucial "lever" when devising the organisational PbDD implementation plan, as it establishes a significant premise: the processing of personal data is permissible only if the data are 'collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.'³⁰⁷ To note that GDPR also identifies compatible purposes as those for 'archiving purposes in the public interest, scientific or historical research purposes or statistical purposes' when in accordance with Article 89(1).³⁰⁸

The Article 29 Data Protection Working Party ('WP29') has published its 'Opinion 03/2013 on purpose limitation'³⁰⁹ with reference to the DPD. The WP29 Opinion comprehensively explains and interprets the various components of this principle via multiple examples and practical guidance, encompassing valid notices, consents, and compatible use. WP29 underscores that purposes must be: a) Specific – precisely and fully identified prior to, and in any event, no later than the point at which personal data is collected; b) Explicit - clearly explained or expressed in a straightforward manner; and c) Legitimate - which extends to other areas of law and must be interpreted within the context of the data processing.

Of particular relevance to the practical implementation of PbDD in business systems and processes is WP29's assertion that any additional processing of personal data that is

³⁰⁶ WP 29, 'Opinion 03/2013 on Purpose Limitation' (2013) 00569/13/EN WP 203.

³⁰⁷ GDPR, Article 5(1)(b).

³⁰⁸ *ibid.*

³⁰⁹ WP 29 (n 298) 20.

inconsistent with the stated purposes of collection is illegal and therefore forbidden. Consequently, stringent controls over the utilisation and reuse of personal data should be deeply ingrained in all processing activities. The compatibility of purposes must be determined on a case-by-case basis, taking into account the following criteria: (i) 'the relationship between the purposes for which the personal data have been collected and the purposes of further processing'; (ii) 'the context in which the personal data have been collected and the reasonable expectations of the data subjects as to their further use'; (iii) 'the nature of the personal data and the impact of the further processing on the data subjects'; and (iv) 'the safeguards adopted by the controller to ensure fair processing and to prevent any undue impact on the data subjects'.^{310,311}

4.1.5. PbDD enables information rights: the new principle of transparency in context

The new principle of transparency mandates that the controller establishes effective mechanisms to ensure that data subjects are informed about how their personal data is being processed.³¹² At the first point of collection of personal data, the data controller ought to inform data subjects that any processing will be conducted lawfully and in a transparent manner,³¹³ while also respecting the rights of the data subjects. Transparency refers to (a) the communication given to data subjects before any form of data processing

³¹⁰ WP 29 (n 298).

³¹¹ In the context of processing involving 'Big Data', WP29 recommends the implementation of supplementary TOMs, such as ensuring the functional separation of personal data processing (e.g., pseudonymisation), ensuring the confidentiality and security of the data (e.g., incorporating firewalls in the data processing systems), and acquiring informed individual consent (e.g., opt-in in the case of profiling for targeted and location-based marketing or analogous activities).

³¹² GDPR, Article 12.

³¹³ In accordance with Article 13(2) GDPR.

starts,³¹⁴ (b) the information provided during the processing of their data,³¹⁵ and (c) the information provided by the controller following a request of access to their data (subject access request, “SAR”).³¹⁶ With regards to the principle of transparency, the guidelines on transparency issued by WP29 under Regulation 2016/679 clarifies:

‘Transparency is a long established feature of the law of the EU. It is about engendering trust in the processes which affect the citizen by enabling them to understand, and if necessary, challenge those processes. It is also an expression of the principle of fairness in relation to the processing of personal data expressed in Article 8 of the Charter of Fundamental Rights of the European Union. Under the GDPR (Article 5(1)(a), in addition to the requirements that data must be processed lawfully and fairly, transparency is now included as a fundamental aspect of these principles. Transparency is intrinsically linked to fairness and the new principle of accountability under the GDPR. It also follows from Article 5.2 that the controller must be able to demonstrate that personal data are processed in a transparent manner in relation to the data subject.’³¹⁷

As previously discussed, the GDPR sets forth the information that data controllers are required to provide to data subjects. This obligation may be fulfilled by providing a privacy statement (on the website), incorporating the particulars outlined in 3.1.2.1 (the right to be informed). The PbDD mechanism addressing processing transparency must, at a

³¹⁴ GDPR, Articles 13 and 14.

³¹⁵ For guidance on what information to provide to data subjects, see WP29, ‘Opinion 2/2017 on Data Processing at Work’ (Article 29 Data Protection Working Party 2017) WP 249.

³¹⁶ GDPR, Article 15.

³¹⁷ Article 29 Data Protection Working Party, ‘Guidelines on Transparency under Regulation 2016/679’ 17/EN WP260.

minimum, ensure that the information disseminated to data subjects is concise, transparent, understandable, and easily accessible.³¹⁸

4.1.6. Data minimisation: PbDD's most powerful ally in achieving GDPR compliance

The principle of data minimisation,³¹⁹ strengthened by the GDPR, determines that data collected and processed should not be stored or further processed unless it is necessary for reasons that have been clearly stated in advance to such processing. The principle of data minimisation also presents a model for organisations to ensure and preserve individuals' trust, while simultaneously mitigating the risks of unauthorised access, data loss incidents, and other security threats. When an organisation puts the principle of data minimisation into practice in a practical scenario, it entails using only the minimal amount of personal data essential for the specific purpose of the processing activity. If a PbDD programme effectively integrates the data minimisation principle into an organisation's processing operations, the security of the processed data, and, as a result, the protection of data subjects' rights and freedoms, is already halfway achieved.³²⁰

A key tenet of the data minimisation principle, which triggers a specific PbDD mechanism, is that processing of personal data should be solely limited to what is strictly necessary to accomplish a legitimate purpose, and only in situations where the purpose of

³¹⁸ It is noteworthy that EU supervisory authorities have imposed significant fines amounting to €237,002,595 as of January 2023, for insufficient fulfilment of information obligations. According to the analysis of fines conducted in this study, this type of violation is ranked third in terms of the number of fines levied.

³¹⁹ Personal data should be processed only if the purpose could not reasonably be fulfilled by other means. See Recital 39 GDPR.

³²⁰ This statement may appear overstated, but it emphasises the importance of the data minimisation principle for a 'fast' PbDD deployment.

the processing cannot be achieved otherwise. From an operational point of view, the elements of personal data collected or otherwise processed must be limited to those necessary to achieve the objectives of the processing operation.³²¹ Controllers must periodically review their processing activities³²² to ascertain that the personal data they hold is still relevant and adequate for the purposes it was originally collected and delete any data element no longer needed, in accordance with the principles of accuracy and storage limitation, both of which are summarised below.

4.1.7. To what degree does PbDD ensure the accuracy of data?

In all processing operations, data controllers must take appropriate measures to ensure that the personal data they hold, or otherwise process, 'is not incorrect or misleading as to any matter of fact.'³²³ To ensure compliance with the GDPR, organisations must have mechanisms in place to promptly rectify or erase any inaccurate personal data. This necessitates periodic reviews of the processed data for inaccuracies and subsequent updates. However, it is essential to consider the purpose of personal data processing, as there may be instances where lawful alteration of data can be construed as unlawful, such

³²¹ See, *Digital Rights Ireland [2014]* (n 98). The ends (for processing) do not justify the means; frequently, regulations pursue honourable and genuine interests (e.g., Data Retention Directive, fight against serious crime) and this could be considered as fulfilling an objective of general interest. However, whenever a measure covers, in a generalized fashion, 'all individuals and all means of electronic communications as well as all traffic data without any differentiation, limitation or exception [...] in the light of the objective' it compromises the principle of data minimisation, and thus, is invalid. (emphasis added)

³²² In this context, PbDD assumes a crucial role; the assimilation of the three data standard principles, (i.e., data minimisation, storage limitation, and accuracy), into an organisation's systems and processing operations is an essential aspect of any PbDD strategy. It is imperative that these aspects are addressed during the early stages of data processing design to ensure comprehensive data protection.

³²³ ICO, 'Principle (d): Accuracy' (17 October 2022) <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/>>.

as in the case of academic registers or medical records where the purpose of data storage is to register an event for retrospective memory. Hence, it is imperative that the PbDD plan takes into account the lawful basis for processing personal data and ensures that any updates or alterations to the data are carried out in accordance with the purpose of processing and the applicable legal requirements.

Data subjects are entitled to request that organisations rectify inaccurate data about them or delete incomplete or inaccurate information.³²⁴ Therefore, it must anticipate and concretely outline the necessary steps to ensure the accuracy of information, including identifying and correcting inaccurate data in a timely manner. This obligation is of particular importance when responding to data subjects' information rights, as it ensures that their personal data is accurate and up to date. In the *Rijkeboer* case, the CJEU stated that the 'right to privacy means that the data subject may be certain that his personal data are processed in a correct and lawful manner, that is to say, in particular, that the basic data regarding him are accurate and that they are disclosed to authorised recipients.'³²⁵

4.1.8. Storage limitation: the most significant challenge for PbDD?

Personal data must be 'kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed'.³²⁶ To

³²⁴ In order to comply with data subjects' rights, a PbDD programme must not only focus on preventing the creation of inaccurate data but also address the issue of already existing inaccurate data.

³²⁵ *Rijkeboer* [2009] (n 93).

³²⁶ GDPR, Article 5(1)(e).

ensure compliance with the storage limitation principle, a PbDD mechanism should be implemented that allows for the regular review and deletion of personal data that is no longer necessary for the purposes for which it was collected. This requires a clear understanding of the purpose for which each type of personal data is collected, as well as any relevant legal requirements or business needs for retaining the data. By regularly reviewing and deleting unnecessary personal data, organisations can minimise the risk of data breaches, unauthorised access, and other security threats, while also upholding the rights and freedoms of data subjects. It is essential that the PbDD plan includes clear procedures and processes for reviewing and deleting personal data, as well as ensuring that any retention periods are clearly documented and regularly reviewed to ensure compliance with GDPR requirements.³²⁷ In *S. and Marper*, the ECtHR found that data retention should be proportionate to the purpose for which it was collected, and that further processing should be limited in time.³²⁸

As previously discussed, the regular review of data sets enables organisations to effectively manage their personal data, enabling them to erase or anonymise unnecessary data. This practice reduces the risk of data becoming irrelevant, excessive, inaccurate, or out of date, thus ensuring compliance with the data minimisation and accuracy principles. Additionally, this approach enhances an organisation's ability to respond to individuals' information requests under the GDPR, thereby improving their overall data management practices.³²⁹ Regrettably, numerous organisations possess substantial amounts of

³²⁷ See Recital 39 GDPR.

³²⁸ *S and Marper v the United Kingdom (2008) ECHR 1581* (n 30).

³²⁹ ICO, 'Principle (e): Storage Limitation' (*Guide to the General Data Protection Regulation (GDPR)*) <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/>>.

unstructured and unclassified legacy data, which is progressively emerging as a constraining element in their GDPR compliance endeavours. Olly Jackson argues that organisations 'are struggling to consolidate unstructured data (...)'³³⁰ and 'companies either don't understand or are surprised by the amount of unnecessary data they hold, which provides a big risk and increases the chances of a data breach.'³³¹

Presently, there are few affordable tools available in this domain that can effectively fulfil the practical data retention requirements. An example of a tool providing interpretive 'AI Technology for Data Detection and Classification' is MinerEye, which technology promises to continually track data, regardless of its form or location inside the organisation's data ecosystem. This tool claims that sensitive data can be mapped and secured according to data protection and compliance Regulations including GDPR, HIPPA, PCI-DSS, and SOC2.³³²

I argue that an approach that is less dependent on 'loose technology' could potentially offer a more cost-effective and efficacious solution to address this compliance issue. One such approach is to adopt a zero-risk policy towards unstructured data, which could be achieved through the implementation of document linking systems or customer relationship management systems (CRM). These systems can correlate unstructured data sets with structured objects. Nonetheless, as Gately suggests, this could prove to be a

³³⁰ Jackson (n 92).

³³¹ *ibid.*

³³² 'MinerEye to Demonstrate Interpretive AI Technology for Data Classification on GPUs at Nvidia's GTC Israel 2018: MinerEye Automatic Data Classification Is Critical to Unstructured Data Intensive Environments Accelerated by GPU, Including Hybrid Cloud and Data Center Storage' *PR Newswire* (New York, 15 October 2018) <<https://www.proquest.com/wire-feeds/minereye-demonstrate-interpretive-ai-technology/docview/2119923322/se-2?accountid=13460>>.

formidable task that numerous organisations currently appear to lack the capability to undertake autonomously.³³³

The storage limitation requirement is an enduring principle of European data privacy law, which has been present in various legislations. For instance, it is stipulated in Article 6 of the Directive 95/46/EC and in Article 5 (e) of the Convention 108.³³⁴ The GDPR principle of storage limitation, expressed in Article 5(1)(e) and, likewise, in Article 5(4)(e) of Modernised Convention 108,³³⁵ requires personal data to be erased (or anonymised) when their purposes have been served. This obligation evolves into an operational responsibility and must be integrated into the PbDD programme.

Data controllers must thus consider that the lawful processing of each category of data is contingent on specific business requirements, assessed in conjunction with different legal and regulatory situations that can be constructed. Such scenarios may include statutes of limitations (such as tax law or periods for litigation) or even the legitimate interests of the organisation. In *S. and Marper*,³³⁶ the ECtHR determined that unlimited retention of biodata (fingerprints, cell samples and DNA) was ‘disproportionate and unnecessary in a democratic society’ if no criminal proceedings against the applicants were in course.³³⁷ From an operational standpoint, this decision necessitates the

³³³ Edward Gately, ‘80 Percent of Companies Still Not GDPR-Compliant’ (13 June 2018) <<https://www.channelpartneronline.com/2018/07/13/80-percent-of-companies-still-not-gdpr-compliant/>>.

³³⁴ Convention 108.

³³⁵ Council of Europe, Protocol (CETS No. 223) amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) 2018 (No 223).

³³⁶ *S and Marper v the United Kingdom (2008) ECHR 1581* (n 30).

³³⁷ *ibid.*

implementation of PbDD mechanisms to ensure that any retention of personal data is proportional to its purpose of collection and time limitation.³³⁸

Nonetheless, the principle of storage limitation has always proved difficult in practical application. In the *Digital Rights Ireland* case,³³⁹ the CJEU raised the issue of the lack of objective criteria in the Data Retention Directive (DRD)³⁴⁰ on the premise that a precise period of data retention needs to be established to ensure that such period is 'limited to what is strictly necessary'. The CJEU examined the compatibility of the Data Retention Directive (DRD) with the Charter of Fundamental Rights of the European Union (CFR). The DRD intended to harmonise member-states' laws for retaining personal data processed by Internet Service Providers for eventual transfers of data to competent authorities for the prevention and prosecution of serious crime, inter alia, organised crime and terrorism. Although this was considered, *prima facie*, a purpose in the scope of 'objectives of general interest,' the generalisation given by the DRD, in which 'all individuals and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime',³⁴¹ raised the court's concerns and led to the declaration of incompatibility with Articles 7, 8 and 52 (1) of the CFR. The decision asserts that any processing activity involving personal data cannot disproportionately hinder the rights and freedoms of data subjects. Furthermore, the Court found that the DRD,

³³⁸ The ECtHR's ruling serves as a resounding warning to both public and private organisations against the indefinite retention of personal data "just in case" it may prove useful in the future.

³³⁹ *Digital Rights Ireland [2014]* (n 98).

³⁴⁰ Directive 2006/24/EC.

³⁴¹ *Digital Rights Ireland [2014]* (n 98). See, paras 51, 53, 54, 56, 57, 60, 61, 63-66, 69.

‘[E]ntails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary.’³⁴²

To address the legal issue of excessive retention of personal data, I suggest a solution involving the adoption of PbDD strategies that prioritise personal data management policies. Specifically, the implementation of PETs, such as data masking techniques (e.g., obfuscation, synthetic data generation), can assist in mitigating the risk of non-compliance with data protection principles. Additionally, organisations can leverage tools capable of archiving legacy data across the information ecosystem to facilitate the identification and removal (or anonymisation) of personal data sets, including clusters of unstructured data (such as loose text or spreadsheet files). Personal information should be retained only if it is pertinent for business, legal, or historical purposes. This is a crucial area for organisations, as one of the reasons cited by supervisory authorities for imposing significant fines³⁴³ is the controllers' lack of legal justification for storing personal data beyond the necessary duration.³⁴⁴

The GDPR recognises certain scenarios in which personal data may be retained indefinitely, such as for archiving, scientific, historical, or statistical purposes. However, it

³⁴² *ibid.*

³⁴³ Annex 1 provides a visualisation of GDPR fine statistics utilised in this work.

³⁴⁴ See, e.g., Christoph Ritzer and Natalia Filkina, ‘First Multi-Million GDPR Fine in Germany: €14.5 Million for Not Having a Proper Data Retention Schedule in Place’ (Norton Rose Fulbright LLP, Data Protection Report 2019) <<https://www.dataprotectionreport.com/2019/11/first-multi-million-gdpr-fine-in-germany-e14-5-million-for-not-having-a-proper-data-retention-schedule-in-place/>>.

is crucial to note that such retention must be accompanied by adequate safeguards, such as pseudonymisation, to protect the fundamental rights and freedoms of individuals.³⁴⁵

As complicated as embedding privacy and data protection into the design and architecture of an IT system may present, PbDD will ensure that data protection principles are embedded as an integral part of the core functionality delivered. My contention is that internal compliance challenges, such as those related to data retention and destruction, must be also thoroughly addressed by PbDD. For example, consider the challenge of implementation of the storage limitation principle into businesses systems and processing activities: currently, there are several privacy-friendly tools that allow for the discovery of personal data elements in sets of unstructured data and also in customised systems³⁴⁶ which alleviates the problem of data discovery in that ‘finding the precise location of data defined as “personal” under GDPR amongst the thousands of tables and columns (or fields) in customised systems, represents a significant challenge.’³⁴⁷ PMTs, such as “OneTrust,” offer integrated data discovery capabilities that complement their more traditional, accountability-focused tools. These typically include privacy assessment automation, data subject access management, risk management, and cookie compliance. The data discovery tool allows for the classification of personal data, the correlation of data across the organisation, the automation of access requests, and the creation of useful data mappings in accordance with the requirements of Article 30 of the GDPR for the recording of processing activities (ROPA).³⁴⁸ Furthermore, it enforces policy and technical controls such

³⁴⁵ GDPR, Recital 156.

³⁴⁶ This investigative exercise is crucial to keep a good data hygiene – where personal data is maintained accurate, up to date and relevant – and to address the requirements of Article 17 GDPR (Right to Erasure).

³⁴⁷ ‘Safyr Accelerates Personal Data Discovery in ERP & CRM Systems for GDPR Compliance’ *Journal of Engineering* (23 October 2017) 148.

³⁴⁸ GDPR, Article 30.

as encryption, and it does so via automated system integrations. The incorporation of these privacy management tools into a PbDD programme empowers businesses to exercise greater control over their data and implement policies that prioritise default risk elimination, thereby advancing privacy and security.

The GDPR specifies that organisations' retention policies must comply with both the 'data minimisation' and 'storage limitation' principles, and any personal data must be stored and destroyed in a compliant manner. Although the GDPR does not set specific time limits for different types of data, rather it makes organisations responsible for determining on how long they need the data for their specified purposes, it establishes the obligation on controllers to take in consideration the following factors when implementing PbDD: (i) personal data held for too long will, by definition, be unnecessary, (ii) organisations are unlikely to have a lawful basis for retention, (iii) from a more practical perspective, it is inefficient to hold more personal data than an organisation needs, and there may be unnecessary costs associated with storage and security, (iv) organisations must also respond to subject access requests for any personal data they hold and this may be more difficult if they are holding old data for longer than they need, (v) good practice around storage limitation (with clear policies on retention periods and erasure) is also likely to reduce the burden of dealing with queries about retention and individual requests for erasure.^{349,350}

However, it is essential for organisations to recognise that PbDD may not fully address all data security issues, and thus any strategy for GDPR compliance must be

³⁴⁹ ICO, 'Principle (e): Storage Limitation' (n 321).

³⁵⁰ This checklist provided by the UK regulator highlights the crucial importance of data protection authorities in providing further guidance on the practical application of legal requirements and filling any gaps in the GDPR.

accompanied by appropriate Information Security Policies³⁵¹ (statements and rules protecting personal data, systems, and digital assets) and if possible, anchored on strong industry security frameworks (such as ISO 27001), to ensure that personal data is always processed according to the paradigms outlined in the Regulation.

4.1.9. The data security principle: A “trust-building” facilitator

The principle of integrity and confidentiality is crucial to ensure the security of personal data and in preventing detriment to the rights and freedoms of data subjects that may emerge from accidental, unauthorised, or unlawful access, use, modification, disclosure, loss, destruction or damage of that data.³⁵² The GDPR obliges organisations to implement appropriate measures to achieve data security, which depending on the specific circumstances of the case, may include pseudonymisation - ‘a security technique for replacing sensitive data with realistic fictional data,’³⁵³ and encryption – a technical process that ‘exhibits the original data incomprehensible and the process cannot be reversed without access to the correct decryption key.’³⁵⁴ Such implementation should consider ‘the state of the art, the costs of implementation and the nature, scope, context and purpose

³⁵¹ See, Dimitar Kostadinov, ‘Key Elements of an Information Security Policy’ (*Management, compliance & auditing*, 20 July 2020) <<https://resources.infosecinstitute.com/topic/key-elements-information-security-policy/>>. ‘An information security policy is a set of rules enacted by an organisation to ensure that all users of networks or the IT structure within the organisation’s domain abide by the prescriptions regarding the security of data stored digitally within the boundaries the organisation stretches its authority. An information security policy governs the protection of information, which is one of the many assets a corporation needs to protect.’

³⁵² GDPR, Article 5(1)(f). GDPR, Recital 39.

³⁵³ Peter Štarchoň and Tomáš Pikulík, ‘GDPR Principles in Data Protection Encourage Pseudonymization through Most Popular and Full-Personalized Devices - Mobile Phones’ (2019) 151 *The 10th International Conference on Ambient Systems, Networks and Technologies (ANT 2019)* / *The 2nd International Conference on Emerging Data and Industry 4.0 (EDI40 2019)* / *Affiliated Workshops* 303.

³⁵⁴ *ibid.*

of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.’³⁵⁵

Data security has been an area of interest for over half a century, and I believe it is a crucial factor to take into account when developing a PbDD plan. The GDPR lacks specificity regarding the TOMs required to achieve compliance; however, Article 32 GDPR identifies pseudonymisation and encryption as suitable measures that data controllers must adopt to ensure the principles of integrity and confidentiality are met. These measures provide an effective way for organisations to integrate safeguards into their business practices, thereby meeting the GDPR's requirements for protecting data subjects' rights. Additionally, the security principle is closely linked to personal data breaches, which often pose a significant risk to individuals' rights and freedoms. As the EDPB states in its Guidelines on Article 25, Data Protection by Design and by Default,³⁵⁶ ‘having robust security measures contributes to build trust with the data subjects.’ Public trust is a fundamental premise of the Regulation, as indicated by the accountability principle summarised below, which states that the controller is responsible for and must demonstrate compliance with all data protection principles. Following this line of reasoning, I will proceed to add a new “attribute” to PbDD: the “trust-building” facilitator.³⁵⁷

³⁵⁵ GDPR, Article 32(1).

³⁵⁶ European Data Protection Board (EDPB) (n 206).

³⁵⁷ For a discussion on privacy and trust, see, e.g., Priscilla M Regan and Deborah G Johnson, ‘Privacy and Trust in Socio-Technical Systems of Accountability’ in Daniel Guagnin and others (eds), *Managing Privacy through Accountability* (Palgrave Macmillan UK 2012) <https://doi.org/10.1057/9781137032225_7>. See also, Theo Lynn and others, *Data Privacy and Trust in Cloud Computing: Building Trust in the Cloud Through Assurance and Accountability* (Springer International Publishing AG 2020) <<https://go.exlibris.link/HQxtCksX>>.

In the context of data protection, cybersecurity plays a crucial role in safeguarding personal data from unauthorised access, loss, or destruction. Therefore, I argue for organisations to incorporate cybersecurity measures as an integral part of their PbDD strategy to ensure the protection of data subjects' rights and freedoms. This includes assessing and identifying potential privacy risks and implementing appropriate measures to mitigate these risks, such as access controls, encryption, and firewalls.³⁵⁸

The potential impact of a data breach on individuals' rights and freedoms cannot be overstated, and the organisation's PbDD strategy must prioritise cybersecurity measures to mitigate these risks. It is worth emphasising that as of January 2023, EU supervisory authorities have imposed significant fines totalling €375,780,219.00 for insufficient TOMs to ensure information security. As evidenced by the analysis of fines imposed by supervisory authorities, the failure to implement adequate security measures ranks as the third factor that leads EU regulators to levy fines on organisations.

4.1.10. PbDD beyond stated intentions: the accountability principle

The accountability principle correlates with all personal data protection principles. It is a fundamental feature of PbDD since it requires organisations to 'actively and continuously implement measures to promote and safeguard data protection in their processing

³⁵⁸ Incorporating cybersecurity measures also ensures compliance with the accountability principle, as outlined in Article 5(2) of the GDPR, which requires organisations to demonstrate their compliance with the GDPR's data protection principles. Failure to adopt adequate cybersecurity measures can result in significant reputational damage, financial losses, and legal liabilities, including hefty fines and penalties. Furthermore, the increasing frequency and sophistication of cyberattacks highlight the importance of cybersecurity in protecting personal data.

activities.³⁵⁹ The GDPR establishes an obligation for organisations to comply with the Regulation and assigns an onus to demonstrate such compliance at any time, to both individuals³⁶⁰ and supervisory authorities.³⁶¹ This means that ‘organisational privacy programs become mandatory, as opposed to merely a sensible way of achieving compliance.’³⁶²

Inga Kroener and David Wright suggest that ‘accountability provides the “teeth” for PbD; it assures that PbD is more than stated intentions.’ In general, accountability implies a process whereby one body holds another body accountable, which should include a process of rebuttal if the first body is found to be non-compliant. It is argued that the existing gap between the GDPR principles espoused by PbDD and the operationalisation of these principles by organisations, is partly due to the lack of guidelines for translating the abstract principles into concrete methodologies and tools. The upcoming chapters will delve into this significant topic in greater detail.

The ICO guidelines outline some activities that organisations can undertake to demonstrate compliance, namely; carrying out DPIAs for uses of personal data that are likely to result in high risk to individuals’ interests; appointing a data protection officer; and adhering to relevant codes of conduct and signing up to certification schemes.³⁶³ Moreover, according to the OECD, the data controller must be accountable for complying with measures that give effect to data protection principles, namely, have a privacy

³⁵⁹ European Data Protection Board (EDPB) (n 206).

³⁶⁰ GDPR, Articles 12 and 14.

³⁶¹ *ibid.* Articles 30,31,35,39 and 40.

³⁶² Aleksei Yu Churilov and National Research Tomsk State University, ‘Principles of the EU General Regulations for the Protection of Personal Data (GDPR): Problems and Perspectives for Implementation’ (2019) 16 *Vestnik of the Omsk Law Academy* 29.

³⁶³ ICO, ‘Accountability and Governance’ (n 50).

management program in place and be prepared to demonstrate its privacy management program as appropriate. This is attributed to the following reasons:

‘The data controller decides about data and data processing activities. It is for his benefit that the processing of data is carried out. Accordingly, it is essential that under domestic law accountability for complying with privacy protection rules and decisions should be placed on the data controller [...]. Accountability under Paragraph 14 refers to accountability supported by legal sanctions, as well as to accountability established by codes of conduct, for instance.’³⁶⁴

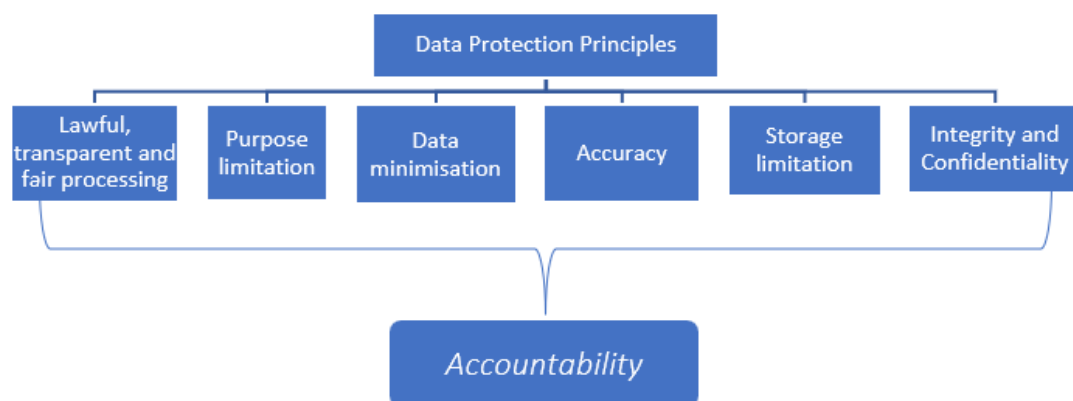


Figure 7 - The principle of accountability - Federico Marengo, Data Protection Law in Charts, 2021 (adapted).

Integrating the seven general principles of data protection described above, which derive from the ethical dimension³⁶⁵ of the CFR,³⁶⁶ into the routine operations of organisations

³⁶⁴ OECD, ‘OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data’ <<https://www.oecd-ilibrary.org/content/publication/9789264196391-en>>.

³⁶⁵ See, Markus Frischhut, ‘Status Quo of Ethics and Morality in EU Law’ in Markus Frischhut (ed), *The Ethical Spirit of EU Law* (Springer International Publishing 2019) <https://doi.org/10.1007/978-3-030-10582-2_3>.

³⁶⁶ Charter of Fundamental Rights of the European Union (2000/C 364/01).

poses a significant challenge, as it often requires a structured approach to data protection, especially PbDD, which can be both complex and costly. However, I believe that the DPPA presented in this study can provide organisations with a roadmap to navigate these challenges and successfully implement the GDPR principles in their data processing activities.

4.2. Compliance through accountability: should the legislator aim for a more prescriptive model of GDPR instead?

As mentioned earlier *en passant*, GDPR is not a Rules-Based Regulation (RBR) but a Principles-Based Regulation (PBR). In this regard, I would like to begin this section by drawing attention to three (of seven) paradoxes that Julia Black has identified in her research:³⁶⁷ the compliance paradox, the internal management paradox, and the ethical paradox.

Principles-based regulatory regimes are designed to offer organisations the flexibility to comply with Regulations in a manner that is tailored to their unique circumstances. However, a lack of certainty in some cases can lead to organisations adopting overly conservative compliance attitudes, which is the first concern. The second concern is whether an organisation's internal compliance systems are capable of dealing with this type of Regulation. Black argues that while principles-based Regulations can empower compliance systems, these systems are often the least developed component of institutions' internal systems and controls and may not always be capable of fulfilling their

³⁶⁷ Julia Black, 'Forms and Paradoxes of Principles-Based Regulation' (2008) 3 Capital markets law journal 425.

assigned function. The third, ethical paradox, is that while a principles-based Regulation can help organisations build an ethical compliance culture, it also requires organisations to take a risk-based approach to compliance, which can stifle the development of such a culture.³⁶⁸

Essentially, PBR requires that organisations adopt a risk-based approach to compliance, whereby data controllers need to possess a comprehensive understanding of the application of data protection principles and individual rights in practice. This knowledge is critical in developing an ethical, effective, and easily understandable compliance strategy that integrates PbDD principles.

As noted in Chapter one, a prominent critique directed towards the GDPR pertains to the perceived ambiguity and uncertainty of its provisions, resulting in difficulties for organisations to comprehend the practical implementation of GDPR requirements, namely, PbDD. The CJEU in *Deutsche Milchkontor*³⁶⁹ asserted that the ‘the principles of legitimate expectation and assurance of legal certainty are part of the legal order of the Community’; legal certainty and legitimate expectation are, as the Court underscores, related. If the law is certain, citizens (and data controllers) know what to expect.

It has also been noted that PbDD is intrinsically connected to abstract variables, such as the ‘state of the art’, ‘cost of implementation’, ‘nature, scope, context and purpose of processing’, as well as to the ‘risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing’, all factors that, according to Article 25 GDPR, must be considered when implementing a PbDD programme. GDPR’s PbDD relies

³⁶⁸ *ibid.*

³⁶⁹ *Deutsche Milchkontor* [1993] (n 80).

thus on the assessment and mitigation of 'risks of varying likelihood', where a risk-based approach may not always be consistent with the data processing principles and PbDD itself, which from a practical standpoint requires a certain degree of "concreteness," or tangibility, to the extent that it relies heavily on specific technological tools to control personal data. Due to its wide practical applicability, this exercise requires clear and functional concepts, which, as the CJEU demonstrated in *Jehovah Witnesses (2017)*,³⁷⁰ must rely on 'factual rather than formal analysis.'

Moreover, the GDPR's inherent lack of a parameterisation of legal values creates a loophole that can result in the infringement of individuals' rights and freedoms and result in encouraging the use of unregulated practices.³⁷¹ Thus, to ensure GDPR compliance, a stricter, rule-based approach may be advocated over an accountability-based approach, given the compelling justifications outlined earlier.³⁷²

The accountability approach to compliance has indeed been widely adopted by most organisations in recent years and is enshrined in the Regulation. Cavoukian defines the accountability-based privacy governance model as follows:

'[O]ne where organisations are charged with societal objectives, such as using personal information in a manner that maintains individual autonomy and which protects individuals from social, financial and

³⁷⁰ *Case C-25/17 Jehovan todistajat (GC) (2018) ECLI:EU:C:2018:551 17.*

³⁷¹ Michael Veale, Reuben Binns and Jef Ausloos, 'When Data Protection by Design and Data Subject Rights Clash' (2018) 8 *International data privacy law* 105.

³⁷² Tzanou (n 6). "[D]ata protection as a fundamental right should be able to function both positively and negatively. It should be able, on the one hand, to regulate, channel, and control power, and on the other hand, to prohibit power."

physical harms, while leaving the actual mechanisms for achieving those objectives to the organisation.’³⁷³

To successfully protect the rights and freedoms of data subjects, it is not possible to rely solely on theoretical approaches to privacy and technology while moving away from reliance on detailed, prescriptive rules.³⁷⁴ A rigorous commitment to complying with data protection principles, along with the implementation of TOMs and PETs, appears to be the only viable path forward in order to achieve GDPR compliance in the current landscape. Such an approach would not only enhance data protection and privacy, but also increase trust between data controllers and data subjects.

Understanding how the law will flow into organisations' activities so as to guarantee effective protection of rights and freedoms of individuals, is not achievable by resorting to compliance models mainly focused on broad societal objectives (e.g., Fair Information Practices, “FIPS”),³⁷⁵ attached to an unrealistic concept of ‘full functionality,’³⁷⁶ which *Birnstill et al.* illustrates as focused on ‘regulating trade-offs between privacy and functionality [which] is questionable from a theoretic as well as from an operational point of view’.³⁷⁷

³⁷³ Cavoukian, Taylor and Abrams (n 255).

³⁷⁴ In this context, I would like to clarify that my intent is not to question the effectiveness of the privacy design approach for technological systems (software and hardware), where the data controller is responsible for implementing data protection principles into processing operations. Instead, my concerns arise from the absence of a well-structured legal framework to enable the successful implementation of data protection principles in practical, real-world situations with the degree of success envisioned by the legislator.

³⁷⁵ Cavoukian, Taylor and Abrams (n 255).

³⁷⁶ Cavoukian, ‘Privacy by Design: The Definitive Workshop. A Foreword by Ann Cavoukian, Ph.D.’ (n 26).

³⁷⁷ Christoph Bier and others, ‘How Is Positive-Sum Privacy Feasible?’ in Nils Aschenbruck and others (eds), *Future Security* (Springer Berlin Heidelberg 2012). (emphasis added).

It is worth noting that while the accountability principle undoubtedly characterises the GDPR, the majority of the Regulation's requirements are not comprehensively or formally integrated into the logic of the full-functionality principle, as described by Cavoukian: 'Privacy can and must co-exist alongside other critical requirements: security, functionality, operational efficiency, organisational control, business processes, and usability in a "positive-sum", or doubly enabling "win-win" equation'.³⁷⁸ Furthermore, the GDPR does not contain any explicit reference to consideration of such trade-offs between privacy and functionality, importantly, when requiring the integration of PbDD into business systems and processes. The controller is solely required to implement 'appropriate TOMs, (...) to implement data-protection principles (...) in order to meet the requirements of this Regulation and protect the rights of data subjects.'³⁷⁹

In fact, I would suggest that there are instances where the full-functionality principle becomes irreconcilable with the data protection principles that PbDD seeks to uphold, particularly in the context of the risk-mitigation exercise proposed by the Regulation. My concern centres on the potential unilateral restriction of the rights and freedoms of individuals based on the outcomes of a risk assessment or risk score. Such a practice is viewed as incompatible with the GDPR principle of fairness of processing, as it may neglect individual circumstances and fail to allow meaningful input from data subjects. Furthermore, risk assessments and risk scores have the potential to introduce subjectivity, possibly resulting in discriminatory outcomes. If specific groups bear a disproportionate impact from risk-mitigation measures, it could be considered unfair and contrary to the

³⁷⁸ Cavoukian, 'Privacy by Design: The Definitive Workshop. A Foreword by Ann Cavoukian, Ph.D' (n 26).

³⁷⁹ GDPR, Article 25(1).

principle of treating individuals equitably. Additionally, if the process of risk assessment and its implications for individuals' rights lacks transparency, it may run afoul of the GDPR principle of fairness, which underscores the importance of transparency in data processing practices.

To uphold fairness, akin to the processes involving automated decision-making, individuals should receive information about the associated risks, the rationale behind the assessment, and the significance and expected consequences of such processing for them. Additionally, data subjects should have the right to express their perspectives and contest decisions. In practice, this would require organisations to disclose their privacy risk-optimisation processes on a case-by-case basis, a task that could prove impracticable.

The GDPR demands a delicate balance between the interests and rights of data subjects and the legitimate interests pursued by data controllers. Unilateral risk-mitigation measures, lacking adequate consideration for individual rights, may upset this balance and be perceived as unfair. Fair processing also entails granting individuals a level of control over their data and the processing activities. Unilateral risk-based limitations could undermine this empowerment, appearing inconsistent with the principle of fairness regarding data subjects' control over their information.

In general, the accountability approach relies heavily on privacy risk-optimisation,³⁸⁰ with business practices and operations focused more on risk mitigation, rather than attempting to root out the causing risk factor. In my view, the impact assessment that Article 35 GDPR requires organisations to conduct in case of a processing

³⁸⁰ In my view, this approach falls short of fully integrating the fundamental principles of data protection into the business's operations. Instead, as a business-friendly approach to privacy compliance, it tends to remain anchored on 'economic logics within the boundaries of the law.' See, Veale, Binns and Ausloos (n 363).

activity 'is likely to result in a high risk to the rights and freedoms of natural persons,'³⁸¹ does not produce in practice the legislator's desired outcomes. To explicate my viewpoint further: consider a scenario in which a controller conducts a DPIA that yields an unfavourable outcome, indicating that the processing activity may result in harm to the data subject. Despite this, due to the constraining factors mentioned above, namely the ostrich effect, the controller may choose to proceed with the processing activity due to the organisation's high-risk appetite and economic considerations, thereby ignoring the potential negative impact on the data subject. This decision is often made within legal boundaries, under the guise of a "win-win" assessment, which is frequently based on economic reasoning.³⁸²

Over time, academics and practitioners, often in collaboration with regulators, have provided recommendations to better inform the use of the accountability approach, arguing that such an approach helps ensure that organisations take a holistic view of their data protection practices, rather than just focusing on technical solutions and requiring them to take proactive steps to identify and manage risk to personal data. Unquestionably, the accountability approach is the most prevalent method of attaining compliance with GDPR,³⁸³ standing firmly rooted in the principle of accountability, which obliges organisations to put in place appropriate measures to demonstrate their adherence to GDPR, as and when required. In practice, this model integrates two premises into the businesses processes: (i) controllers and processors are always responsible for complying

³⁸¹ GDPR, Article 35.

³⁸² Veale, Binns and Ausloos (n 363).

³⁸³ For a discussion of the accountability approach in the context of data protection, see, *Managing Privacy through Accountability* (n 170).

with the GDPR, and (ii) controllers and processors must be able to demonstrate compliance, which means that data controllers must take responsibility for their actions and be willing to answer for their decisions, choices, and actions.

To achieve this, controllers must rely on a data protection management framework capable of creating a culture of commitment to data protection across the organisation and shift their focus from reactive to proactive compliance, backed by controls based on GDPR obligations,³⁸⁴ appropriate reporting structures,³⁸⁴ and assessment mechanisms including processing evaluation procedures.³⁸⁵ To illustrate, consider an organisation that acquires personal data from data subjects for a specific purpose. Subsequently, it chooses to utilise that data for another purpose. The organisation conducts an evaluation following the requirements of Article 6(4) of GDPR and concludes that the new processing operation aligns with the initial purpose for which the personal data was procured. Under the accountability approach proposed by GDPR, the organisation must document this processing compatibility - incorporating its reasoning behind the decision and detailing the TOMs in effect - so that it can subsequently furnish proof of its conformity to a supervisory authority.

³⁸⁴ Particular measures to demonstrate compliance: Designating a DPO (Articles 24(2) and 37-39 GDPR); adhering to approved codes of conduct or certification mechanisms (Articles 24(3), 40 and 42 GDPR); implementing modalities and procedures for the exercise of the rights of the data subject (Articles 12 and 24 GDPR); ensuring data protection by design and by default (Article 25 GDPR); keeping a record of processing activities and making them available to supervisory authorities (Article 30 GDPR); undertaking a DPIA (Article 35 GDPR). Although Art. 5(2) GDPR is only addressed to data controllers, data processors must also be held accountable for the processing of personal data: designating a DPO (Articles 37-39 GDPR); Keeping a record of processing activities and making it available to the Supervisory authority upon request (Article 30 GDPR); ensuring the implementation of all the measures to guarantee a safe data processing (Article 28(3)(c) GDPR); assisting the controller in some compliance requirements and obligations (Article 28(3)(d) GDPR). For both, data controllers and data processors, accountability measures must be reviewed and updated where necessary (Article 24(1) GDPR).

³⁸⁵ See Kate Brimsted, 'GDPR Series: Accountability - a Blueprint for GDPR Compliance' (*Thomson Reuters Practical Law, Privacy and Data Protection*) <<https://uk.westlaw.com/Document/I58CF05C0F57511E6A70DB1D5CDC31199/View/FullText.html>>.

This methodology has led many critics of the accountability approach to depict it as primarily scrutinising data protection compliance from a business perspective. I aim to rectify this situation by advocating for the adoption of the DPPA, which I will elaborate on comprehensively in Chapters eight and nine. By doing so, the emphasis will shift from a predominantly business-centred approach to data protection compliance to one that is more attuned to the data subject's viewpoint.

The European Data Protection Supervisor, explains the importance of applying an accountability framework for compliance with data protection law as follows:

‘Accountability is a common principle for organisations across many disciplines; the principle embodies that organisations live up to expectations for instance in the delivery of their products and their behaviour towards those they interact with. The General Data Protection Regulation integrates accountability as a principle which requires that organisations put in place appropriate TOMs and be able to demonstrate what they did and its effectiveness when requested. Organisations, and not Data Protection Authorities, must demonstrate that they are compliant with the law. Such measures include: adequate documentation on what personal data are processed, how, to what purpose, how long; documented processes and procedures aiming at tackling data protection issues at an early state when building information systems or responding to a data breach; the presence of a Data Protection Officer that be integrated in the organisation planning and operations etc.’³⁸⁶

³⁸⁶ European Data Protection Supervisor, ‘Accountability’ (*Our work by topics*) <<https://edps.europa.eu/data-protection/our-work/subjects/accountability>>.

With this in mind, and while the concept of accountability is not new, it is noteworthy that its execution under the GDPR necessitates a sustained, systematic, and proactive approach to processing operations via PbDD. Crucially, to conform to this principle, organisations must not only perform an annual review of their activities in preparation for possible regulatory inspections but should also be able to evidence, consistently, that they are fulfilling their GDPR obligations. The efficacy of this approach is significantly contingent on the financial, technical, and governance maturity of each organisation, thereby bringing to fore questions regarding the practicability of fully implementing GDPR. This is particularly pertinent when considering that accountability, while essential, poses a risk of circumvention.

4.3. The development of the practical application of PbDD

This section identifies the complexities and challenges of putting the GDPR's legal requirements into practise through PbDD, while considering the current state of art, businesses' efforts and capacity to protect personal data, and the existing legal situation in the EU. In other words, it assesses the practical feasibility of the GDPR legal framework by asking whether it is possible to integrate PbDD into modern organisational systems and activities.

The concept of Privacy by Design (PbD) which is the basis of today's concept of Data Protection by Design and by Default (PbDD), was developed in the 1990s by Ann Cavoukian to become the 'framework to proactively embed privacy directly into information technology, business practices, physical design, and networked infrastructures – making it

the default.³⁸⁷ It was developed as a way of thinking about systems engineering,³⁸⁸ and as demand for the consideration of privacy throughout each and every step of the engineering process, directed towards systems engineers rather than toward lawyers.³⁸⁹ The GDPR now requires data controllers and processors to appoint a data protection officer³⁹⁰ under certain circumstances³⁹¹ who as ‘a person with expert knowledge of data protection law and practises should assist the controller or processor to monitor internal compliance with this Regulation’.³⁹² Controllers must ‘ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the

³⁸⁷ Cavoukian, ‘Privacy by Design [Leading Edge]’ (n 25).

³⁸⁸ See, Bednar, Spiekermann and Langheinrich (n 43). ‘Privacy by Design “requires the guts and ingenuity of engineers”, as it is the systems engineers (i.e., software architects, information architects, interaction designers, product designers, and related specialities) who have to find a competent and creative way to realize privacy protection implementations.’

³⁸⁹ *ibid.* ‘Taken together, our theoretical and empirical insights suggest that there may be an underlying conflict between the legal world and the engineering world, with lawyers imputing responsibility on engineers that the engineers do not want to embrace.’

³⁹⁰ GDPR, Article 37.

³⁹¹ The mandatory designation of DPO applies to public authorities or bodies, except for courts acting in their judicial capacity (Article 37(1)(a) GDPR). ‘They may designate a single DPO for several authorities or bodies, considering their organisational structure and size’ (Article 36(3) GDPR); private controllers or processors whose core activities require, by virtue of their nature, scope and/or purposes, regular and systematic monitoring of personal data on a large scale (Article 37(1)(b) GDPR); private entities whose core activities entail processing, on a large scale, special categories of personal data or data relating to personal convictions and offences (Article 37(1)(c) GDPR); EU or Member State law may require the designation of DPO (Article 36(3) GDPR), e.g., the Spanish data protection law requires the mandatory designation of a DPO, namely, to the following organisations: financial companies, insurance and reinsurance companies, investment companies, certain public utilities companies (Articles 34(1)(f),(i) Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales).

³⁹² In terms of person qualifications, the DPO should be designated on the basis of: Professional qualities (Article 37(5) GDPR); ‘expert knowledge of data protection law and practices’ (Article 37(5) GDPR). The necessary level of expert knowledge should be determined in particular according to the data processing operations carried out and the protection required for the personal data processed by the controller or the processor (Recital 97 GDPR); The DPO must be able to fulfil the tasks referred to in Article 39 GDPR (Article 37(5) GDPR). Following a public consultation, The French Data Protection Act, as amended by the Act dated 20 June 2018, provides the French Supervisory authority (CNIL) with a new task as regards the certification of the data protection officers (DPOs). Since September 2018, CNIL can adopt certification criteria and accredit bodies in charge of issuing such certification. The Spanish Data Protection Agency (AEPD) was the first in Europe to set up regulations for data protection officer certification schemes. This certification issued together with Spain's National Entity of Accreditation, allows for data protection professionals certified under the scheme to demonstrate that they are up to the GDPR standards for the role of DPO, by showing off their "seal of conformity".

protection of personal data.³⁹³ Data protection officers are generally responsible for implementing Article 25 of the GDPR and thus for embedding PbDD into business systems and operations.

Article 25 of the GDPR outlines the fundamental instructions pertaining to PbDD that form the basis of the GDPR's operational framework. In one hand, to ensure 'privacy by design', organisations must implement appropriate TOMs to uphold data protection principles from the outset of the planning process. On the other hand, 'privacy by default' mandates that all personal data must be handled with the highest level of privacy protection. This involves collecting, storing, or otherwise processing only the necessary information, and restricting access to the data to a limited number of authorised individuals.³⁹⁴

Therefore, to ensure compliance, it is crucial to determine whether and how PbDD can be integrated into current business systems and operations. In the 2018 Preliminary Opinion on privacy by design, the former European Data Protection Supervisor, Giovanni Buttarelli, stated that '[W]hile privacy by design has made significant progress in legal, technological and conceptual development, it is still far from unfolding its full potential for the protection of the fundamental rights of individuals.'³⁹⁵ I contend that this "work-in-

³⁹³ GDPR, Recital 97.

³⁹⁴ Please see the following examples on the official website of the European Union: 'Data protection by design - The use of pseudonymisation (replacing personally identifiable material with artificial identifiers) and encryption (encoding messages so only those authorised can read them). Data protection by default - A social media platform should be encouraged to set users' profile settings in the most privacy-friendly setting by, for example, limiting from the start the accessibility of the users' profile so that it isn't accessible by default to an indefinite number of persons. <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en>.

³⁹⁵ 'EDPS Opinion 5/2018 - Preliminary Opinion On Privacy By Design' (2018) <<https://link.gale.com/apps/doc/A549172127/ITOF?u=rdg&sid=ITOF&xid=e41d0c3c>>.

progress" characteristic of PbDD, along with the employment of outdated risk-mitigation approaches to compliance, undermines the applicability of the Regulation.

Although Article 25 GDPR predominantly concerns the development of information systems and processes, its underlying rationale is rooted in the belief that integrating data protection principles into the architecture of these systems will imbue them with greater significance. Moreover, it implicitly acknowledges that information systems can influence human behaviour more effectively than mere legal or contractual requirements.³⁹⁶ Of course, methods exist to translate legal requirements into software and system requirements, such as testing legal requirements as if they were functional requirements (although a widely accepted method of dealing with data protection, for example, during software and system development is the use of PbDD, as privacy is directly embedded in the process).³⁹⁷ The following are some of the challenges I have identified in relation to the implementation of the PbDD principles: (i) One of the primary challenges associated with implementing PbDD principles is the technical complexity involved in incorporating data protection into the design of products and systems. This endeavour necessitates a high degree of technical proficiency and may require a considerable investment of resources, expertise, and time; (ii) Another key challenge that arises with respect to PbDD principles pertains to balancing privacy and innovation. This is because PbDD may potentially restrict an organisation's ability to leverage data in novel and innovative ways, thereby creating a tension between privacy and innovation; (iii) Interoperability is another significant challenge associated with PbDD implementation. This challenge involves ensuring that

³⁹⁶ Bygrave (n 67).

³⁹⁷ M. Colesky, J. Hoepman, and C. Hillen (n 84).

products and systems are designed to be compatible with other systems and to meet the diverse needs of various stakeholders. Achieving interoperability requires a high degree of technical expertise and a thorough understanding of the specific needs and requirements of each stakeholder; (iv) Another critical challenge associated with the implementation of PbDD principles is keeping pace with the rapid advancements in technology. As the technological landscape continues to evolve at a swift pace, organisations must be able to adapt quickly to new developments to ensure that their data protection measures remain effective. This requires a deep understanding of emerging technologies and a commitment to continuous improvement to stay ahead of the curve; and (v) Yet another notable challenge in the implementation of PbDD principles is adapting to changing privacy expectations. As privacy expectations shift over time, controllers must remain agile and adapt their data protection measures to remain relevant and effective. In this work, I will concentrate on the challenges that I believe have a greater impact on an organisation's operational efforts.

The legal concepts of "data protection by design" and "data protection by default" are central to the GDPR. However, criticisms around the formulation of PbDD include that it is vague and amorphous, to the extent that complaints have been voiced about the ambiguous language of Article 25 GDPR and the "legalese" that obscures the meaning of the text and hinders the engineering and business community's ability to conduct its business in the desired manner.³⁹⁸ Moreover, PbDD lacks practical tools to assist developers in building and implementing privacy-friendly systems, and Article 25 GDPR

³⁹⁸ Ira S Rubinstein and Nathaniel Good, 'The Trouble with Article 25 (and How to Fix It): The Future of Data Protection by Design and Default' (2020) 10 International Data Privacy Law 37.

does not provide a clear framework for translating specific legal data protection requirements into system requirements.³⁹⁹

An analysis of Article 25 of the GDPR reveals several technical or technological shortcomings. First, the Article is argued to overlap with several accountability provisions in an unclear manner, which could lead to ambiguity in the application of the Regulation. Second, the scope of Article 25 is not precisely specified, making it difficult to identify what exactly needs to be achieved by implementing the TOMs prescribed. Third, the Article offers very few examples of relevant TOMs, apart from pseudonymisation. Fourth, the provision is written in vague and abstract language, making it challenging to understand the specific meaning and requirements of the Regulation. Finally, the Article omits any specific privacy engineering methodologies, tools, or techniques, which only further complicates understanding of its meaning or requirements.

It is thus critical that policymakers and regulators address these shortcomings to ensure that Article 25 is effectively implemented and enforced.⁴⁰⁰ Without a clear and concise translation of Article 25 of the GDPR into technical terms or a more easily understandable format for business stakeholders and practitioners, it remains an empty abstraction that businesses will largely ignore except to claim credit for procedural measures.⁴⁰¹

³⁹⁹ M. Colesky, J. Hoepman, and C. Hillen (n 84).

⁴⁰⁰ Clear and unambiguous language that specifies the scope and requirements of the Regulation, along with practical examples and specific privacy engineering methodologies, tools, and techniques, should be included to assist organisations in meeting their obligations under the GDPR. Failure to address these shortcomings could result in inconsistent interpretations and applications of the Regulation, which could undermine its overall effectiveness.

⁴⁰¹ Rubinstein and Good (n 390).

Regrettably, the practical implementation of Article 25 GDPR has received relatively scant attention from the academic community. Thus, in order to evaluate the feasibility of PbDD implementation, this study will eschew the purely theoretical limitations of PbDD and instead focus on examining the practical implications of the legal obligation for PbDD under the GDPR, specifically for data controllers. Based on these discussions, I intend to draw conclusions on how PbDD ought to be interpreted, but more crucially, how it should be implemented, and whether it can be practically successful.

4.4. Assessing the feasibility of GDPR's PbDD implementation in practice

The European Commission (EC) launched a public consultation on 9 July 2009 concerning the future of the right to data protection in the European Union. The Commission asked for opinions regarding the new challenges presented by new technologies and globalisation to the protection of personal data.⁴⁰² On 1 January 2012, following the consultation, the EC presented a proposal for a comprehensive reform of the DPD in the form of a General Data Protection Regulation.⁴⁰³ The legislation which is now universally recognised as the GDPR was adopted in 2016, and became effective on 25 May 2018, after a two-year adaptation period.⁴⁰⁴

⁴⁰² Article 29 Data Protection Working Party and Working Party on Police and Justice, 'The Future of Privacy - Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data' (Article 29 Data Protection Working Party, Working Party on Police and Justice 2009) 02356/09/EN, WP 168.

⁴⁰³ European Commission, 'Proposal for GDPR, 25.01.2012, COM(2012) 11' (n 130).

⁴⁰⁴ See CJ Hoofnagle, B Sloat and FJ Zuiderveen Borgesius, 'The European Union General Data Protection Regulation: What It Is and What It Means' (2019) 28 Information & communications technology law 65. ('The GDPR has been law since 2016, but did not enter most lawyers' attention until 2018, when its provisions became enforceable.').

The GDPR expands on the principles and rights of data subjects, already present in the repealed DPD,⁴⁰⁵ and introduces new obligations⁴⁰⁶ for data controllers and processors, namely, it makes compulsory for organisations to implement PbDD, to comply with the right to portability and with the principle of accountability. Under some conditions, organisations must also employ a Data Protection Officer ('DPO'). As EU Regulations benefit from direct applicability⁴⁰⁷ in all member states, consistency across the whole EU area is now (at least theoretically) guaranteed. The GDPR allows member states to enact specific rules in certain circumstances, particularly where sector-specific legislation already exists, for example on the processing of employee personal data;⁴⁰⁸ archiving purposes in the public interest, scientific or historical research purposes, and statistical purposes;⁴⁰⁹ processing of special categories of personal data;⁴¹⁰ and processing in compliance with a legal obligation.⁴¹¹

The territorial scope of GDPR is vast as it protects the fundamental rights and freedoms of individuals (data subjects) who are in the Union, in particular their right to the protection of personal data, where their data is subject to (wholly or partly) automated

⁴⁰⁵ *ibid.* 'Much of the GDPR's requirements were reflected in an earlier law – the Data Protection Directive – which had poor enforcement and compliance.'

⁴⁰⁶ *ibid.* 'The GDPR is the most consequential regulatory development in information policy in a generation. The GDPR brings personal data into a complex and protective regulatory regime.'

⁴⁰⁷ Both, EU treaties and EU regulations are directly applicable. They do not need any other acts of parliament in the member state to make them into law- they are automatically integrated in the national legislation beginning with entry into force. Therefore, once a treaty is signed or a regulation is passed in Brussels by the Council of Ministers, it instantly becomes applicable in all member states.

⁴⁰⁸ GDPR, Article 88.

⁴⁰⁹ *ibid.* Article 89.

⁴¹⁰ *ibid.* Article 9(4).

⁴¹¹ *ibid.* Article 6.

processing⁴¹² or is otherwise processed by way of a filing system. It is evident that the GDPR's concept of personal data is inextricably linked to the concept of identity: information which 'identifies an individual or renders an individual identifiable',⁴¹³ and which requires protection from any form of electronic or manual processing (including storage and transmission) by data controllers or processors.⁴¹⁴

As discussed in Chapter one, the concept of personal data,⁴¹⁵ as defined by the GDPR and further developed by case law, will continuously be subject to shifting and evolving technology, namely, in how data is created, collected or shared in the information age.⁴¹⁶ As such, when dealing with personal data, organisations have a statutory duty to implement PbDD, both at the time of determining the means of processing and at the time of the processing itself, including, putting in place appropriate TOMs⁴¹⁷ in order to

⁴¹² See, de Hert and Gutwirth (n 11). The genesis of data protection law in Europe can be traced back to the 1970s, driven by the objective of safeguarding individuals from the perils associated with the automated processing of their personal data.

⁴¹³ See, Andrea Monti and Raymond Wacks, *Protecting Personal Information: The Right to Privacy Reconsidered* (Bloomsbury Publishing Plc 2019). 22. 'The starting point of any data protection law is the concept of 'personal data' or, in some statutes, 'personal information'. Article 4(1) of the GDPR defines personal data as '[A]ny information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.'

⁴¹⁴ GDPR, Article 2(2)(c). The GDPR does not apply to processing activities carried out 'by a natural person in the course of a purely personal or household activity'.

⁴¹⁵ The European Consumer Commissioner defined personal data as follows: 'Personal data is the new oil of the internet and the new currency of the digital world.' See, Kuneva (n 29).

⁴¹⁶ See, OECD, 'Data in the Digital Age' (OECD 2019) OECD Going Policy Note <<https://www.oecd.org/going-digital/data-in-the-digital-age.pdf>>. 'The growing interactions between data, algorithms and big data analytics, connected things and people are opening huge new opportunities. But they are also giving rise to issues around "data governance" at the national and international levels. These include questions around the management of data availability, accessibility, usability, integrity and security, as well as concerns about ownership, impacts on trade and competition, implications for personal privacy, and more.'

⁴¹⁷ Article 24(1) GDPR determines the controller's obligation to implement appropriate technical and organisational measures to ensure compliance with the regulation. This means that, de facto, requires controllers to put in place physical and technical measures (security defences), as well as data protection organisational policies. See also Article 24(2) GDPR; such measures must be adapted to the nature, scope, context and purposes of the processing, considering the risks and severity presented by the processing

safeguard individuals' rights and freedoms, and ensuring compliance with the data protection principles and any other requirements of the Regulation,⁴¹⁸ so that if one does nothing, privacy remains intact. As Cavoukian argues that no action whatsoever should be required on the part of the data subject to protect their own privacy — it must be built into the organisations' systems, by default.⁴¹⁹

Such ambitious operationalisation of the law⁴²⁰ – bridging and incorporating legal requirements into information systems and contemporary business operations, has been flagged as one task of very difficult accomplishment, as many technical practicalities involving the electronic processing of personal data⁴²¹ not always seem to be entirely compatible with the PbDD measures prescribed by the Regulation.⁴²² The suggestion that Article 25 GDPR needs to be interpreted as requiring the implementation of privacy engineering and privacy-enhancing technologies, to advance data protection in its own right, 'rather than merely reinforce the general principles of the Regulation,' appears to be valid.⁴²³ As the concept of PbDD finds its roots in privacy technology,⁴²⁴ and considering that most PETs come from the technological sphere, Rubinstein and Good propose the following approach to Article 25 GDPR, which I believe is worthy of support:

activity, to the rights and freedoms of individuals. In addition, Recital 78 GDPR states that 'In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default'.⁴¹⁸ GDPR, Article 25.

⁴¹⁹ Cavoukian, 'Privacy by Design: The Definitive Workshop. A Foreword by Ann Cavoukian, Ph.D' (n 26). Cavoukian lists 'Privacy as the default setting' as a PbD foundation principle.

⁴²⁰ Arguably, the operationalisation of the law should also consider the 'technology-neutrality' of the legal text. Recital 15 GDPR states that 'In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used.'

⁴²¹ See Bednar, Spiekermann and Langheinrich (n 43).

⁴²² See M. Colesky, J. Hoepman, and C. Hillen (n 84).

⁴²³ Rubinstein and Good (n 390).

⁴²⁴ Bygrave (n 67).

[M]arrying it to privacy engineering and the consideration and adoption of ‘hard’ PETs [...] emphasising privacy engineering and technology rather than more policy - or process-oriented measures. [...] only this interpretation of Article 25 ensures that it both accomplishes something useful in its own right, distinct from the general principles of the GDPR, and remains true to its roots in privacy technology.’⁴²⁵

This statement reinforces my perspective that a more prescriptive approach to Article 25 GDPR is necessary. Although there is a risk of the GDPR forfeiting its technology neutrality, providing a clear indication of the technical measures available to controllers (such as PETs) in addition to pseudonymisation would unquestionably reduce ambiguity and enhance certainty, resulting in a more effective implementation of PbDD in practice. I do not advocate prioritising privacy engineering and technology over policy since I believe that the latter is essential for safeguarding information rights. Instead, given that privacy engineering mainly pertains to the technical protocols for privacy protection, as opposed to the comprehensive approach to privacy and data protection mandated by the GDPR, I suggest incorporating a requirement in Article 25 GDPR for organisations to establish a structured Privacy Management System (PMS). This PMS would ensure that the legal, organisational, and technical facets of the Regulation are jointly considered and integrated into the processing operations.

The analysis of supervisory authority fines demonstrated that organisations often push legal boundaries to avoid operational constraints, resulting in significant penalties for data breaches or poor data protection practices. Moreover, research on the behavioural

⁴²⁵ Rubinstein and Good (n 390).

economics of privacy unequivocally establishes that people make irrational privacy decisions and consistently underestimate long-term privacy risks. This is attributable to several factors, including limited understanding of technology and privacy.⁴²⁶ This statement applies not only to individuals but also to business leaders making data protection decisions for their organisations.

The primary concern with a risk-based approach to PbDD is the perceived latitude afforded by the GDPR to conduct personal data processing based on a risk assessment, which can easily undermine the intentions of the legislature and jeopardise individuals' rights. Hence, the PMS should include: (i) identification of applicable technologies (assets); (ii) security and organisational measures (controls); and (iii) legal obligations and prerogatives (data protection principles and data subject rights). While I concur that a risk-based approach could be used for (i) and (ii), with regards to (iii), the data controller should avoid using this approach. Instead, the maxim of roman civil law, *Dura lex sed lex*, must be applied, which states that regardless of how regrettable the outcome of a legal provision may be, the law must be enforced. A zero-tolerance approach regarding respect for data protection principles and individuals' rights is the sole viable path towards a successful implementation of PbDD. As Tzanou suggests,

'In essence, the 'hard core' [*principles*] of data protection would be what needs to be protected, so that the final values that data protection

⁴²⁶ For a discussion of the behavioural economics of privacy see, Alessandro Acquisti, 'The Economics and Behavioral Economics of Privacy' in Helen Nissenbaum and others (eds), *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (Cambridge University Press 2014) <<https://www.cambridge.org/core/books/privacy-big-data-and-the-public-good/economics-and-behavioral-economics-of-privacy/A8FFC368B41B90B49479970A05E71B77>>.

pursues such as individual autonomy, dignity, and personal identity are safeguarded.⁴²⁷

Organisations must agree on what they need to protect – and that needs be personal data. Although conceptually privacy is often confused with security, organisations must start distinguishing them to understand how to meet data protection obligations. From a data protection perspective, security is one of the ways to preserve privacy. Of course, a successful PbDD strategy would be impossible to implement without a solid information security policy. Data protection also refers to the scarcity of personal data in an organisation's data ecosystem (data minimisation), as well as designing user-centric solutions that optimise user control while minimising network engagement. Most importantly, maximising individuals' control over their personal data must be seen as a priority.⁴²⁸

This prioritisation may not always be achievable, especially in situations where technological demands or other operational limitations hinder the extent to which individual rights can be accommodated. This is evident in the following Chapter five, where the intricate interplay between emerging technologies and the GDPR is examined. Hence, it is vital for organisations to carefully consider the implementation of PbDD, weighing the potential benefits against the practical challenges and limitations that may emerge in the backdrop of their activity.

⁴²⁷ Tzanou (n 6). (emphasis added).

⁴²⁸ I would like to reiterate my belief that the GDPR PbDD approach is, for the most part, feasible and practical for organisations to implement. However, the successful integration of PbDD into an organisation's systems and processes necessitates the adoption of an operational framework and PMS that prioritises the protection of individual rights and the principles of GDPR.

4.5. Concluding remarks

The comprehensive exploration of PbDD in this chapter highlights the pivotal role of the DPPA as an operational cornerstone within the realm of data protection, especially in its applicability. In fulfilling this role, the DPPA not only facilitates the seamless integration of appropriate TOMs but also serves as a key mechanism in effectively addressing specific areas brought to the forefront in this research. These encompass a range of aspects, from data subject's rights to data minimisation, storage limitation, and data security requirements.

As we immersed ourselves in the practical application of PbDD within the intricate landscape of the GDPR, the DPPA naturally emerged as a guiding framework, offering practical tools for its effective implementation. Notably, the application of the core pillars in data protection – the data protection principles and the data subjects' rights – received robust support within the DPPA, underscoring its instrumental role in grounding these areas into practical considerations.

This chapter established thus the groundwork for a nuanced understanding of the interrelationships between PbDD, the principles of the GDPR, and the role of the DPPA. Building upon this foundation, the subsequent chapter shifts its focus to the challenges posed by emerging technologies to PbDD. The transition is seamless as we extend our inquiry into the contemporary challenges presented by emerging technologies and how PbDD can navigate these challenges to maintain its efficacy and relevance in a dynamic technological environment where the protection of personal data is held as paramount. In this context, the DPPA, with its emphasis on practical implementation, emerges as a

linchpin in aligning theoretical principles with pragmatic applications, reinforcing its significance in the evolving landscape of data protection operations.

Chapter 5 – Reflections on the challenges that emerging technologies pose to PbDD

Introductory notes

Blockchain is a decentralised model of data collection and transfer on which many organisations, particularly those in the health and financial sectors, are increasingly relying on.⁴²⁹ However, the implementation of PbDD on blockchain is very challenging due to the particularities of systems processing personal data as well as the specificity of processes involved in such processing.

The technology design of blockchain undermines the applicability of the controller and processor concept as defined in Article 4(7) of the GDPR, thereby rendering many GDPR requirements unenforceable in blockchain transactions. The challenges arising from this include the identification of relevant data controllers and processors within a network, the establishment of reversible processing restrictions, the provision of satisfactory explanations and adherence to objections regarding automated processing, and the facilitation of compliant cross-border data transfers. These are some challenges for which the GDPR fails to provide a solution.⁴³⁰

⁴²⁹ For a discussion on the application of blockchain in the future of health sector, see Asad A Siyal and others, 'Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives' (2019) 3 *Cryptography*. 'A range of issues including data privacy, data integrity, data sharing, record keeping, patient enrolling, and so on, may arise in clinical trials. Blockchain, being the next internet generation, can provide viable solutions to these problems. Healthcare researchers are working on resolving these issues with the help of blockchain technology. The healthcare industry will soon be taken by storm with the applications of blockchain, accompanied by artificial intelligence (AI) and machine learning.'

⁴³⁰ Elizabeth Renieris, 'Forget Erasure: Why Blockchain Is Really Incompatible with the GDPR' (*Governance of technology & the internet, The Berkman Klein Center for Internet & Society at Harvard University*, 23 September 2019) <<https://cyber.harvard.edu/story/2019-09/forget-erasure-why-blockchain-really-incompatible-gdpr>>.

Blockchain and ledger-based projects contend that they are too decentralised to identify data controllers or be held accountable for upholding data subjects' rights, leading to areas of incompatibility between technology and the law. For example, it is impractical to implement the data subject's "right to be forgotten" within an immutable, append-only ledger. The GDPR stipulates that personal data must solely be collected, processed, and retained for specific, explicit, and legitimate purposes. Nevertheless, in blockchain environments, data is automatically replicated across all nodes on the network, making it impossible to assert that the data is not further processed for additional purposes after it is recorded on the ledger.

The principle of storage limitation mandates that personal data must not be kept in a format that enables the identification of data subjects for any longer than what is required for the intended purpose of processing. To accomplish this, a retention period must be precisely determined, supported by a sound rationale, subject to regular data reviews, and removal or anonymisation of data after a legitimate and justifiable retention period. However, these objectives cannot be met using blockchain technology.

In the context of the IoT, an important consideration is the current state of the art, which does not facilitate the implementation of PbDD and may also limit the applicability of the GDPR. This situation raises concerns about individuals' ability to protect their privacy from possible intrusion by IoT technology. The tension between IoT and privacy is evident in several cases, such as that of James Bates from Arkansas, USA, who was accused of killing a friend in 2015.⁴³¹ Prosecutors relied on data sourced from Bates smart meters and

⁴³¹ Holly Kathleen Hall, 'Arkansas v. Bates: Reconsidering the Limits of a Reasonable Expectation of Privacy' (2017) 6 University of Baltimore Journal of Media Law & Ethics 22.

Amazon's Echo device to build their case. Although Bates has consented to using the data, Amazon refused to disclose the Alexa data it collected, raising concerns about the extent of surveillance by IoT devices and the potential impact on individual privacy. Although the case was ultimately dismissed in December 2017, the incident garnered significant media attention and revealed the extent to which IoT devices can collect personal data without individuals' explicit knowledge or consent.⁴³² This case underscores the potential dangers of IoT devices in compromising privacy, which could eventually result in a "big brother is watching you" society, where an individual's every move is monitored and recorded. Against this backdrop, a pertinent question arises as to whether "big AI" should be subject to legal limitations, especially when it comes to continuously monitoring individuals.

In this context, I believe it is critical to examine what role PbDD could have had in ensuring privacy protection, specifically through appropriate technical measures aimed at data retention and erasure. Regrettably, the bulk of AI systems based on voice commands, including Alexa and Siri, operate in "listening" mode in order to reply to a command,⁴³³ such as: "Alexa, turn on the light." Moreover, these technologies hinge on perpetually collated (and stored) data to foster their "skills" via self-directed "learning" processing. If data is destroyed immediately after the task is completed (e.g., when the light is turned off), the critical "learning" function is circumvented.

In 2015, a comparable instance arose with Fitbit, concerning a murder case in Connecticut, where prosecutors relied upon GPS data (processed by AI) to buttress their argument. The data harvested by the AI app not only assisted in ascertaining the victim's

⁴³² Elliott C McLaughlin, 'Suspect OKs Amazon to Hand over Echo Recordings in Murder Case | CNN Business' (CNN, 7 March 2017) <<https://www.cnn.com/2017/03/07/tech/amazon-echo-alexa-bentonville-arkansas-murder-case/index.html>>.

⁴³³ Hall (n 423).

recent whereabouts but also confirmed the involvement of the victim's husband in the crime. Following this case, the American publication *Rolling Stone* cited various instances wherein AI devices are aiding 'cops solving crimes' in the United States.⁴³⁴

As an organisation defines its GDPR compliance strategy, the legal principles of PbDD should not be ignored, even when deploying "new to the world" technologies. Regrettably, since PbDD is described very broadly, its fitness for purpose is 'significantly undermined by a variety of weaknesses, including fuzzy legalese and a more general lack of clarity over the parameters and methodologies for achieving its goals.'⁴³⁵ Perhaps for this reason, technology experts and information systems engineers still consider PbDD as a mere prerequisite for technological privacy measures to be applied in the development of information systems,⁴³⁶ an approach certainly inherited from Cavoukian's PbD concept, which disregards, to large extent, the data protection "by default" requirement, which imply the 'default application of particular data protection principles and default limits on data accessibility'⁴³⁷ throughout the personal data processing lifecycle.

It is clear that relying solely on a technological approach is inadequate for achieving GDPR compliance, particularly in IoT settings. Instead, a comprehensive and holistic strategy must be devised, incorporating the principles of PbDD, which are fundamental for the practical operationalisation of the legislation, as highlighted in Article 25 of the GDPR. It is important to note that I do not view PbDD as paradoxical; particularly when dealing with emerging technologies, it is vital to distinguish between the "by design" stipulations

⁴³⁴ Lilly Dancyger, 'Fitbits Are Snitching on Criminals -- Here's How' (*Rolling Stone*, 4 October 2018) <<https://www.rollingstone.com/culture/culture-news/fitbit-apple-watch-crime-help-solve-733050/>>.

⁴³⁵ Bygrave (n 67).

⁴³⁶ Fei Bu and others, "'Privacy by Design" Implementation: Information System Engineers' Perspective' (2020) 53 *International Journal of Information Management* 102124.

⁴³⁷ Bygrave (n 67).

specified in Article 25(1) of the GDPR and the "by default" provisions articulated in Article 25(2) of the GDPR. While PbD has a primary focus on process-oriented measures,⁴³⁸ PbDD places emphasis on achieving a high level of systemic personal data protection through minimising data usage and upholding confidentiality.⁴³⁹ This results in a complementary relationship between the two principles. The "by default" approach entails pre-selection of appropriate data protection measures that apply to a given processing activity (or system processing data), except when the data subject intervenes to specify otherwise. This approach ensures that data protection measures are automatically implemented and do not require manual intervention, thereby minimising the risk of, inter alia, inadvertent data breaches. The "by design" approach requires a conscious and proactive integration of data protection measures, especially concerning the implementation of data protection principles, throughout the entirety of the data processing life cycle. In summary, both the "by design" and "by default" approaches are integral components of PbDD, which is essential for GDPR compliance.

⁴³⁸ To further examine the implementation of PbD strategies and tactics in the context of business processing operations, see, Jaap-Henk Hoepman, 'Privacy Design Strategies (The Little Blue Book)' (University of Groningen 2020) <<https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf>>. 'The process oriented strategies focus on the processes surrounding the responsible handling of personal data. They deal with the organisational aspects and the procedures that need to be in place. We distinguish the following four. Inform - Inform data subjects about the processing of their personal data in a timely and adequate manner. Control - Provide data subjects adequate control over the processing of their personal data. Enforce - Commit to processing personal data in a privacy-friendly way, and adequately enforce this. Demonstrate - Demonstrate you are processing personal data in a privacy-friendly way.'

⁴³⁹ The idea of data protection by default refers to an organisation ensuring that only data strictly essential for the specified purpose of the processing is processed by default (without the intervention of the individual).

5.1. Looking ahead: The blockchain paradox

Despite blockchain-based technology⁴⁴⁰ being purported to provide privacy, security, trust, accountability, and transparency, recent studies have identified several inconsistencies between blockchains and the GDPR. For instance, Haque et al. performed a comprehensive systematic literature review⁴⁴¹ to investigate GDPR provisions that had been previously scrutinised for integration with blockchain technology. Their study uncovered various issues with GDPR compliance, as evidenced by the following list: 1) Data deletion and rectification (Articles 16, 17, and 18 GDPR). Of particular note, Article 17 GDPR, which establishes the "right to be forgotten," is frequently cited as a significant contradiction in prior research. This contradiction arises because the blockchain cannot be altered or erased,⁴⁴² rendering it incompatible with the "right to be forgotten" requirement. A similar issue arises with Article 16 GDPR (right to rectification), as data stored on the blockchain cannot be edited. 2) Responsibilities of controllers and processors (Articles 24, 26, and 28 GDPR). Article 4 GDPR defines, inter alia, personal data, the controller, the processor, and

⁴⁴⁰ See, Rob Sumroy, Duncan Mykura and Ian Ranson, 'Blockchain and Data Protection (UK)' (*Practical Law*) <<https://uk.practicallaw.thomsonreuters.com/w-020-5436>>. 'Simply put, a blockchain is a synchronised digital database made up of a series of data blocks linked together by a cryptographic hash. One of the foundations of blockchain technology is cryptographic hashing, which uses an algorithm to convert any length of data into a random fixed-length output (that is, a "hash"). A hash of the previous block is included in each block of data in the blockchain. The blocks form a continuous, unbroken chain that is decentralised, accessible, and reliable because the previous block in the chain includes a hash of the block before that (and so on back to the first block). Each block of the chain stores a hash that acts as a fingerprint of the previous block. The previous block in the chain can then be passed through a hashing algorithm to ensure that it generates the correct hash. If the previous block is altered in any way, the correct hash will not be generated, and the chain will be broken. This is where blockchain's immutability comes from: any block in the chain's data can't be changed without changing the hash of every block after it.'

⁴⁴¹ A. B. Haque and others, 'GDPR Compliant Blockchains—A Systematic Literature Review' (2021) 9 IEEE Access 50593.

⁴⁴² For an overview of the reasons why data cannot be deleted from Blockchain, see Katie Rees, 'No, You Cannot Remove Data From the Blockchain. Here's Why.' (*MUO*, 4 August 2022) <<https://www.makeuseof.com/no-you-cannot-remove-data-from-the-blockchain-heres-why/>>.

pseudonymisation. Articles 24 and 28 GDPR further expound upon the functions and obligations of data controllers and processors. However, identifying these roles presents a particular challenge in the context of blockchain, as there is no centralised authority to oversee all the nodes.⁴⁴³ 3) Protection and privacy by design (Article 25 GDPR). Prior research has indicated that some of the privacy and protection by design compliance issues are inherent to the blockchain. Consequently, these studies have concluded that blockchain services adhere to Article 25 of the GDPR.⁴⁴⁴ The blockchain offers data immutability, confidentiality, and integrity by default, thereby safeguarding individuals' data from unauthorised access, data modification, or alteration, as well as from integrity threats. Moreover, blockchain employs cryptographic hash functions that make block data immutable. 4) Consent management (Article 7 GDPR). Users have the right to provide and withdraw consent for the processing and storage of their data. Without consent, users' data cannot be stored and processed. However, managing user consent in blockchain presents a challenge due to the absence of fixed controllers or processors, contradicting the principle of accountability. To address this issue, smart contracts have been proposed as a mechanism for consent management. 5) Data processing principles and 'lawfulness' (Articles 5, 6, and 12 GDPR). Blockchain data is distributed across network nodes, and each block utilises the hash value of the preceding block. This process continues indefinitely as

⁴⁴³ See, Fahd Saifuddin, 'Is There Any Central Authority in Blockchain Technology?' (*Blockchain Magazine*, 19 May 2022) <<https://blockchainmagazine.net/is-there-any-central-authority-in-blockchain-technology/>>.

⁴⁴⁴ See Manisha Patel, "'Privacy by Design' or Blockchain Transparency: Who Wins?' (*The Fintech Times*, 28 August 2018) <<https://thefintechtimes.com/privacy-by-design-or-blockchain-transparency-who-wins/>>. 'According to GDPR, one of the most important company obligations is secure data storage. For this purpose, the company has to implement all necessary measures and ensure safe technology for data storage. This is also called 'Data Protection by Design'. However, the design of blockchain technology aims to give a new level of transparency for customers. Every transaction is available for checking and tracking in 'blockchain explorers'. Therefore, this situation results in contradictions between GDPR approaches and blockchain principles.'

long as the chain remains unbroken. Consequently, as long as the chain remains active, block data is automatically processed. However, GDPR recommends limiting automatic data processing, collecting as little personal data as possible, and processing it to a limited scope. 6) Territorial scope (Article 3 GDPR). In the context of public blockchain, nodes are dispersed worldwide, making it challenging to prevent user data from being processed and stored outside the EU's geographic region. However, the situation differs in the case of private and federated blockchains, as nodes are distributed within a specific region.⁴⁴⁵

Although this work, based on prior research, enabled me to identify the primary discrepancies between blockchain and GDPR by identifying situations where blockchain appears to be non-compliant with GDPR provisions, there are instances, particularly with regard to point 3, where I respectfully disagree with its conclusions; the complex and decentralised nature of blockchain may actually make it more difficult for organisations to implement PbDD effectively, for example, ensuring that data protection measures are integrated into every aspect of a blockchain network can be particularly challenging given the number of nodes involved. Nevertheless, this systematic literature review was instrumental in establishing the groundwork for the ensuing discussion.

The GDPR is arguably influencing the way data is collected and stored on emerging blockchains, potentially deterring organisations from adopting blockchain-based business models and pursuing related commercial activities due to a lack of understanding about the role of the data controller in processing peer-to-peer ('P2P') data. In a decentralised process involving numerous "nodes" (computers), determining who the data controller is

⁴⁴⁵ For a discussion of public vs. private blockchain, please see Toshendra Kumar Sharma, 'Public Vs. Private Blockchain: A Comprehensive Comparison' (7 August 2019) <<https://www.blockchain-council.org/blockchain/public-vs-private-blockchain-a-comprehensive-comparison/>>.

when each node can process a single transaction data point belonging to third parties is challenging. It is possible that the legal concepts of "controller" and "processor" do not apply to the processing of blockchain data, or that all intervening nodes should be regarded as data controllers as they determine the purposes and methods of processing when deciding whether or not to update the ledger? Alternatively, the algorithm's creator, Satoshi Nakamoto in the case of Bitcoin, may be considered the controller, although this person (or persons) remains anonymous? How can an organisation monitor processing activities⁴⁴⁶ and explain such personal data flows to a supervisory authority? Given that the concept of data controller, as defined in Article 4(7) of the GDPR, does not apply, GDPR cannot be directly enforced.

In recent years, blockchain technology has gained prominence in the digital economy and it is claimed that it will 'revolutionise how business is conducted by its way of storing data and sharing it with others.'⁴⁴⁷ Bitcoin and other digital currencies are now widely used as a digital payment mechanism between businesses and individuals around the world, owing to the fact that they provide a secure online payment system that is not reliant on any central entity to facilitate the transaction, lowering the cost of sending money across borders and speeding up financial transactions. However, when bitcoin is transferred from point A to point B, it contains various items of personal data, raising concerns about how PbDD can be applied to ensure GDPR compliance.

As illustrated in the figure below, the number of business-to-business ('B2B') cross-border transactions executed on blockchain networks is anticipated to surge in the

⁴⁴⁶ GDPR, Article 30.

⁴⁴⁷ Florian Zemler and Markus Westner, *Blockchain and GDPR: Application Scenarios and Compliance Requirements* (2019).

forthcoming years. In 2020, the Asian market represented over one-third of all transactions. By 2025, the volume of cross-border B2B blockchain transactions is projected to reach an impressive 745 million. Europe is expected to be the second-largest region in terms of blockchain transactions, with the number of transactions predicted to rise to 466 million by 2025.

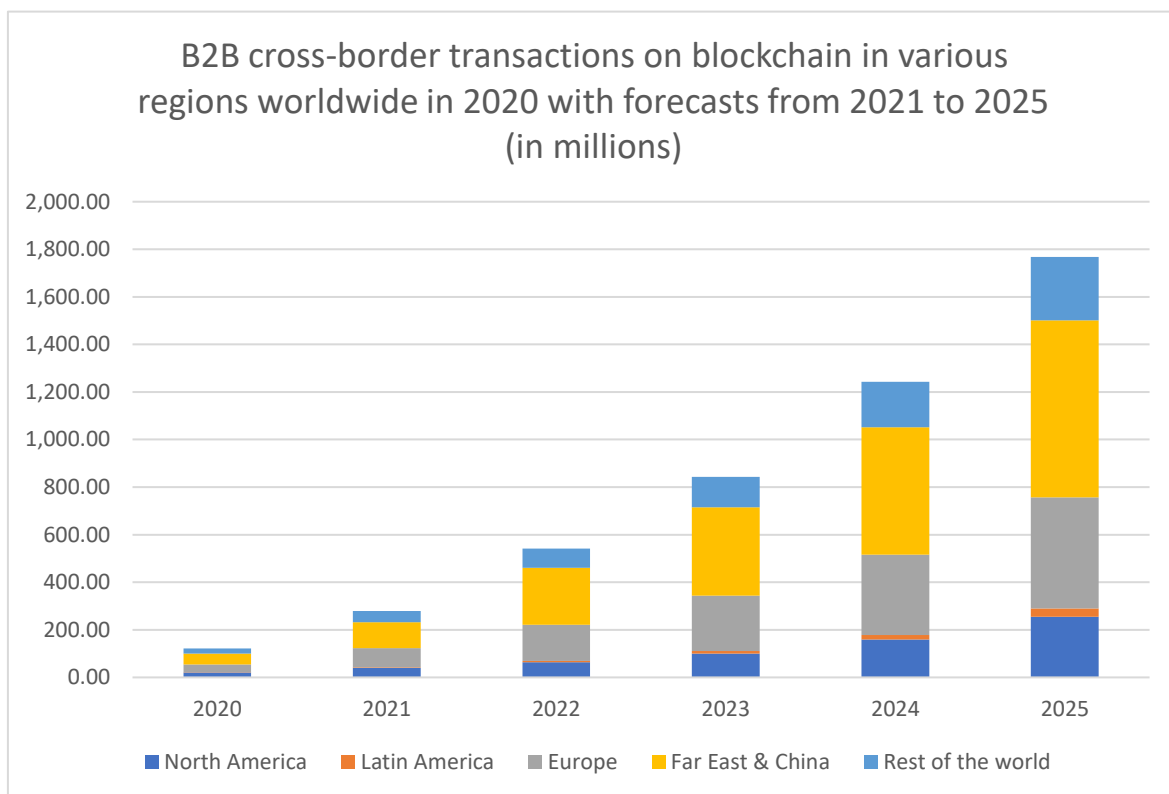


Figure 8 - Juniper Research. (March 23, 2021). B2B cross-border transactions on blockchain in various regions worldwide in 2020 with forecasts from 2021 to 2025 (in millions) [adapted]. In Statista. <<https://www.statista.com/statistics/1228825/b2b-cross-border-transactions-on-blockchain-worldwide/>>.

Bitcoin is based on blockchain technology that operates on a P2P protocol – that is, between individuals, or "peers", without the need for any "physical" central server to process or store personal data. Despite its independence from data centralisation, blockchain relies on secure cryptographed data transfers. Data is sent between parties in

"blocks," with each new block containing a cryptographic image of the previous block, ensuring that data cannot be tampered with. Any new data is then linked to the previous set of data in a continuous chain. Each user has a unique "public key" that uniquely identifies them and their account and is shared publicly in order to complete a financial transaction. This public key is linked to a "private key" that allows the account owner to decrypt the data. This process aligns with the GDPR requirements for security of processing of personal data and is unquestionably a powerful technical measure that PbDD might use to ensure the security of international data transfers. The transfer of data itself is based on a "hash" mechanism that prevents reverse engineering from locating the original data; however, a hash of a transaction, such as an identification document that was required for a transaction, is still considered personal data.

The WP29 Opinion 05/2014 on Anonymisation Techniques⁴⁴⁸ considers hash function as pseudonymisation, and 'reduces the linkability of a dataset with the original identity of a data subject; as such, it is a useful security measure but not a method of anonymisation'.⁴⁴⁹ In accordance with the GDPR, personal data that has undergone pseudonymisation remains classified as personal data. Consequently, certain data stored within the blockchain network falls under the Regulation's purview, both in the "ledger," which encompasses the hash elements of the transaction, and in the unencrypted "header," which includes text data pertaining to the transaction's date and time, as well as the originating IP address. The fact that the EU legislator has not satisfactorily addressed the processing of personal data within blockchain environments is alarming, particularly

⁴⁴⁸ Article 29 Data Protection Working Party, 'Opinion 05/2014 on Anonymisation Techniques' (WP29 2014) 0829/14/EN WP216 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf>.

⁴⁴⁹ *ibid.*

given the technology's growing significance for businesses and the obligations outlined in Article 30 GDPR to maintain a comprehensive record of processing activities.

In the wake of Schrems II, organisations are obligated to perform an individualised transfer risk evaluation, which factors in subjective considerations such as the probability of receiving a public authority access request. They must scrutinise data flows using the records of processing activities to verify the presence of sufficient protection for personal data transfers and to ensure the implementation of appropriate safeguards, which includes taking into account the intrusive surveillance laws of any potential third countries.⁴⁵⁰ The report 'Blockchain and the GDPR' from the European Union Blockchain Observatory and Forum provides a nuanced response to the question "Is there a GDPR-compliant blockchain?" The report states that 'a blockchain implementation that processes personal data can be GDPR-compliant, depending on how it is designed and used.' It goes on to explain that 'the GDPR does not forbid the use of blockchain to process personal data,' but rather requires that data protection principles, such as those related to data minimisation and storage limitation, be taken into account during the design and implementation of blockchain systems. Additionally, the report emphasises the importance of conducting a thorough DPIA before implementing a blockchain system that involves the processing of personal data.⁴⁵¹ Furthermore, it is my contention that the following statement serves to exacerbate the existing ambiguity surrounding the utilisation of blockchain technology:

⁴⁵⁰ Virgilio Emanuel Lobato Cervantes, 'The Schrems II Judgment of the Court of Justice Invalidates the EU – U.S. Privacy Shield and Requires "Case by Case" Assessment on the Application of Standard Contractual Clauses (SCCs)' (2020) 6 European Data Protection Law Review <<https://doi.org/10.21552/edpl/2020/4/18>>.

⁴⁵¹ Tom Lyons, Ludovic Courcelas and Ken Timsit, 'Blockchain and the GDPR' (European Union Blockchain Observatory and Forum 2018) <https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf>.

‘GDPR compliance is not about the technology, it is about how the technology is used. Just like there is no GDPR-compliant internet, or GDPR-compliant artificial intelligence algorithm, there is no such thing as a GDPR-compliant blockchain technology. There are only GDPR-compliant use cases and applications.’⁴⁵²

Undoubtedly, GDPR is (also) about technology. Paradoxically, although PbDD is considered technology-agnostic, processes, enterprise processing activities, systems, and applications will never be GDPR compliant if the underlying technology does not allow for its implementation; this is due Article 25 GDPR requiring the controller ‘both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate TOMs’.⁴⁵³ It is crucial for businesses to ensure that any technology they deploy, including blockchain, is privacy-friendly by accepting and incorporating data protection principles both by design and by default. Regarding the processing of personal data in the context of blockchain, the blockchain observatory noted that: (a) personal data that has been reversibly encrypted remains personal data, but in the case of hashed data, the answer will be largely determined by the sophistication of the hashing techniques used; (b) personal data should be avoided on public blockchains whenever possible, and a variety of obfuscation, encryption, aggregation, and other techniques should be implemented to anonymise such data stored on public blockchains; and (c) personal data should be collected and stored off-chain, if possible, or in private permissioned blockchain networks if this cannot be avoided.⁴⁵⁴

⁴⁵² *ibid.*

⁴⁵³ GDPR, Article 25.

⁴⁵⁴ Lyons, Courcelas and Timsit (n 443). (emphasis added).

To ascertain whether data stored on a blockchain in a hashed format qualifies as personal data, a technical evaluation is necessary. Nonetheless, it is advisable to take a cautious approach and consider such data as personal data if it, when combined with other information, can lead to the identification of a living individual.⁴⁵⁵ Despite the considerable technical challenge involved in reverse engineering the hashed data and linking it to a particular individual within the blockchain, the data will be categorised as pseudonymous data, and the GDPR will apply as if it were personal data unless it is irreversibly anonymised.⁴⁵⁶ In *Breyer*,⁴⁵⁷ the CJEU explained that personal data will be considered anonymised where identifying a data subject would be ‘practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant.’⁴⁵⁸ Furthermore, the Article 29 Working Party in its Opinion 05/2014,⁴⁵⁹ has come to the conclusion that in order for data to be considered anonymous, the anonymisation technique used must be irreversible.

In the context of the public blockchain system, it is essential to recognise that a wide range of data, including personal and special categories of data, is processed. Therefore, it is crucial to incorporate technological mechanisms within the processing workflow to enable the implementation of PbDD and PETs. Such measures must ensure

⁴⁵⁵ See GDPR, Recital 26. ‘[T]o determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly.’

⁴⁵⁶ *ibid.* ‘Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person.’

⁴⁵⁷ *Breyer [2016]* (n 277).

⁴⁵⁸ *ibid.*

⁴⁵⁹ Article 29 Data Protection Working Party, ‘Opinion 05/2014 on Anonymisation Techniques’ (n 440).

that the privacy rights and freedoms of data subjects are constantly protected against unauthorised interference or theft. It is highly unlikely that organisations will be able to process their blockchain transactions in compliance with the GDPR without appropriately addressing and clarifying these issues.

In 2018, CNIL published a document titled ‘Solutions for a Responsible Use of Blockchain in the Context of Personal Data’,⁴⁶⁰ which made a significant contribution to the ongoing discussion around the use of blockchain technologies for processing personal data and the implications for GDPR compliance. It is noteworthy that, prior to this report, no data protection regulator in the European Union had released a similar analysis. The report recognises the fact that GDPR was designed for a world in which data management was centralised within an organisation, which raises concerns about its applicability to decentralised systems such as blockchain.⁴⁶¹ The CNIL acknowledges the complexities and conflicting aspects that arise from the interplay between the GDPR in its current state and the advancements of blockchain applications. This perspective is shared by numerous privacy practitioners and scholars who are concerned about the compatibility of this technology with data protection Regulations.⁴⁶² The decentralised nature of blockchain,

⁴⁶⁰ Commission Nationale de l’Informatique et des Libertés (CNIL), ‘Blockchain and the GDPR: Solutions for a Responsible Use of the Blockchain in the Context of Personal Data’ (*Blockchain*, 6 November 2018) <<https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data>>.

⁴⁶¹ It is evident that the blockchain's decentralised nature is the primary reason why PbDD (whose implementation and ongoing maintenance is centralised in the data controller) is incompatible with this technology.

⁴⁶² See, e.g., Robert Herian, ‘Blockchain, GDPR, and Fantasies of Data Sovereignty’ (2020) 12 *Law, Innovation and Technology* 156. ‘Impacts from GDPR versus blockchain remain inconclusive. What is obvious already however is the desire some blockchain stakeholders have to exploit, as best they can, uncertainties existing within the four corners of the GDPR using know-how, or what Biegel calls ‘the ability to resist’ that comes from understanding a technology, its capabilities and limitations, better than the regulator. Thus while the regulation is forcing compliance to some extent, it is by no means watertight and concerns for regulators ought to surround greater desires of stakeholders to undermine the regulations rather than comply with

which is a fundamental characteristic, poses a significant challenge to the GDPR. It is important to note that there is no central node operating on blockchain networks, and instead, each blockchain network is comprised of decentralised nodes adding data to and processing data from the network. However, data controllers are still responsible for using personal data in accordance with GDPR. This raises the question of who can be considered a data controller in the context of blockchain. According to the CNIL, participants who have the right to write on the blockchain and send data for validation to the miners can be considered as "data controllers." While there are recognised differences in roles between data controllers and data processors, the current nature of blockchain networks may lead to a variety of entities being considered data controllers.⁴⁶³

It is undeniable that certain individual rights granted by the GDPR can be compatible with blockchain technology, including the right to information, access, and portability, which can be incorporated into blockchain technology through PbDD. However, there are significant challenges in the context of an immutable and append-only ledger, particularly the inability to facilitate the data subject's right to be forgotten. This represents a significant departure from the GDPR's obligations to uphold the data subject's rights to rectification and erasure, as they are inconsistent with a system whose most important attribute is the absolute and unchangeable nature of the data it processes. Additionally, blockchain-based projects argue that they are too decentralised to identify data controllers or to take responsibility for implementing data subject rights, which creates further inconsistencies. Furthermore, PbDD is unable to incorporate the necessary TOMs to ensure

them. Test cases in the coming months and years will necessarily interpret the regulation further, and these cases are guaranteed to involve blockchain as long as stakeholders push concepts and use-cases to the limits of compliance.'

⁴⁶³ Commission Nationale de l'Informatique et des Libertés (CNIL) (n 452).

that personal data is only collected, processed, and retained for explicit, legitimate, and specific purposes (principle of purpose limitation). The blockchain process automatically replicates data across all network nodes, making it impossible to guarantee that data is not 'further processed' after being written to a ledger. Finally, the principle of storage limitation requires that personal data should not be stored in a form that allows for identification of data subjects for longer than is necessary for the purpose for which it is processed, which necessitates a clearly defined retention period, logical justification, periodic reviews, and deletion or anonymisation after a valid and justified retention period. Unfortunately, blockchain technology is currently unable to allow PbDD to address these tasks.

The transnational nature of many blockchain activities necessitates consideration of how to ensure compliance with the GDPR's cross-border data transfer provisions. While data subject consent may seem like a potential solution, practical issues arise such as the ability to revoke consent and the inability to seek consent from all data subjects. Additionally, revocation would necessitate the deletion of data from the ledger, which is technically impossible.

The review of blockchain characteristics and their compatibility challenges with PbDD underscores the need to harmonise law and technology to establish a shared foundation for developing GDPR-compliant blockchains.⁴⁶⁴

⁴⁶⁴ This is a critical area for future development, and an in-depth examination of the issues raised - including blockchain fundamentals and GDPR principles - is expected to grow alongside the continued adoption of this technology in Europe by both businesses and individuals. The emergence of blockchain technology as an innovative and increasingly important tool across a wide range of sectors, from health to finance, underscores the pressing need for an in-depth examination of the challenges surrounding privacy and data protection law. While the implementation of PbDD in the context of blockchain may pose challenges, it is without question the approach that best protects the rights and freedoms of data subjects.

The EPTA project report, 'Blockchain and the General Data Protection Regulation',⁴⁶⁵ released in July 2019, offers an in-depth analysis of the relationship between blockchain technology and the GDPR, highlighting the existing tensions and potential solutions. The report focuses on developments up to March 2019, and it concludes that blockchain technology has been proposed as a possible mechanism for achieving some of the GDPR's primary goals. Blockchain technology has emerged as a promising tool for data governance, providing various advantages over existing alternatives. Paradoxically, one of the key benefits is the potential to enable decentralised data exchange without relying on a trusted intermediary. Additionally, blockchains can enhance transparency into data access and automate data transfer, reducing transaction costs. The crypto-economic incentive structures within blockchains may also have transformative effects on the global economy. As such, blockchain technology may offer significant benefits to the modern data economy and contribute to the advancement of AI in the European Union. The features inherent in blockchain technology can serve as a valuable tool in facilitating several of the objectives set forth by the GDPR, including empowering individuals with greater agency over their personal data, whether directly or indirectly related. Furthermore, the utilisation of blockchain technology may aid organisations and governmental entities alike in the identification and prevention of data breaches and fraudulent activity.⁴⁶⁶

⁴⁶⁵ Michèle Finck, 'Blockchain and the General Data Protection Regulation - Can Distributed Ledgers Be Squared with European Data Protection Law?' (2019) <<https://eptanetwork.org/database/policy-briefs-reports/1796-blockchain-and-the-general-data-protection-regulation-can-distributed-ledgers-be-squared-with-european-data-protection-law-stoa>>.

⁴⁶⁶ *ibid.*

5.2. Is PbDD a mirage, given that GDPR undervalues IoT, a technology that supports over thirty billion devices?

The march of technological progress has left an indelible mark on the global economy in recent times. The advent of the internet economy ushered in a new era of interconnectedness, enabling organisations to revolutionise the way they communicated, collaborated, and delivered their products and services. In subsequent years, the data economy emerged as a major force, with an ever-increasing reliance on personal data and sophisticated data analytics to drive informed decision-making. Among the most conspicuous manifestations of the data economy has been the rapid proliferation of the IoT, with its attendant innovations such as smart homes, smart cities, health and fitness wearables, and the development of advanced industrial applications such as smart factories.⁴⁶⁷ The pervasive adoption of IoT is a testament to the central importance of data science in contemporary technological innovation. A growing number of devices, ranging from commonplace items like light bulbs, clothing, refrigerators, and bicycles to specialised containers, are now interconnected to the internet, generating vast amounts of data. These devices are increasingly imbued with intelligence, as they learn and adapt from the data they capture on a real-time basis, ultimately transitioning into "smart" entities; '[T]he Internet of Things (IoT) depends on the whole data science pipeline [...]. We are (or will be)

⁴⁶⁷ Eline Chivot and Daniel Castro, 'The EU Needs to Reform the GDPR To Remain Competitive in the Algorithmic Economy' (*Artificial Intelligence*, 13 May 2019) <<https://datainnovation.org/2019/05/the-eu-needs-to-reform-the-gdpr-to-remain-competitive-in-the-algorithmic-economy/>>.

surrounded by smart devices collecting data and the impact of this cannot be overestimated.⁴⁶⁸

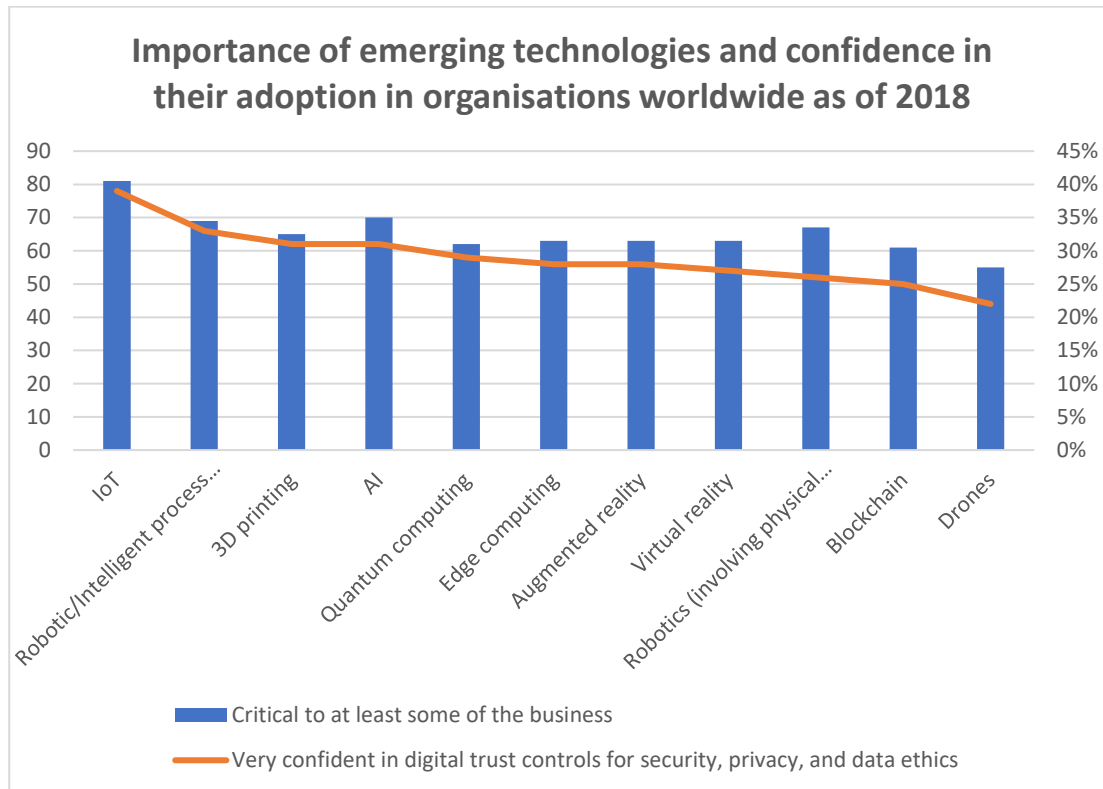


Figure 9 - PwC. (November 7, 2018). Importance of emerging technologies and confidence in their adoption in organisations worldwide as of 2018 [adapted]. In Statista. <<https://www.statista.com/statistics/945047/worldwide-emerging-technology-importance-confidence/>>.

The significance of emerging technologies and organisations' confidence in their adoption is effectively illustrated in Figure 9, which displays data from 2018. Despite roughly 81 percent of respondents affirming IoT's importance to their business in some capacity, only 39 percent reported high levels of confidence in digital trust controls that ensure security,

⁴⁶⁸ Wil MP van der Aalst, 'Responsible Data Science in a Dynamic World: The Four Essential Elements of Data Science', *IFIP Advances in Information and Communication Technology* (2019) <<https://go.exlibris.link/t3HD9bDW>>. (emphasis added).

privacy, and ethical data practices for IoT technology. These findings raise cause for concern, particularly in light of the GDPR's implementation. IoT denotes a network of devices and objects that can independently communicate data with one another, typically to collect, analyse, and act upon information. IoT applications can be found in a variety of technologies such as smart wearables, smart homes, and telematics (e.g., insurance vehicle black boxes). As such, the majority of data processing activities involved in IoT operations will be subject to the provisions of the GDPR. Consequently, PbDD plays a crucial role in this context, as data protection must be integrated into the development of any IoT system from inception, remaining operational throughout its lifecycle. The design of the IoT product should incorporate transparency, fairness, purpose limitation, data minimisation, data accuracy, and the capacity to fulfil data subject rights as part of the PbDD programme. Therefore, a judicious appraisal of how to balance the advantages of this evolving technology with potential risks to individuals is warranted.

Furthermore, as a technology with a high potential for becoming a Privacy-invading technology,⁴⁶⁹ and frequently processing special categories of personal data, one might wonder what role PbDD plays in this context.

There are compelling reasons why policymakers should give due consideration to the implementation of PbDD in the specific context of IoT. One such example is that of smart wearables, which have the capacity to gather data that, over time, may reveal an individual's health status. In such cases, it is imperative to incorporate a PbDD mechanism to govern the collection and subsequent processing of this data in compliance with both

⁴⁶⁹ Demetrius Klitou, 'Privacy by Design and Privacy-Invasive Technologies: Safeguarding Privacy, Liberty and Security in the 21st Century' (2011) 5 *Legisprudence* 297.

Articles 6 and 9 of the GDPR. This is because certain forms of health data can be linked to vulnerable data subjects and may have the potential to trigger discriminatory actions by data controllers, particularly if the data is utilised to infer an individual's well-being for insurance purposes. Wearables have attracted attention in the context of data processing, as evidenced by the Fitbit data processing incident that surfaced following a murder in Connecticut in 2015.⁴⁷⁰ Prosecutors utilised Fitbit's GPS data to bolster their case, which facilitated the identification of the victim's last movements and substantiated the involvement of the victim's husband in the crime. While one could argue that this deployment of technology resulted in a just outcome, it is essential to implement precise TOMs to ensure transparency. Without such measures, IoT could evolve into, yet another tool used to infringe upon the privacy rights of individuals, ultimately resulting in a society where the "Big Brother is (always) watching (you)."

An additional instance of IoT's involvement in a criminal case⁴⁷¹ arose in Arkansas, US, which garnered significant media attention. In this case, Bates was charged with first-degree murder in the death of Collins, who was discovered face down in Bates' hot tub. The Amazon Echo smart speaker became implicated in the investigation after a witness reported hearing music streaming through the device on the night of Collins' death. Media reports indicated that Amazon challenged the prosecution's request to provide access to the device's recorded data for that night. Eventually, Bates consented to furnish the recordings, rendering the dispute moot. The judge dismissed the case due to insufficient

⁴⁷⁰ Christine Hauser, 'In Connecticut Murder Case, a Fitbit Is a Silent Witness' (*New York*, 27 April 2017) <<https://www.nytimes.com/2017/04/27/nyregion/in-connecticut-murder-case-a-fitbit-is-a-silent-witness.html>>.

⁴⁷¹ Nicole Chavez, 'Arkansas Judge Drops Murder Charge in Amazon Echo Case' (*Crime + Justice*, 2 December 2017) <<https://edition.cnn.com/2017/11/30/us/amazon-echo-arkansas-murder-case-dismissed/index.html>>.

evidence to convict Bates "beyond a reasonable doubt." Despite the dismissal of the case, it is noteworthy that the incident generated significant media coverage, resulting in the public exposure of the defendant's personal life. The absence of adequate privacy protection in this case can be attributed to a technological incompatibility with PbDD. Specifically, the Amazon Echo smart speaker, by default, continuously listens for the wake word "Alexa" or "Amazon," and subsequently records and analyses the user's voice to perform tasks or provide information. This highlights the importance of incorporating PbDD into the design of IoT devices to mitigate potential privacy risks and to safeguard the privacy rights of data subjects.

The use of IoT also carries with it significant potential risks in terms of user data security, primarily due to the inadequate implementation of PbDD or the immature state of related technology. Another challenge that exacerbates the PbDD implementation challenge is the prevalence of cameras in many consumer IoT products, which hackers can easily exploit. For instance, Pen Test Partners recently identified a critical security flaw in a Swann IoT video camera,⁴⁷² which enabled a hacker to gain access to video footage from another user's camera. By entering a serial number into a mobile phone app, a live video feed from the camera could be immediately accessed (serial numbers are readily available), underscoring the need for effective privacy protection measures to be embedded within IoT devices.

⁴⁷² Andrew Tierney, 'Hacking Swann & FLIR/Lorex Home Security Camera Video' (*Internet of Things*, 26 July 2018) <<https://www.pentestpartners.com/security-blog/hacking-swann-home-security-camera-video/>>.

In 2015, Rapid7 discovered that 8 out of 10 baby monitors failed to meet security compliance standards.⁴⁷³ To this day, various well-known vulnerabilities continue to plague consumer IoT products,⁴⁷⁴ with manufacturers unable to address them, despite the implementation of GDPR. These vulnerabilities stem from issues such as unencrypted communication channels and APIs, rendering cameras susceptible to interception and hijacking. As such, the lack of adequate PbDD implementation in IoT systems underpins the root cause of these security flaws.

The Global Privacy Enforcement Network conducted a study in 2016,⁴⁷⁵ which revealed that the majority of IoT devices fail to provide clear explanations to individuals about the processing of their personal data, particularly with respect to identifying third parties involved in data processing (e.g., hardware manufacturers, IoT system providers, software providers, mobile network operators, app developers). Hence, ascertaining whether a party is acting as a data controller or data processor poses a significant challenge in the IoT context. In this regard, the WP29 underscored the necessity for a distinct allocation of legal responsibilities amongst the various parties involved in the processing of personal data, considering the characteristics of each party's involvement in the system. This is highlighted in its opinion on 'Recent Developments on the Internet of Things',⁴⁷⁶

⁴⁷³ Mark Stanislav and Tod Beardsley, 'HACKING IoT: A Case Study on Baby Monitor Exposures and Vulnerabilities' (2015) <<https://www.rapid7.com/globalassets/external/docs/Hacking-IoT-A-Case-Study-on-Baby-Monitor-Exposures-and-Vulnerabilities.pdf>>.

⁴⁷⁴ Larisa Brown, 'Beware the Spy in Your Baby Monitor and Smart Camera' (*Mail Online*, 3 March 2020) <<https://www.dailymail.co.uk/news/article-8067561/Beware-spy-baby-monitor-smart-camera-security-chiefs-warn-cyber-crooks-hack-them.html>>.

⁴⁷⁵ GPEN, '2016 GPEN Sweep Internet of Things [with a Focus on Accountability]' (2016) <<https://ico.org.uk/media/about-the-ico/disclosure-log/1625142/irq0648379-attachment.pdf>>.

⁴⁷⁶ Article 29 Working Party, 'Opinion 8/2014 on the on Recent Developments on the Internet of Things' 14/EN WP 223 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm>.

wherein the WP29 emphasised the importance of a clear and unambiguous division of responsibilities to ensure compliance with data protection principles in the context of IoT. According to WP29, device manufacturers qualify as controllers for the personal data generated by their devices, as they design the operating system or determine the overall functionality of the installed software. As such, they bear a clear obligation to implement PbDD under Article 25 of the GDPR. Additionally, third-party app developers who create interfaces enabling individuals to access data stored by the device manufacturer are also considered data controllers and therefore bear responsibility for implementing suitable TOMs to uphold data protection principles and integrate safeguards that protect the rights of individuals and comply with GDPR requirements. When IoT devices are employed to collect and process personal data, all other third parties involved in the processing chain must also be viewed as data controllers. These third parties typically use the data collected by the device for purposes other than those of the device manufacturer. This implies that other stakeholders, such as IoT data platforms and social platforms, may also be classified as controllers for the processing activities over which they have authority. Conversely, they may be considered data processors if they process data on behalf of another IoT stakeholder serving as a controller. Consequently, the existence of gaps in the implementation of PbDD in the complex IoT processing network is surprising and can result in such explicit privacy breaches as exemplified in the case of the baby monitors mentioned earlier.

Despite significant technological advancements in the intervening years since 2014, the IoT remains in a similar technological and legal context. As the director of the UK

National Cyber Security Centre (NCSC) pointed out, these devices are vulnerable to cyber-attackers, despite being 'fantastic innovations.'⁴⁷⁷

The implementation of PbDD in IoT gives rise to a fresh set of significant privacy and data protection challenges, which are further amplified by the exponential increase in data processing associated with its ongoing evolution. Some of these challenges include: a) Data subject's loss of control over their data - As technology is required to provide pervasive services in an unobtrusive manner, personal data can be transferred for monitoring, storage, or further processing to third parties, which may result in data subjects losing control over their data; b) Quality of the individual's consent - In many cases, individuals may be unaware that specific devices are processing their data, hindering their ability to give valid consent under the GDPR, as data subjects must be fully informed about the processing before their data are processed; c) Inferences derived from data - The vast amount of data generated by the IoT (sometimes in conjunction with big data analysis) can be used to make inferences about personal aspects of an individual's life; d) Repurposing of original processing for secondary purposes - Third parties may gain indirect access to information and use it for purposes other than those for which it was originally collected, such as marketing; e) Profiling and intrusive elicitation of behavioural patterns - A sufficient amount of data collected by different devices can reveal specific aspects of an individual's habits, behaviours, and preferences; f) Losing anonymity - Wearable items kept close to data subjects may result in identifiers, such as the MAC addresses obtained from other devices, which could be used to generate a fingerprint allowing individuals' location

⁴⁷⁷ 'Smart Camera and Baby Monitor Warning given by UK's Cyber-Defender' *BBC News* (3 March 2020) <<https://www.bbc.com/news/technology-51706631>>.

tracking; and g) Security risks - The IoT poses several security challenges. Security and resource constraints force device manufacturers to balance battery efficiency and device security, leading to potential vulnerabilities.

In summary, the IoT poses a unique set of challenges in implementing PbDD due to the various risks associated with data collection, processing, and storage, which must be carefully addressed to ensure compliance with data protection principles and safeguard the privacy rights of data subjects.

Efforts have been made to ensure GDPR compliance in IoT applications. For example, Kannen and Petrakis, 'advocate that compliance must be considered in the design phase of the system, by analysing the dependencies between system entities (e.g., personal data, users etc.) and the processes enacted upon them.'⁴⁷⁸ They propose a methodology for achieving compliance for IoT applications, demonstrating how PbDD can be engineered to be systemically embedded in IoT system design processes. The authors demonstrate how PbDD can be systematically embedded into the design processes of IoT systems to achieve compliance. While their methodology may not offer a comprehensive study of GDPR (or PbDD) implementation in the IoT context, as it only focuses on data protection principles and individual rights, it provides a foundation for future research in this area.⁴⁷⁹

⁴⁷⁸ Christos Karageorgiou Kaneen and Euripides GM Petrakis, 'Towards Evaluating GDPR Compliance in IoT Applications' (2020) 176 Knowledge-Based and Intelligent Information & Engineering Systems: Proceedings of the 24th International Conference KES2020 2989.

⁴⁷⁹ In the current technological landscape, it is paramount to identify and evaluate potential privacy hazards in relation to the ever-evolving IoT and the existing EU regulatory framework. As previously noted, IoT has significantly amplified the risk of identification, tracking, and profiling of individuals, which can be especially perilous with the predicted evolution of the technology. Consequently, it is necessary to address both legal and technical challenges specific to each threat and provide unambiguous guidelines for the lawful deployment of IoT, including the incorporation of privacy defence mechanisms through PbDD.

Chaudhuri and Cavoukian propose a proactive and preventive approach for enabling privacy in the context of IoT, which they call the 'Proactive and Preventive Privacy (3P) Framework.'⁴⁸⁰ They argue that the technology of IoT has not yet matured enough to standardise security and privacy requirements, and therefore, their user-centric approach prioritises privacy, security, and safety in a "win-win" positive outcome for all business domains.^{481,482}

To mitigate the impact of privacy breaches in IoT systems, it is crucial to proactively anticipate and address potential threats during the design and development phases. A constructive outcome for all stakeholders can be achieved by adopting a win/win approach. Central to this approach is the prioritisation of end-user requirements and interests in IoT device and service designs, through the implementation of a 'Users First' strategy. By prioritising user needs, trust and confidence in IoT offerings can be established, resulting in wider acceptance of these technologies.⁴⁸³

Whilst this framework is undoubtedly a valuable contribution towards integrating PbDD into IoT technology, my critique pertains mainly to the limitations of its full functionality. Specifically, there appears to be an excessive reliance on risk mitigation

⁴⁸⁰ Abhik Chaudhuri and Ann Cavoukian, 'The Proactive and Preventive Privacy (3P) Framework for IoT Privacy by Design' (2018) 57 EDPACS 1.

⁴⁸¹ Kaneen and Petrakis (n 470).

⁴⁸² The 3P Framework is based on Cavoukian's "Privacy by Design" principles and incorporates adaptive principles, which include: (1) Proactively Prevent Privacy Invasive IoT Events; (2) Ensure IoT Privacy by Default; (3) Embed Privacy Enhancing Capabilities into IoT Service Design and Device Architecture; (4) Adopt a Stakeholder Approach to IoT Privacy for Full Functionality, Positive Sum Outcome; (5) Provide Full Lifecycle Protection of IoT Data for End-To-End Security and Privacy; (6) Opt for a Verification Based Trust Approach to IoT; and (7) Consider Users at the Core of IoT Services. One key feature of this framework is the use of privacy-enhancing technologies (PETs) built into IoT devices to prevent privacy infringements, acting as a PbD "firewall" to protect users' data. Overall, this framework presents an innovative and promising approach to tackling the privacy and security challenges of the IoT era. In my opinion, it is deserving of consideration by legislators.

⁴⁸³ Chaudhuri and Cavoukian (n 472).

approaches, which could potentially result in a failure to fully comply with the requirements set forth by the GDPR. Furthermore, there is an insufficient emphasis on the legal scope of the framework, including a lack of consideration for data protection principles and data subjects' rights.

My suggestion would be to adopt a derived approach: the first step in developing a PbDD strategy for IoT should involve identifying a suitable legal basis for processing data.⁴⁸⁴ In accordance with Article 6 of the GDPR, data controllers are required to ensure that any processing of personal data is lawful. In the context of IoT, the following legal bases are potentially relevant: i) Consent (Article 6(1)(a) GDPR), which should be primarily relied upon; ii) Performance of a contract (Article 6(1)(b) GDPR), which is subject to the "necessity" criterion, requiring a direct and objective relationship between the processing and the expected contractual performance from the data subject; and iii) Legitimate interests (Article 6(1)(f) GDPR), which allows for the processing of personal data where it is necessary for the legitimate interests of the controller or a third party, unless such interests are overridden by the interests or fundamental rights and freedoms of the data subject, particularly where the data subject is a child.⁴⁸⁵

Secondly, it should consider the data quality principle (this is where the Proactive and Preventive Privacy (3P) Framework can add value in the context of PbDD

⁴⁸⁴ See Article 29 Working Party (n 468). 'In its judgment in the Google Spain case, the European Court of Justice has provided substantial guidance in this respect, in addition to the one already provided in the previous joint cases ASNEF and FECEMD (C-468/10 and C-469/10). In the context of IoT, the processing of individuals' personal data is likely to have a significant impact on their fundamental rights to privacy and to the protection of personal data in situations where data could not have been interconnected or only with great difficulty without IoT devices. Such situations may arise when the data collected relates to the individual's state of health, home or intimacy, location, and a variety of other aspects of their private life. Given the potential severity of that interference, it is clear that such processing will be difficult to justify solely on the basis of an IoT stakeholder's economic interest in that processing.'

⁴⁸⁵ GDPR, Article 6(1)(f).

implementation), which combined with the other principles enshrined in Article 5 GDPR, form a cornerstone of EU data protection law: personal data should be collected and processed fairly and lawfully. This approach is particularly important in the context of IoT since sensors are designed to be as inconspicuously as possible and (all) data controllers operating in the IoT offer must notify individuals when data is being collected about them (or those around them). Compliance with this principle is more than just a legal requirement, as fair collection is an expectation of data subjects, especially when it comes to wearable computing.

According to the purpose limitation principle, data can only be collected for specific, explicit, and legitimate purposes. Any further processing deemed incompatible with the original purpose is unlawful under GDPR. This principle empowers individuals by enabling them to understand how and why their data is being used, and to decide whether or not to entrust their data to a data controller. These purposes must be thus identified and addressed by the PbDD programme before any data processing. In addition, the personal data collected should be only the strictly necessary for the purpose determined by the data controller (principle of data minimisation). Data that is unnecessary for this purpose should not be collected just in case it might be useful later. Some argue that the principle of data minimisation could limit the IoT potential and thus act as a barrier to innovation, based on the idea that potential benefits of data processing would result from an exploratory analysis aimed at uncovering non-obvious correlations and trends.⁴⁸⁶ Therefore, if data

⁴⁸⁶ The WP29 does not share this view and insists that the principle of data minimisation plays an essential role in protecting the data protection rights afforded to individuals by EU law and as such should be respected. In particular, this principle implies that when personal data are not required to provide a specific service performed on the IoT, the data subject should at least be given the opportunity to use the service anonymously. See Article 29 Working Party (n 468) 29.

minimisation is strictly adhered to, valuable insights may be missed, and the potential benefits of IoT may not be fully realised. In other words, the argument suggests that limiting data collection and processing through data minimisation, could lead to a missed opportunity to unlock valuable insights and innovation that could come from exploring large amounts of data.

Article 5 of the GDPR requires that personal data collected and processed in the context of the IoT must not be kept for longer than necessary to fulfil its intended purpose, thus ensuring adherence to the principle of storage limitation. Given the variance in the objectives of data processing across different service providers in the IoT ecosystem, it is imperative that all involved parties conduct a comprehensive evaluation of the appropriateness of data retention for their respective services. In this regard, a cooperative approach to PbDD may be adopted by the “chain-controllers,” which includes carrying out a collective DPIA and identifying effective TOMs for ensuring GDPR-compliant security and information management throughout the various stages and facets of IoT processing.

In accordance with Article 13 GDPR, data controllers must also communicate specific information to data subjects, including the identity of the controller, the purposes of the processing, the recipients of the data, the existence of their rights of access, erasure of personal data (including information on how to disconnect or unlink the device to prevent further data processing), and the right to portability.

In accordance with the principle of fair processing, this information must be provided in a clear and understandable manner, which raises a question of technical feasibility. It will be difficult for the various “chain-controllers” to comply with the data protection principles unless the legislator, or regulators, provide a clear indication of how to deliver the information to IoT users, including specific sensor users. Furthermore, if the

GDPR aims to effectively address and remedy this challenge, it may be necessary for the legislator to forego the principle of technological neutrality. This is because the solution to the problem may entail the adoption of very precise technical measures, which may not align with the principle of neutrality.⁴⁸⁷

IoT controllers are obligated to adhere to the provisions set forth in Articles 15 to 22 of the GDPR, which stipulate the rights of data subjects, and to implement appropriate organisational measures to fulfil these obligations. These rights extend to all individuals whose personal data is processed and are not confined to IoT service subscribers or device owners. Moreover, data subjects have the right to retract previously provided consent for specific data processing and to raise objections against the processing of their personal data. The unfettered exercise of these rights is crucial, and any technical or organisational barriers that obstruct their implementation must be removed. Additionally, tools for registering the revocation of consent must be readily accessible, transparent, and effective.⁴⁸⁸

To conclude, the nascent stage of IoT technology notwithstanding, the security and privacy concerns that accompany the diverse IoT apps, sensors, and devices currently

⁴⁸⁷ The GDPR recognises the need for a technological neutral approach to data protection, which permits organisations to develop their own solutions and technical measures for complying with the Regulation. However, this approach may not always be feasible, especially in complex technological environments like the IoT. To ensure that IoT users are equipped with clear and comprehensive information, it is essential that regulators provide specific guidelines on the implementation of appropriate measures that are tailored to the IoT ecosystem.

⁴⁸⁸ As previously mentioned, PbDD should entail the inclusion of collective DPIAs to be conducted prior to the launch of new IoT applications. Controllers may also contemplate the possibility of making relevant assessments available to the public, where appropriate. For more intricate IoT systems, it may be necessary to create specific "framework based" DPIAs. In most cases, it is advisable for IoT controllers to employ aggregated data instead of identifiable (raw) data that is collected from IoT devices, and to consider deleting raw data once the necessary information for data processing has been extracted. Deletion should take place at the earliest stage of data collection, and PbDD measures that empower data subjects, such as mechanisms to access or delete data, should be incorporated. The criterion of data self-determination must apply in full, as data subjects should be able to exercise their rights at all times and be de facto in control of their data.

available in the market are widely acknowledged. Therefore, it is imperative to address the legal aspects of IoT devices with alacrity to enable the complete realisation of their potential. One of the critical legal aspects of IoT devices is GDPR, which stipulates stringent data protection measures that IoT controllers must comply with. However, the inherent complexity of IoT systems and the diverse entities involved in their development and implementation present significant challenges in adhering to the GDPR's requirements. Moreover, the absence of clear and comprehensive guidelines regarding how to implement data protection measures in the IoT ecosystem further exacerbates the situation.

A solution to this challenge would involve the creation of regulatory measures that are specifically tailored to the IoT environment. For instance, the development of a comprehensive legal framework that outlines the various data protection measures that IoT controllers should implement, as well as clear guidelines for their implementation, would be a significant step towards ensuring data protection compliance in IoT devices. Additionally, regulators could facilitate the adoption of a cooperative approach to PbDD among the various stakeholders in the IoT ecosystem, which would promote transparency and accountability in the implementation of data protection measures.

5.3. Artificial Intelligence and big data: Quo vadis?

In the last decade, much research has focused on the impact of artificial intelligence (AI) on society, addressing ethical and legal issues, including those related to data protection. According to the EDPB, processing of personal data through an algorithm falls within the

scope of GDPR.⁴⁸⁹ Therefore, whenever AI systems use personal data, the GDPR applies. AI relies heavily on data – particularly on personal information, as organisations seek to create, inter alia, added value and customer loyalty through automation. Previous research has identified some tensions between AI technology and the incorporation of data protection principles in AI data processing activities, namely: (i) the transparency principle - the EU's guidelines clarify that although complete disclosures of the algorithms are not necessary, the information provided should be sufficiently comprehensive for the data subject to understand the reason for the decision. Because of the technical nature of AI technologies, it can be difficult for controllers to be transparent about the rationale behind AI operations.

In its report on 'Big Data, Artificial Intelligence, Machine Learning, and Data Protection',⁴⁹⁰ the UK supervisory authority highlights the potential opaqueness of big data analytics processing for citizens and consumers whose data is employed. Additionally, the fairness principle dictates that the processing of personal information should be conducted while respecting the data subject's interests and in line with their reasonable expectations. To ensure compliance, data controllers must put in place measures that forestall arbitrary discrimination against data subjects. Similarly, the Norwegian supervisory authority, cited in the WLC blog, observes that algorithms and models are not inherently objective and may carry the biases of their designers or builders. The personal data used for training may result in incorrect or discriminatory outcomes if it presents a biased representation of

⁴⁸⁹ Andrea Jelinek, 'EDPB Response to the MEP Sophie in't Veld's Letter on Unfair Algorithms' (October 2020) <https://edpb.europa.eu/sites/default/files/files/file1/edpb_letter_out2020_0004_intveldalgorithms_en.pdf>.

⁴⁹⁰ ICO, 'Big Data, Artificial Intelligence, Machine Learning, and Data Protection' <<https://ico.org.uk/media/for-organisation/documents/2013559/big-data-ai-ml-and-data-protection.pdf>>.

reality or is irrelevant to the area under consideration. The use of such personal data would run counter to the fairness principle; '[T]he model's result may be incorrect or discriminatory if the training data renders a biased picture reality, or if it has no relevance to the area in question. Such use of personal data would be in contravention of the fairness principle.'⁴⁹¹ Furthermore, GDPR mandates that data subjects be informed about the purpose of data collection and processing. This could pose a challenge for AI-powered solutions since data is used to identify patterns and derive insights that may not be compatible with the original purpose of data collection. For instance, using social media data to calculate insurance rates. Under GDPR, data can only be processed further if the new purpose is compatible with the original one or the data controller obtains additional consent from the data subject.

AI technology also has a notable impact on individuals' rights, particularly the right to be forgotten. Using AI, input data is scrutinised to identify patterns that enable the system to generate outcomes relevant to its intended purpose. As data volumes grow, algorithms improve, and the conclusions they generate are either corroborated or enhanced. However, the patterns discovered by the original data set persist and are employed to make more accurate predictions on subsequent data sets. From a PbDD perspective, this presents a challenge, as the right to be forgotten suggests that after erasure, the data's use comes to an end, and the data subject is effectively forgotten, which is not technically feasible.

⁴⁹¹ 'Artificial Intelligence and the GDPR: Incompatible Realities?' (*White Label Consultancy*, 31 March 2021) <<https://whitelabelconsultancy.com/2021/03/artificial-intelligence-and-the-gdpr/>>.

AI technology relies on the systematic (and correlative) analysis of vast quantities of data to provide results, a processing that is commonly referred to as big data analytics. Sandra Wachter and Brent Mittelstadt, argue that 'data protection law is meant to protect people's privacy, identity, reputation, and autonomy, but is currently failing to protect data subjects from the novel risks of inferential analytics.'⁴⁹² This statement raises the critical issue of unethical use of personal data by global organisations such as Facebook, which have been granted permission to use their "oceans" of personal data in ways that the EU legislator could not have imagined when drafting the GDPR.

The Cambridge Analytica scandal provided a terrifying example of such data use, in which external app developers were allegedly granted access to several aspects of personal data of Facebook users (including their own political views through the analysis of "likes" or "angry faces" given to several publications within the social media platform), as well as their network of friends⁴⁹³ (data harvesting). These data were then allegedly used for big data analysis,⁴⁹⁴ profiling, and data crossing with strategic communication systems⁴⁹⁵ during electoral processes in several countries, including the United Kingdom (Brexit referendum)⁴⁹⁶ and the United States (Presidential elections).⁴⁹⁷ This particular case serves

⁴⁹² Sandra Wachter and Brent Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI Survey: Privacy, Data, and Business' (2019) 2019 Columbia Business Law Review 494.

⁴⁹³ Brian Tarran, 'What Can We Learn from the Facebook—Cambridge Analytica Scandal?' (2018) 15 Significance 4.

⁴⁹⁴ Maria Tzanou, *Health Data Privacy under the GDPR: Big Data Challenges and Regulatory Responses* (Taylor and Francis 2020) <<https://go.exlibris.link/8JD6V6Kj>>.

⁴⁹⁵ David Ingram, 'Factbox: Who Is Cambridge Analytica and What Did It Do?' (*Technology News*, 20 March 2018) <<https://www.reuters.com/article/facebook-cambridge-analytica-idINKBN1GW0A4>>.

⁴⁹⁶ Alex Hern, 'Cambridge Analytica Did Work for Leave. EU, Emails Confirm' *The Guardian* (30 July 2019).

⁴⁹⁷ Channel 4 News Investigations Team, 'Exposed: Undercover Secrets of Trump's Data Firm' (20 May 2018) <<https://www.channel4.com/news/exposed-undercover-secrets-of-donald-trump-data-firm-cambridge-analytica>>.

as a prime example of the complete failure of PbDD in that neither Facebook nor Cambridge Analytica implemented the necessary technical or organisational measures to effectively integrate data protection principles and safeguard the rights and freedoms of data subjects. This highlights the significance of GDPR, which requires the automatic activation of data protection mechanisms to prevent any unauthorised or unethical access or processing of personal data without the data subject's knowledge. One possible approach to this could be the deployment of a PET, such as incorporating a technical measure into the PbDD programme that necessitates the data subject's positive action whenever a data processing activity is flagged as potentially leading to data misuse or unethical use of data. The operationalisation of consent in this manner may require a more dynamic model, perhaps resembling the "Two Factor Authentication."⁴⁹⁸ In 2017, the European Commission presented proposals for the EU to develop civil law Regulations on the use of robots and artificial intelligence, including the following premises:

‘[H]ighlights the principle of transparency, namely that it should always be possible to supply the rationale behind any decision taken with the aid of AI that can have a substantive impact on one or more persons’ lives; considers that it must always be possible to reduce the AI system’s computations to a form comprehensible by humans; considers that advanced robots should be equipped with a ‘black box’ which records data on every transaction carried out by the machine, including the logic that contributed to its decisions; [...] and [P]oints out that the guiding ethical framework should be based on the principles of beneficence, non-maleficence, autonomy and justice, on the principles and values

⁴⁹⁸ Steve Watts, ‘Intelligent Combination – the Benefits of Tokenless Two-Factor Authentication’ (2014) 2014 Network Security 17.

enshrined in Article 2 of the Treaty on European Union and in the Charter of Fundamental Rights, such as human dignity, equality, justice and equity, non-discrimination, informed consent, private and family life and data protection, as well as on other underlying principles and values of the Union law, such as non-stigmatisation, transparency, autonomy, individual responsibility and social responsibility, and on existing ethical practices and codes.⁴⁹⁹

To ensure compliance with GDPR in AI projects, organisations should eschew the pursuit of legal loopholes and instead align their practices with the most stringent rules possible. Integrating the best possible data protection settings and technical measures, such as data pseudonymisation and anonymisation, directly into processing activities via PbDD can confer significant long-term advantages for AI data processing. In April 2021, the Superintendence of Industry and Commerce, with inputs and technical guidance from the Presidential Council for Economic Affairs and Digital Transformation of Colombia, developed a Sandbox⁵⁰⁰ aimed at fostering privacy by design and default in AI projects, whereby companies interested in developing artificial intelligence projects collaborate to develop compliance solutions. These compliance solutions could involve the implementation of tools such as collective DPIAs, privacy by design and default, and accountability mechanisms, among others.⁵⁰¹

⁴⁹⁹ *European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL))*, OJ C 252, 1872018, p 239–257.

⁵⁰⁰ Regulatory sandboxes are, inter alia, supervised environments designated for temporary experimentation purposes..

⁵⁰¹ Superintendence of Industry and Commerce, ‘Sandbox on Privacy by Design and by Default in Artificial Intelligence Projects’ (2021) <<https://globalprivacyassembly.org/wp-content/uploads/2021/07/B6.-SIC-Colombia-Sandbox-on-privacy-by-design-and-by-default-in-AI-projects.pdf>>.

Although the regulatory framework considered there was Statutory Law 1581 of 2012 and Decrees 4886 of 2011 and 1377 of 2013 (incorporated in Decree 1074 of 2015) rather than the GDPR, the results of this experimentation will undoubtedly be important for the application of PbDD in AI projects carried out in the EU. Organisations are incentivised to pursue the most efficient method of implementing the following measures, as outlined in the ‘Resolution on accountability in the development and use of artificial intelligence’⁵⁰² which was approved in October 2020 by the Global Privacy Assembly, in order to: i) assess the potential impact to human rights (including data protection and privacy rights) before the development and/or use of AI; ii) test the robustness, reliability, accuracy and data security of AI before putting it into use, including identifying and addressing bias in the systems and the data they use that may lead to unfair outcomes; and iii) implement accountability measures that are appropriate with respect to the risks of interference with human rights.

The potential threats of IoT interfering with human rights have been a topic of considerable debate in both political and academic circles. Of particular concern are facial recognition systems, which have undergone rapid evolution from rudimentary image recognition to near-instantaneous identification of individuals due to the proliferation of digital photos available through social media, websites, and surveillance cameras. Such systems are being deployed in public areas across the globe, and China's use of facial

⁵⁰² *ibid.* ‘In those documents it is suggested that privacy by design and by default is considered as a proactive measure to, among others, comply with the Principle of Accountability. By introducing the principle of privacy by design and by default, it seeks to guarantee the adequate processing of the data that is used in the projects that involve the collection, use or processing of personal data. So, an adequate processing of the information must be an essential component of the design and implementation of AI projects.’

recognition as a tool of authoritarian control has drawn widespread criticism and calls for a ban on the technology.

The challenge for EU lawmakers is to draft privacy and data protection legislation that shields individuals from any adverse effects of personal information utilisation in AI, while simultaneously avoiding undue constraints on AI development or entanglement of GDPR in even more complex legal complexities. Although the GDPR does not explicitly mention artificial intelligence, it does refer to "automated decision-making," implying the use of algorithms. The possibility that algorithms will produce a discriminatory effect⁵⁰³ in their decisions is a source of concern for individuals, organisations, and legislators alike. As a result, where algorithmic decisions are consequential, it makes sense to combine PbDD measures and PETs with human decision review, as this could help identify and remediate unfair outcomes.

Understanding the legal and technical feasibility of explainability of algorithmic decisions is thus critical in determining whether the GDPR's right to information is a practical right in the context of AI. Prior research has demonstrated that algorithmic decision-making, particularly the right to explanation, calls for a more extensive and lucid policy framework. It is imperative to clarify the type of explanation mandated by GDPR, whether it extends to decisions based on non-personal data, and whether such explanations can allow for flexibility depending on the employed model.⁵⁰⁴

⁵⁰³ Robin Allen and Dee Masters, 'Artificial Intelligence: The Right to Protection from Discrimination Caused by Algorithms, Machine Learning and Automated Decision-Making' (2019) 20 ERA-Forum 585.

⁵⁰⁴ Maja BRKAN and Grégory BONNET, 'Legal and Technical Feasibility of the GDPR's Quest for Explanation of Algorithmic Decisions: Of Black Boxes, White Boxes and Fata Morganas' (2020) 11 European Journal of Risk Regulation : EJRR 18.

Despite recent developments in PbDD-based approaches from the AI technology sector to achieve GDPR compliance,⁵⁰⁵ there remains considerable scope for improvement in implementing PbDD in the context of AI. This includes not only the implementation of appropriate measures to ensure the integration of data protection principles in processing but also the effective protection of individuals' rights and freedoms. Therefore, it is imperative to continue working towards full compliance in this critical area.

In my opinion, implementing a PbDD model is necessary to mitigate the risk of discrimination and surveillance of individuals. By embedding data protection principles into AI technologies, PbDD can help prevent discriminatory biases from being built into algorithms, protect individuals' privacy, and limit the monitoring of their activities.⁵⁰⁶ Additionally, it can provide greater transparency, accountability, and control over personal data, which is crucial for building trust between organisations and their customers. Overall, the adoption of PbDD in AI can help ensure that technological innovation is aligned with societal values, and the highest standards of data protection and privacy are upheld.

In conclusion, from my perspective, the intersection of blockchain, IoT, and AI represents a convergence of disruptive technologies that holds the potential to enhance existing business practices and generate innovative business models. One potential thread uniting these technologies is IoT's role in data collection and provision, blockchain's ability

⁵⁰⁵ See, e.g., 'GDPR & AI: Privacy by Design in Artificial Intelligence' (*Silo AI*, 28 February 2018) <<https://silo.ai/gdpr-ai-privacy-by-design-in-artificial-intelligence/>>.

⁵⁰⁶ For an examination of the methods by which contemporary organisations monitor individuals' activities, see, e.g., Theresa M. Payton and Theodore Claypoole, *Privacy in the Age of Big Data* (Rowman & Littlefield 2014). p.121. 'As cities, shops, and businesses install cameras everywhere, store the information they capture, and apply software to examining the video for interesting items, we are being watched. [...] Even your car is becoming an internet-connected computer that sends your information far afield. The tool booths are watching you, even when you are not paying tolls, and they are recording your movements. [...] Finally, your DNA, the core building block of your body, has become a valuable commodity for research and for law enforcement. As you move around the world, your privacy is betrayed by your workplace, your car, and even your body.'

to establish a robust infrastructure and define engagement parameters, and AI's capacity for process optimisation and rule formulation. The inherent complementarity of these technologies implies that their combined utilisation has the potential to unlock their full potential. While it is evident that these technologies have become ingrained in our socio-economic fabric, it remains to be seen when the European Union's governing bodies will formally address their implications with regards to data protection legislation.

5.4. Assessing the Preparedness of PbDD for Cloud Computing

Cloud computing, as defined by Edoardo Celeste and Federico Fabbrini, is a rapidly evolving, cross-border technology that is the result of developments in information and communications technology and globalisation. Several areas of tension exist between the GDPR and cloud computing, including but not limited to: (i) Responsibility for personal data, where the GDPR mandates that data controllers be responsible for protecting personal data, but the delineation of responsibilities between data controllers and data processors in cloud computing can be unclear, particularly in multi-party data processing scenarios; (ii) Data Security, where the GDPR requires appropriate TOMs to ensure the security of personal data. Nevertheless, cloud computing presents inherent security risks such as data breaches, hacking, and unauthorised access that can be difficult to manage and mitigate, even with the implementation of PbDD; (iii) Data location, where the GDPR necessitates that personal data is processed within the boundaries of the EU, but cloud computing makes it challenging to determine the physical location of data, particularly when data is replicated or mirrored across multiple servers worldwide; (iv) Data portability, where individuals are entitled under the GDPR to access their personal data in a commonly used

format and transfer it to another controller. However, cloud computing technology can create difficulties in transferring data between cloud providers or aggregating it in a format that other systems can utilise.

These challenges highlight the significance of implementing clear and effective PbDD measures in cloud computing, which can include enhanced security measures, defined responsibilities for data controllers and processors, and efficient data protection mechanisms for personal data processed and stored in the cloud.⁵⁰⁷ Policymakers have been endeavouring to establish solutions that facilitate legally compliant, secure, and privacy-conscious cloud computing while also enabling businesses to utilise data equitably to stay competitive.⁵⁰⁸

The increasing prevalence of cloud computing has resulted in new challenges, such as information security and privacy concerns,⁵⁰⁹ and a rise in high-profile cloud data breaches (some involving major cloud service providers). High-profile cloud data breaches have the potential to erode consumer trust, damage brand reputations, and result in significant financial losses due to regulatory fines and legal liabilities. These breaches often involve unauthorised access to personal data, theft of sensitive information, or the exposure of confidential business data. The increasing number of such incidents should

⁵⁰⁷ By integrating PbDD principles into the design and operation of cloud computing services, organisations can proactively address potential data protection risks and privacy issues. This includes considerations such as data minimisation, ensuring data confidentiality and integrity, and implementing access controls to prevent unauthorised access to personal data stored in the cloud. Additionally, PbDD measures in cloud computing environments can ensure compliance with legal obligations under the GDPR, such as providing data subjects with the ability to exercise their rights and demonstrating accountability.

⁵⁰⁸ Lynn and others (n 349).

⁵⁰⁹ Privacy concerns in cloud computing stem from the fact that organisations often have limited control over where their data is stored and processed, as well as who has access to it. This can make it difficult for organisations to ensure the privacy of their personal information. Additionally, varying data protection laws and regulations across jurisdictions may complicate compliance efforts for organisations operating in multiple countries.

prompt organisations to prioritise the security and privacy of their cloud environments. For instance, between 2018 and 2019, an estimated 196 security breaches occurred due to misconfigurations of cloud databases, putting 33 billion records at risk, and resulting in an estimated cost of US\$5 trillion for affected organisations.⁵¹⁰ Interestingly, figure 10 indicates that only approximately 63 percent of IT security professionals surveyed in France in 2019 believed that their organisation would undertake significant changes in cloud governance after implementing the GDPR.⁵¹¹

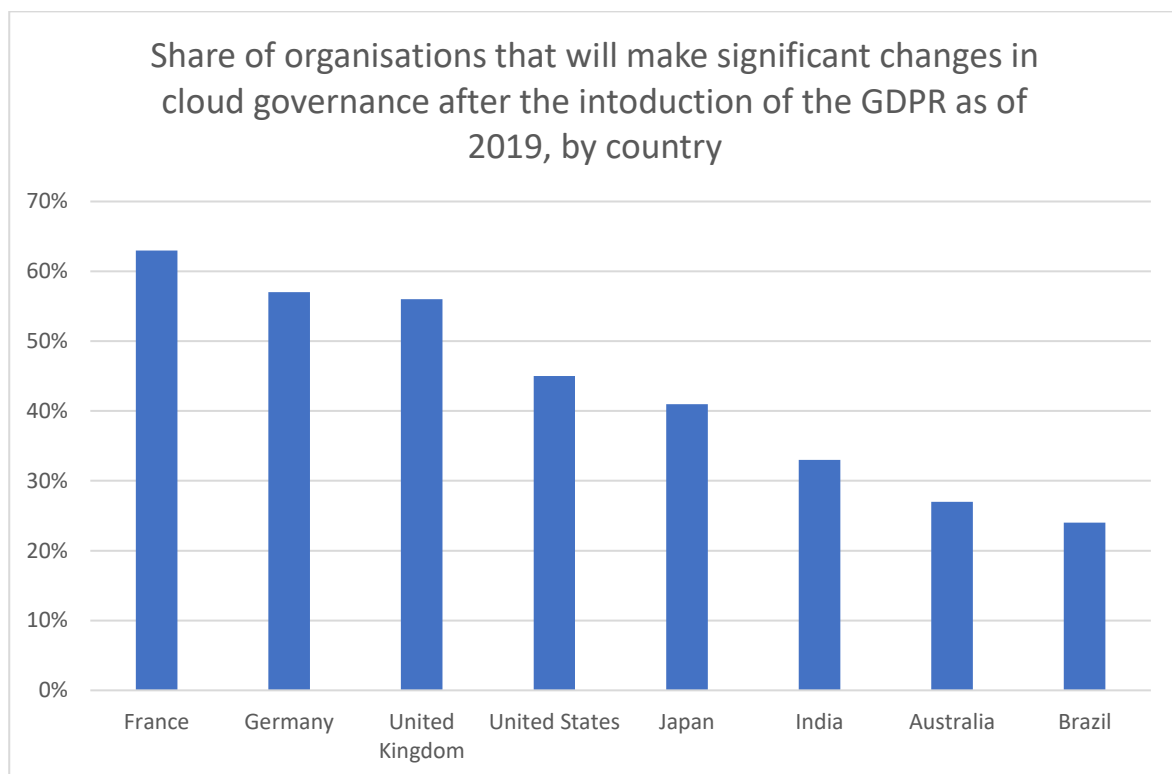


Figure 10 - Ponemon Institute, & Thales Group. (September 30, 2019). Share of organisations that will make significant changes in cloud governance after the introduction of the GDPR as of 2019, by country [adapted]. In Statista, 04 February 2022, <<https://www.statista.com/statistics/1063528/worldwide-cloud-governance-changes-due-to-gdpr/>>.

⁵¹⁰ DivvyCloud, '2020 Cloud Misconfigurations Report' (2020) <<https://divvycloud.com/misconfigurations-report-2020/>>. The denoted values are presented in USD, as published in the original document.

⁵¹¹ Importantly, GDPR's PbDD is now a global standard for data protection and security, making it one of the most important components of an efficient IS governance system.

In addition to the limitations imposed by the GDPR on the transfer of personal data to third countries, the implementation of PbDD is also proving to be challenging in the context of cloud computing technology. This is particularly relevant for organisations, especially in the financial sector, which employ a 'follow-the-sun'⁵¹² model, whereby personal data may be transferred to or accessed from multiple jurisdictions. With an increasing number of companies relying on platforms such as Amazon Web Services ('AWS'), Google Cloud and Microsoft Azure to deploy their IT infrastructures, and service providers offering software as a service ('SaaS') solutions relying on servers placed all over the world,⁵¹³ the legality of such processing has become a major concern, particularly during the Covid-19 pandemic,⁵¹⁴ which forced companies to adopt new work-from-home models based on cloud platforms and researchers turning to cloud services 'to store, monitor, predict and analyse the huge set of patient's data.'⁵¹⁵

The contradictions between the EU's data protection legislative approach and other jurisdictions are further complicated by the borderless nature of cloud computing technology. The EU has been promoting data localisation requirements that mandate

⁵¹² See, ERRAN CARMEL, J ALBERTO ESPINOSA and YAEL DUBINSKY, "Follow the Sun" Workflow in Global Software Development' (2010) 27 *Journal of Management Information Systems* 17. 'Follow the Sun (FTS) is a rather intuitive idea: hand off work at the end of every day from one site to the next many time zones away (e.g., United States to India) so that the work can be advanced while one's team rests for the night.'

⁵¹³ See, Lynn and others (n 349). 'From a technical perspective, this is possible thanks to the so-called "sharding". Data are not concentrated in a single virtual cloud, but are fragmented into a series of "shards", replicated, and stored in different locations. This procedure, which is entirely automated, allows the cloud computing service to maximise its performance. On the one hand, smaller pieces of information can be accessed more quickly. On the other hand, their replication enhances the security of the system by reducing the risks of node failures or data loss.'

⁵¹⁴ See Tzanou (n 486). 'The recent COVID-19 pandemic is not only an unprecedented global health emergency; it has also foregrounded a variety of data privacy issues. Billions of people are required to comply with social distancing rules and endure mass digital surveillance of their location, communications and movements.'

⁵¹⁵ R. Singh, 'Cloud Computing and Covid-19', *2021 3rd International Conference on Signal Processing and Communication (ICPSC)* (2021).

personal data to be stored on servers within the EU, to maintain digital sovereignty, protect fundamental rights, and prevent foreign law enforcement and intelligence agencies from accessing personal data. However, some foreign governments have enacted laws that compel national organisations to disclose data stored in Europe, bypassing the jurisdictional limits based on the physical location of data. This creates a complex regulatory environment, where organisations must navigate conflicting legal obligations and ensure compliance with both EU and foreign data protection Regulations, in addition to PbDD measures.⁵¹⁶

Some scholars and practitioners argue that the language and provisions of the GDPR lack clarity and certainty in relation to new and emerging technologies,⁵¹⁷ which makes it challenging for businesses to understand how to apply the PbDD requirement and address data protection in activities involving privacy-invading technologies⁵¹⁸ ('PITs') such as body scanners, public CCTV microphones and CCTV loudspeakers, and human-implantable microchips (RFID implants). These technological advancements can potentially circumvent privacy rights, thereby creating further uncertainty for businesses on how to integrate PbDD principles. It is important for data controllers and operators of PITs to work together to implement appropriate measures to ensure data protection and privacy. However, the GDPR does not directly regulate the design and development of new technologies, including PITs, as this falls under the purview of manufacturers. While data controllers can

⁵¹⁶ Lynn and others (n 349).

⁵¹⁷ See Purtova (n 76).

⁵¹⁸ See Klitou (n 461). 'Privacy-Invading Technologies (PITs) [...] are generally defined as 'any form or type of technology, whether hardware or software, which poses a particular threat to privacy and/or is capable of being used to substantially violate an individual's right to privacy and/or data protection rights.'

request that manufacturers develop more privacy-friendly technologies, this approach may not be sufficient.⁵¹⁹ To that end, Recital 78 GDPR simply states:

[W]hen developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications *should be encouraged* to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations.⁵²⁰

An ongoing challenge in legislation is keeping pace with the rapid evolution of technology, and the GDPR is no exception. As discussed in Chapter one, several studies have explored emerging technologies and found that while they enable innovation for organisations, they also pose a risk to individual privacy. To further expound on my prior statement, it is my contention that the GDPR does not adopt a "natural approach" towards emerging technologies, resulting in various compliance hurdles between the use of these technologies and PbDD implementation. Particularly, blockchain, IoT, and AI are identified as some of the most popular technologies in dissonance to PbDD principles. Blockchain technology poses significant challenges for the implementation of PbDD due to its unique nature. It is a distributed database that facilitates the sharing and storage of a complete transaction history in a series of blocks on a public ledger among computers connected to

⁵¹⁹ *ibid.*

⁵²⁰ GDPR, Recital 78. (emphasis added).

a network. The ever-expanding and immutable nature of the blockchain ledger raises concerns regarding the GDPR's storage limitation principle, which stipulates that personal data should be retained only as long as it is necessary for the purpose for which it was collected, and in a form that enables identification of data subjects. Additionally, critics argue that this perpetually growing and unchangeable ledger is at odds with the GDPR's data minimisation principle, which requires that personal data must be relevant, adequate, and limited to what is necessary for processing purposes.⁵²¹

In the context of IoT, businesses are benefiting from increased productivity, process automation, service personalization, and real-time focused data generation. However, significant challenges related to privacy and data security, particularly in the practical application of PbDD, have emerged as obstacles to the technology's development, which the GDPR currently fails to adequately address. The primary areas of tension between IoT and GDPR are generally identified as transparency, consent, privacy, discrimination, and complex contractual relationships.⁵²²

The use of artificial intelligence ('AI') presents several challenges to the implementation of PbDD. AI systems are autonomous, self-contained technology⁵²³ that can interpret external data, learn from such data, and use those learnings to achieve specific goals and tasks through flexible adaptation.⁵²⁴ However, the ever-evolving nature of AI creates technical difficulties for the implementation of PbDD, and the processing of

⁵²¹ Rania El-Gazzar and Karen Stendal, 'Examining How GDPR Challenges Emerging Technologies' (2020) 10 *Journal of information policy* (University Park, Pa.) 237.

⁵²² *ibid.*

⁵²³ Wesley Gomes de Sousa and others, 'How and Where Is Artificial Intelligence in the Public Sector Going? A Literature Review and Research Agenda' (2019) 36 *Government information quarterly* 101392.

⁵²⁴ Andreas Kaplan and Michael Haenlein, 'Siri, Siri, in My Hand: Who's the Fairest in the Land? On the Interpretations, Illustrations, and Implications of Artificial Intelligence' (2019) 62 *Business horizons* 15.

personal data using AI raises ethical and legal issues that have not yet been addressed by the GDPR. Specifically, the application of machine learning algorithms ('MLA') and big data analytics⁵²⁵ to the processing of personal data presents challenges in terms of transparency, consent, and discrimination, among others.

In my opinion, the GDPR is not equipped to address the challenges posed by emerging technologies. Therefore, policymakers need to engage in further discourse on the relationship between these technologies and the GDPR. These technologies present unique challenges to the safe and fair processing of personal data that require careful examination to develop a data protection framework that is future-proof. Policymakers should thoroughly evaluate the potential risks and benefits of these technologies while identifying strategies to address any associated ethical and legal issues.

5.5. Concluding remarks

So far, we have observed that AI, IoT, and blockchain technologies are intricately interconnected with and reliant upon cloud computing for their optimal functionality.

For AI, the vast datasets required for training and deploying complex machine learning models necessitate substantial computational power and storage capacity. Cloud computing serves as a fundamental infrastructure, providing the resources essential for AI systems to perform intricate computations, facilitating advanced decision-making, and supporting continuous learning capabilities.

⁵²⁵ See Tzanou (n 486). 'Big data, AI and machine learning are closely related concepts and sometimes are referred to interchangeably. However, there are differences between the two. As the UK Government Office for Science astutely puts it: "If data is the fuel, artificial intelligence is the engine of the digital revolution."'

Similarly, IoT heavily relies on cloud computing as a centralised hub for collecting, storing, and processing the copious amounts of data generated by interconnected devices. The flexibility and scalability inherent in cloud services are indispensable for handling the diverse and expanding data streams produced by IoT devices, enabling real-time analytics and insights. Additionally, cloud-based platforms play a pivotal role in managing and orchestrating the myriad interconnected elements of IoT systems.

Blockchain technology, with its decentralised and secure nature, benefits from the cloud's support in hosting blockchain networks and storing transaction data. Cloud infrastructure enhances the accessibility, scalability, and efficiency of blockchain applications, contributing to the broader adoption and effectiveness of this technology.

However, the interdependence of AI, IoT, and blockchain technologies with cloud computing introduces potential risks, including concerns related to data security, privacy vulnerabilities, and the dependence on centralised systems. These dangers encompass the potential for unauthorised access to sensitive information, the exposure of interconnected devices to security threats, and the reliance on centralised cloud services, which may become a single point of failure. As these technologies become increasingly integrated, addressing these risks becomes crucial for ensuring a secure and resilient technological ecosystem.

Transitioning to the practical applicability of PbDD within this evolving technological landscape, the emphasis on practical implementation becomes paramount. The DPPA, with its focus on embedding data protection measures into the design and operation of systems, aligns with the complex demands of these technologies. As we delve into the practical aspects of PbDD in the next chapter, its relevance and effectiveness in ensuring data protection within these innovative spheres will come to the forefront.

Chapter 6 – Shining a light on the PbDD’s applicability

Introductory notes

This section discusses aspects of GDPR applicability, and it also addresses the PbDD requirements in Article 25 GDPR, which have grown increasingly complex and difficult to implement in practice. Several studies and reviews indicate that many technical procedures connected to electronic personal data processing are not always compatible with PbDD, namely, PbDD tends to be incompatible with technological advances such as Blockchain, the IoT, and AI. In terms of applicability, PbDD is relevant to any technology system or product that collects, stores or otherwise processes personal data. This includes platforms such as websites, mobile applications, IoT devices and cloud services, among others. Theoretically, PbDD can be applied to any technology or product, regardless of its scale or complexity, and can be adapted to the specific needs and requirements of each project. In practice, as we will see, it appears this is not always the case. Furthermore, in terms of technology compatibility, theoretically, PbDD is a flexible framework that can be applied to any technology or programming language. It is not tied to any particular technology stack or platform and can be customised to fit the needs of a specific project. This makes PbDD a “technology-agnostic” approach to data protection that can be applied to a wide range of technology systems and products. In this regard, Axel Voss,⁵²⁶ one of the founding

⁵²⁶ Axel Voss is a German politician and Member of the European Parliament who played a significant role in the creation of the GDPR. In his role as a rapporteur for the European Parliament, Voss led the negotiations on the GDPR, which culminated in the adoption of the regulation by the European Parliament in April 2016. During the negotiations, Voss played a critical role in shaping the final text of the GDPR, which replaced the outdated EU Data Protection Directive. Voss was a strong advocate for enhanced privacy protections for EU citizens, and he pushed for provisions that gave individuals greater control over their personal data, such as the right to be forgotten and the right to data portability. Voss also played a key role in securing the GDPR's extraterritorial reach, which applies to any organisation that processes the personal data of EU citizens,

fathers of the GDPR, considers the Regulation to be outdated and in need of an update.⁵²⁷

According to Voss, the GDPR requires 'some type of surgery' to incorporate emerging technologies such as AI, Blockchain, and Facial recognition. As a member of the European Parliament, he is sceptical that the GDPR will be able to address many of the issues raised by these rapidly evolving technologies, implying that a shift to more technologically informed Regulation is required; a statement with which I agree completely.

In this chapter, I will therefore focus on the GDPR's material scope,⁵²⁸ considering primarily the interaction between PbDD and new technologies. Due to its predominantly technical nature, this chapter may appear to be more technologically oriented; however, I will attempt to provide a sufficient connection between the issues raised on the technological sphere and the legal discussion surrounding them, thus bridging the technical considerations with the GDPR and PbDD, while examining the latter's incorporation into organisations' systems and processing activities.

6.1. The PbDD role in legacy data clean-up for GDPR compliance

In considering whether PbDD should be involved in aspects of legacy data management, one may question whether this is a technical issue that is best addressed by engineers, and

regardless of where the organisation is located. This provision has had a significant impact on global data protection practices and has forced many organisations to overhaul their data processing procedures to comply with the regulation. Overall, Voss's contributions to the creation of the GDPR have had a profound impact on the way that organisations around the world approach data protection and privacy, and his work continues to influence data protection policy and practice.

⁵²⁷ Javier Espinoza, 'EU Must Overhaul Flagship Data Protection Laws, Says a "Father" of Policy' (*Data Protection*, 3 March 2021) <<https://www.ft.com/content/b0b44dbe-1e40-4624-bdb1-e87bc8016106>>.

⁵²⁸ The material scope of the GDPR is outlined in Article 2 GDPR. The Regulation applies to 'processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.' This definition encompasses both automated ("big data" and similar) and human-assisted processing.

whether it falls outside the scope of legal discussion. However, it is important to note that good data cleansing practices and proactive data retention management have become critical under the GDPR. Specifically, organisations must now develop PbDD procedures to enable them to continually review, re-assess, and, where appropriate, delete any data deemed unnecessary to assist with overall compliance efforts. Therefore, it can be argued that PbDD has a crucial role to play in legacy data management, as it ensures that personal data is handled in a way that is consistent with GDPR requirements, and that unnecessary data is disposed of in a timely and appropriate manner.

The GDPR requires organisations to keep personal data for no longer than necessary and to maintain a high level of data quality to help protect personal data and thereby the privacy of individuals. This means that when processing legacy data, the key question is whether the law requires a controller to apply GDPR standards to those legacy data sets; does the notion of processing – the activity that the GDPR seeks to regulate – include legacy data carried over from the DPD?⁵²⁹ Yes, I would say. The GDPR allows for a clear construction in this regard; the definition of processing in Article 4(2) includes storage of personal data, so where a controller stores historical personal data, that action constitutes ongoing processing and the GDPR applies to those records.

Because GDPR emphasises the incorporation of all data protection principles, individual rights, and measures for ensuring data protection and compliance with the Regulation via PbDD, controllers need to create costly operational frameworks to deliver on Article 25 GDPR requirements. In addition, most organisations also need to update their security and communication frameworks (applied in ICT and processing activities,

⁵²⁹ Directive 95/46/EC.

especially in marketing) to close the legal loophole for their legacy data processing. Although many of those data sets were lawfully and fairly collected and processed under the Data Protection Directive,⁵³⁰ the GDPR makes its further processing unfair under the new data subject's "consent for processing" requirements.

Some large organisations store millions of registers of personal data, and the operational consequences of uplifting and review those millions of registers can be daunting. Attempts to identify this personal data sets using predominantly manual processes typically fail for the following reasons: a) the results would be extremely inconsistent and thus unreliable; b) there is no way the process could be completed in any reasonable timescale for GDPR compliance – completion estimates are sometimes in decades, not years, months, or weeks; and c) it would be too disruptive to the business – a significant number of employees would be required to spend a significant portion of their working day on data identification and classification tasks.

Consequently, it is my contention that the implementation of a legacy data strategy within the PbDD programme can yield significant advantages for organisations. By preserving and leveraging existing data assets, companies can gain a better understanding of their operations and utilise historical information to inform their decision-making processes.⁵³¹ Additionally, by incorporating legacy data into the PbDD programme, organisations can avoid duplication of efforts and reduce costs associated with acquiring new data. Furthermore, a well-defined legacy data strategy can also enhance the overall efficiency of the PbDD programme by streamlining data management processes and

⁵³⁰ *ibid.*

⁵³¹ Existing data assets offer valuable insights into past trends, patterns, and customer behaviours, which can be used to refine business strategies, improve efficiency, and optimise resource allocation.

reducing the likelihood of data errors or inconsistencies. By taking a proactive approach to managing legacy data, organisations can ensure that their PbDD programme is operating at its full potential, delivering valuable insights and driving strategic business decisions. Therefore, I posit that the incorporation of a legacy data strategy is an essential element of any effective PbDD programme.

Figure 11 illustrates the results of a 2017 survey of IT decision makers in the UK, regarding the benefits of the GDPR for organisations. During the survey, 41 percent of respondents agreed that mandatory data removal and deletion would help organisations keep the amount of data held under control, while 14 percent of IT decision makers believed that the GDPR would give organisations a competitive advantage.

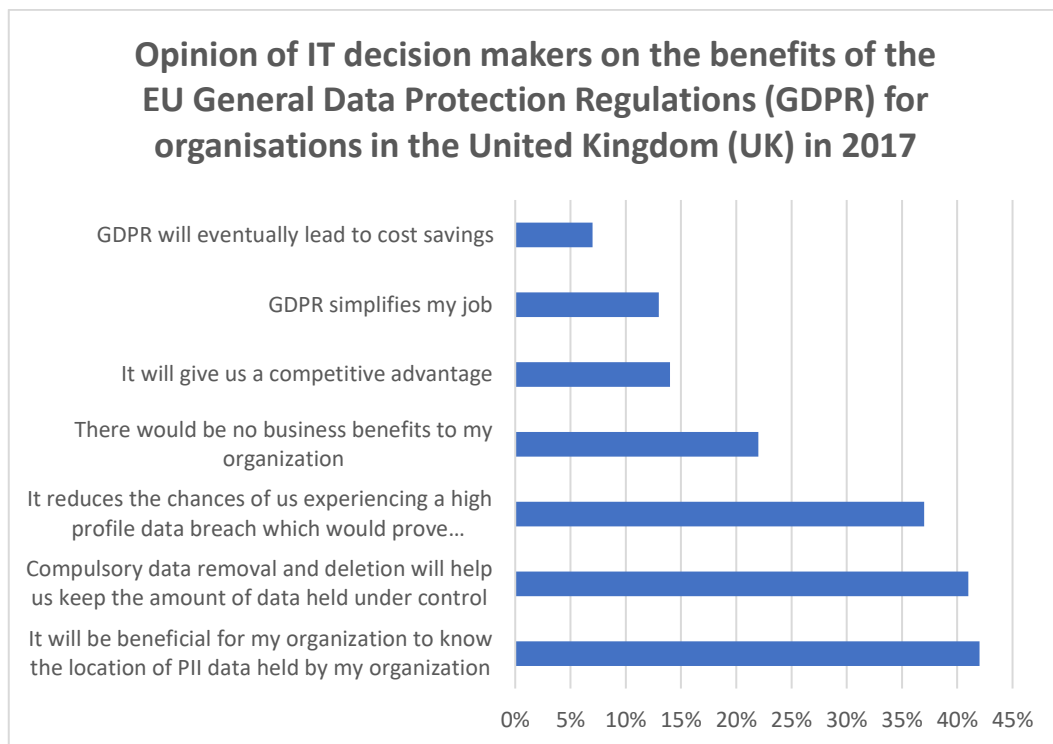


Figure 11 - Varonis. (May 18, 2017). Opinion of IT decision makers on the benefits of the EU General Data Protection Regulations (GDPR) for organisations in the United Kingdom (UK) in 2017 [adapted]. In Statista. <<https://www.statista.com/statistics/796130/gdpr-on-benefits-for-organisations-in-the-uk/>>.

Additionally, Figure 12 shows the results of a 2017 survey of how IT decision makers felt GDPR would benefit UK citizens. During the survey, 24 percent of respondents said they believe less personal information would be collected by organisations, while 61 percent of respondents believed their personal information would be better protected.

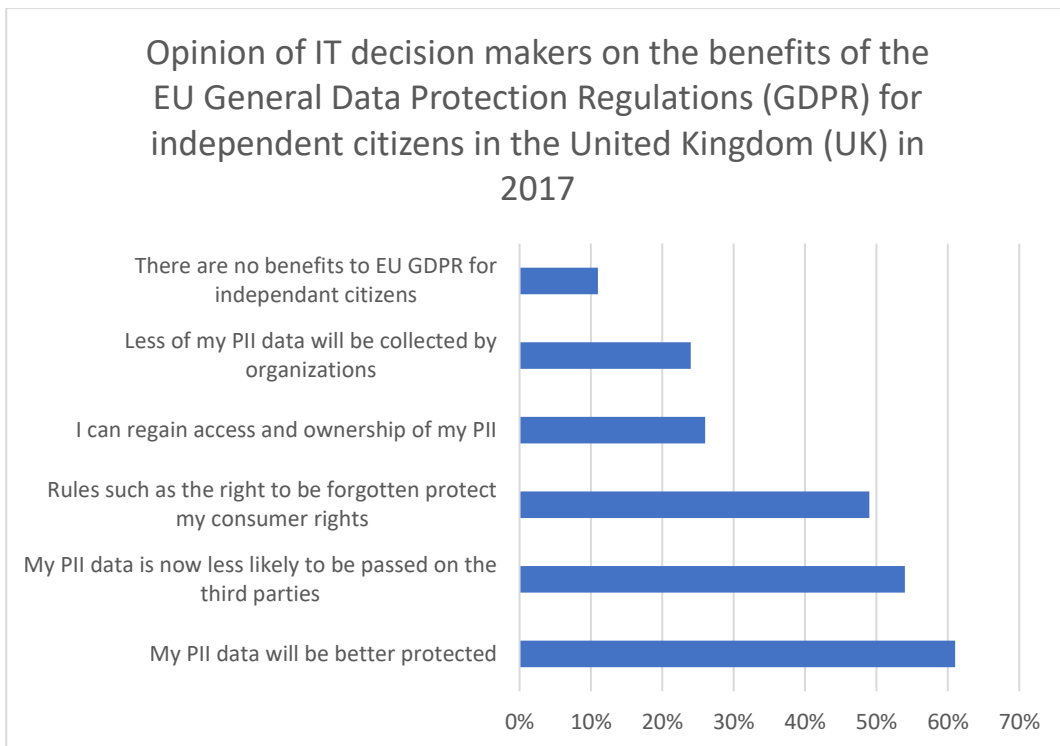


Figure 12 - Varonis. (May 18, 2017). Opinion of IT decision makers on the benefits of the EU General Data Protection Regulations (GDPR) for independent citizens in the United Kingdom (UK) in 2017 [adapted]. In Statista. <<https://www.statista.com/statistics/796041/gdpr-opinion-on-benefits-for-citizens-in-the-uk/>>.

Both statistics show that the GDPR is viewed by organisations as well as individuals as a positive change in terms of legal retention of personal data and would result in a new approach to personal data management, therefore boosting individual's trust on the way their data is protected. To achieve this objective, organisations must consider not only the cost of the program, but also a number of operational factors; in this context, PbDD plays a vital role, as we will see below.

To ensure an effective personal data retention programme⁵³² it is essential to employ a retention schedule that is supported by a comprehensive set of business policies, processes, and procedures embedded in a framework-style PbDD model. By doing so, organisations can significantly reduce the likelihood of data breaches resulting from accidental data damage, cyber-fraud, and cyber-attacks, while also mitigating the risk of personal data over-retention. These risks are among the most prevalent when storing personal data and have the potential to adversely impact the rights and freedoms of data subjects, and consequently, the operations of organisations. In the event of a reportable data breach,⁵³³ data controllers must be able to deal with breach notifications within a very short (72 hours) time frame. Consideration of post-incident actions ensures timely access to accurate and up-to-date contact information of relevant data subjects, as required by GDPR: '[T]he controller should communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person [...].'⁵³⁴

In the following paragraphs, I provide an operational approach to PbDD implementation (in line with the DPPA approach expounded in Chapters seven and eight), that organisations can rely on to address compliance in this area. To commence, the data controller must determine the essential information required to fulfil their intended purpose, by approaching the task at hand with the mindset that 'should hold that much

⁵³² Data retention policies should be developed as part of the data retention program. A data retention policy is a set of guidelines that help organisations keep track of how long information must be kept and how to dispose of it when it is no longer required. The policy should also specify why personal data is being processed. This action also ensures that organisations have documented evidence to support their data retention and disposal periods.

⁵³³ In accordance with Article 33 GDPR.

⁵³⁴ GDPR, Recital 86.

information, but no more.⁵³⁵ In relation to existing data silos made of legacy, free-form text, and unstructured data, a discovery exercise must be carried out across the organisation's repositories – including cloud storage and mobile devices – to identify any personal data previously collected by the organisation that has not yet been verified and validated as "good data." Following the review and validation of these data, a data mapping containing any sensitive data discovered, as well as the anticipated time limits for erasure of the various categories of data must be created. It is critical to link the organisation's PbDD plan to the existing record of processing activities as required by Article 30 GDPR, which must include a list of all TOMs put in place to protect personal data,⁵³⁶ time limits for deletion of various aspects of data,⁵³⁷ related data flows, identified internal dependencies, and external data sharing.

When collecting personal data for the first time, the process must adhere to the purpose specification principle (the principle that a data subject must be informed as to why their personal data is being collected and the specific purposes for which it will be processed and stored), which means that personal data must be collected only for 'specified, explicit, and legitimate' purposes.⁵³⁸ The purpose for processing⁵³⁹ informs and justifies the processing operations in the sense that it determines, for example, which

⁵³⁵ ICO, 'Principle (c): Data Minimisation' (*Guide to the General Data Protection Regulation (GDPR)*) <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/>>.

⁵³⁶ GDPR, Article 30(1)(g).

⁵³⁷ *ibid.*, Article 30(1)(f).

⁵³⁸ *ibid.*, Article 5(1)(b).

⁵³⁹ Article 5(1)(b) of the GDPR sets forth the fundamental notion that personal data must be collected for a specific, explicit and legitimate purpose and cannot be further processed in a way which is incompatible with such original purposes. Purpose limitation is one of the cornerstones of the EU's data protection regime. It was also featured in the Directive 95/46/EC. More importantly, this concept is clearly noted in Article 8(2) CFR.

aspects of data will be collected and the retention periods that will be used (storage limitation requirements).⁵⁴⁰ As a result, 'purpose limitation protects data subjects by limiting how data controllers can use their data while also allowing data controllers some degree of flexibility.'⁵⁴¹

Along with the concept of 'quality' of personal data, storage limitation has long been a well-established principle in data protection and privacy law, and it can be found, for example in Article 5 of the Data Protection Directive,⁵⁴² and in Article 5(4)(e) of the Modernised Convention 108,⁵⁴³ with both sources determining that data must be erased (or anonymised) once their purpose has been served. Because personal data must be stored for the shortest amount of time possible, organisations must consider the reasons for the processing, as well as any obligations regarding a time frame for said processing as well as its accuracy, completeness and up-to-datedness which are all important elements of the data quality concept.⁵⁴⁴ Moreover, data retention must be proportionate to the purpose of collection⁵⁴⁵ as well as to limitation in time.⁵⁴⁶ The ECtHR decision in *S. and Marper*,⁵⁴⁷ provides a strong indication of the importance of implementation of PbDD

⁵⁴⁰ WP 29 (n 298).

⁵⁴¹ *ibid.*

⁵⁴² Directive 95/46/EC.

⁵⁴³ Convention 108.

⁵⁴⁴ Balancing accuracy with storage limitation: See *Rijkeboer [2009]* (n 93). A Dutch citizen petitioned information to the local administration about the persons to which his personal data had been disclosed during the past two years. The administration acceded to the petition, but limited the timeframe to one year, since personal information older than one year was automatically deleted. - The CJEU declared that ('the right to privacy means that the data subject may be certain that his personal data are processed in a correct and lawful manner, that is to say, in particular that the basic data regarding him are accurate and that they are disclosed to authorised recipients'); See also, *S and Marper v the United Kingdom (2008) ECHR 1581* (n 30). Where the indefinite retention of genetic and biometric data (fingerprints, cell samples, DNA profiles) of individuals after the criminal proceedings had been terminated was considered illegal.

⁵⁴⁵ GDPR, Article 5(b).

⁵⁴⁶ *ibid.*, Article 5(e).

⁵⁴⁷ *S and Marper v the United Kingdom (2008) ECHR 1581* (n 30).

mechanisms to ensure adequate data retention and destruction throughout the personal data lifecycle, by emphasising that organisations cannot retain personal data indefinitely, and by determining that infinite retention of some aspects of personal data, in this case bio-details (fingerprints, cell samples, and DNA), was ‘disproportionate and unnecessary in a democratic society’ if no criminal proceedings against the applicants were pending.

The GDPR requires that data be kept for ‘no longer than is necessary’⁵⁴⁸ but it does not specify any time limits or a specific data retention timescale, instead, it places the onus on organisations to implement PbDD and to include appropriate measures to determine how long they must keep personal data for business, contractual, or statutory purposes.⁵⁴⁹ Nonetheless, the GDPR provides some important decision-making aids and indicators, for example, by stating that data controllers should ‘ensuring the period for which the personal data are stored is limited to a strict minimum’⁵⁵⁰ in its binding Recitals. This means that data controllers must be accountable for determining precisely when personal data is no longer required⁵⁵¹ and, as a result, when it must be securely disposed of (or anonymised), implying that organisations must now move more towards a ‘Let’s think about the responsibilities of the business’⁵⁵² attitude, and precisely determine the key life-cycle stages of personal data stored in their systems.

⁵⁴⁸ GDPR, Article 5(1)(e).

⁵⁴⁹ GDPR, Recital 39.

⁵⁵⁰ *ibid.*

⁵⁵¹ Despite the apparent strictness of the GDPR’s data retention periods, no direct rules on storage limitation exist. Instead, organisations can set their own deadlines based on whatever criteria they deem appropriate. The only stipulation is that the organisation document and justify why it has set the timeframe that it has. The decision should be based on two key factors: the purpose of the data processing and any regulatory or legal requirements for data retention.

⁵⁵² Steve Mansfield-Devine, ‘Meeting the Needs of GDPR with Encryption’ (2017) 2017 Computer Fraud & Security 16.

It is important to underline that the GDPR allows for personal data be stored for longer periods of time for archiving purposes in the public interest or for scientific or historical research purposes,⁵⁵³ provided that appropriate measures (including data-review), such as pseudonymisation or anonymisation, are in place.⁵⁵⁴

In principle, the processing of each data element that, alone or in conjunction with others, constitutes personal data is inherently dependent on the specific “business needs.” As such, any business requirements that can be reasonably constructed in relation to the various environmental, regulatory, or legal scenarios in which the business operates, including statutory limitation periods related to tax law, employment law, commercial law, anti-money laundering law, or even the business's legitimate interests, must be assessed on a case-by-case basis.⁵⁵⁵ These assessments must be incorporated into both the data retention programme and the record of processing activities (ROPA) to ensure appropriate implementation of PbDD.

⁵⁵³ However, there appears to be an incongruence between Article 9(2)(j) and Article 89. Specifically, Article 9 (2)(j) provides for a legal basis for processing of special categories of data when necessary for archiving in the public interest and scientific or historical research or statistical purposes, pursuant to Article 89(1) and based on the laws of the Member States. Article 89(1), however, provides for the conditions of processing data for these purposes without requiring that the processing occurs in accordance with a member state's laws. In fact, Article 89(2) and (3) specifies which rights of individuals may be derogated from by Member states subject to the safeguards outlined in Article 89(1).

⁵⁵⁴ GDPR, Article 89.

⁵⁵⁵ The legislator's intention is to impose a duty on data controllers to develop their own mechanisms, such as retention policies, procedures, and time schedules, in accordance with their specific business needs, to reduce the risk of personal data becoming inaccurate, out of date, or irrelevant.

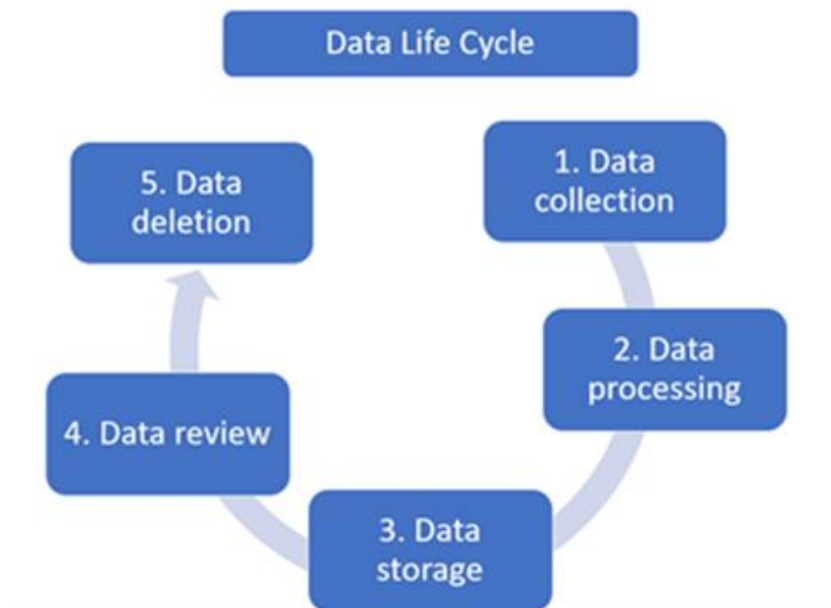


Figure 13 - Example of a business data retention and deletion circular procedure

Below is a practical illustration of an entry in the personal data retention schedule:

Id	Description	Retention Period	Start of Retention Period	Reason - Legal provision	Action at the end of retention period (review, delete, anonymise)
1	Employee Working time opt out forms	2 Years	From the date the opt-out has been rescinded or has ceased to apply	The Working Time Regulations 1998 (SI 1998/1833)	Secure deletion

Table 2 - Example of a data retention schedule entry

The retention period of personal data depends on the nature of the data processed and the type of record. Therefore, it is imperative for data controllers to have a record retention policy that is supported by a realistic data retention time schedule. This will provide objective criteria for determining when a specific aspect of data should be deleted or anonymised, thus helping to mitigate the risks associated with over-processing personal data.⁵⁵⁶ It is important to highlight the CJEU's criticism of the DRD's lack of objective criteria,⁵⁵⁷ as reasoned in the *Digital Rights Ireland* case,⁵⁵⁸ where the Court supported its views on the premise that a precise period for data retention must be constructed and applied, in order to ensure such a period is 'limited to what is strictly necessary.'⁵⁵⁹

Thus, information must only be kept 'as long as it is needed for business, legal or historical purposes, and a retention policy must be devised and applied to all information held.'⁵⁶⁰ In order to facilitate compliance with the GDPR's storage limitation principle, it is important for regulators to provide guidance to businesses on creating retention schedules, disposal processes for obsolete information, decision-making on trigger points, and incorporating disposal into digital systems where possible. However, data controllers have noted that this requirement can be particularly challenging to meet due to technical constraints associated with updating and upgrading legacy data silos, especially in cases where the originally obtained permission for processing is no longer in compliance with the

⁵⁵⁶ In accordance with Article 30(1)(f) GDPR, which reads as follows: '[W]here possible, (*the records of processing activities shall contain*) the envisaged time limits for erasure of the different categories of data'. (emphasis added).

⁵⁵⁷ Directive 2006/24/EC.

⁵⁵⁸ *Digital Rights Ireland* [2014] (n 98).

⁵⁵⁹ *ibid.*

⁵⁶⁰ The National Archives, 'Advice on Retention' (*Information Management*) <<https://www.nationalarchives.gov.uk/information-management/manage-information/policy-process/disposal/advice-on-retention/>>.

more stringent GDPR consent standards. Some of the underlying causes of this problem are clearly identified by Chris Taylor,⁵⁶¹ marketing executive for TIBCO. These include, but are not limited to, a lack of tools to manage unstructured data, difficulties in linking and integrating unstructured data with existing information systems, and a skills shortage to conduct the required technical operations.

Some of the key factors that data controllers must take into account when devising compliance mechanisms for their privacy programs are as follows: (a) old data will, by definition, become obsolete;⁵⁶² (b) personal data cannot be held forever 'just in case' it is needed at a later stage⁵⁶³ – a lawful basis for retention is always required; (c) responses to SARs and requests for erasure for any personal data organisations must be upheld⁵⁶⁴ (it may be a much more difficult task if the organisation holds significant legacy or widespread unstructured data); (d) Anonymisation should be considered if data is only required for research, business insights, or broader business analysis,⁵⁶⁵ as 'the principles of data protection should therefore not apply to anonymous information, [...] personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.'⁵⁶⁶

A PbDD plan plays a crucial role in facilitating the tasks of regular review and deletion of all "non-essential" categories of personal data⁵⁶⁷ and enabling data subjects to

⁵⁶¹ Chris Taylor, 'What's the Big Deal With Unstructured Data?' (*Partner content: Tibco*) <<https://www.wired.com/insights/2013/09/whats-the-big-deal-with-unstructured-data/>>.

⁵⁶² ICO, 'Principle (e): Storage Limitation' (n 321).

⁵⁶³ *ibid.*

⁵⁶⁴ *ibid.*

⁵⁶⁵ *ibid.*

⁵⁶⁶ GDPR, Recital 26.

⁵⁶⁷ *ibid.*, Recital 39.

exercise their rights. By providing added value in terms of overcoming any difficulties related to the operationalisation of legal requirements, PbDD plans are instrumental in ensuring compliance with the accountability principle.⁵⁶⁸ This principle is upheld by demonstrating the application of appropriate TOMs⁵⁶⁹ and promoting a proactive attitude towards data retention management during the period personal data is stored or processed.

Moreover, the implementation of a comprehensive PbDD plan, coupled with sufficient operational resources, can ensure that all personal data sets in the business are adequate, relevant, and limited to what is necessary,⁵⁷⁰ accurate and up to date,⁵⁷¹ and secure at all times.⁵⁷²

Furthermore, when feasible, organisations may consider integrating industry standards related to personal data processing and data protection, such as ISO/IEC 27001:2013, ISO/IEC 27701:2019, and ISO15489-1:2016, into their management activities. Aligning PbDD with these standards, and with the organisation's Information Security Management System⁵⁷³ (ISMS), can ensure that all security and data quality requirements mandated by the GDPR are not only met, but potentially surpassed.⁵⁷⁴

⁵⁶⁸ *ibid.*, Article 5(2).

⁵⁶⁹ *ibid.*, Article 32(1).

⁵⁷⁰ *ibid.*, Article 5(c).

⁵⁷¹ *ibid.*, Article 5(d).

⁵⁷² *Ibid.*, Article 5(f).

⁵⁷³ An Information Security Management System (ISMS) describe and demonstrate an organisation's approach to information security and privacy. It assists in identifying and addressing threats and opportunities associated with valuable information and any related assets. This safeguards organisations against security breaches and protects them from disruption if and when they occur.

⁵⁷⁴ Adopting a holistic approach to data management provides operational benefits to organisations by allowing them to gain comprehensive business intelligence on the personal data they process. This approach enables organisations to justify the necessity of retaining data, comply with standard retention periods, and schedule regular data reviews to trigger appropriate erasure or anonymisation mechanisms.

6.2. Storage limitation: data quality and security are a PbDD concern

The GDPR does not introduce a new requirement for 'data quality.' Article 6 of the EU Data Protection Directive already stated that any personal data retained should be 'accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified'.⁵⁷⁵ The Court of Justice of the European Union has also emphasised the importance of adhering to the 'data quality' principles outlined in Article 6 of the Directive. Namely, in its *Google Spain* decision, the CJEU refers to the danger of data to become 'incompatible with the Directive where those data are no longer necessary in the light of the purposes for which they were collected or processed.'⁵⁷⁶ To some extent, the contemporary data protection law approach to this 'data quality' requirement is informed by the principle 5 of the OECD recommendation 1980, which states:

'Personal data must be [...] -accurate and, where necessary, kept up to date [...] evaluated taking into account their degree of accuracy, their source, the categories of data subjects, the purposes for which they are processed and the phase in which they are used.'⁵⁷⁷

⁵⁷⁵ Directive 95/46/EC.

⁵⁷⁶ *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González* (2014) (n 69).

⁵⁷⁷ Organisation for Economic and Co-operation and Development, 'OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data - OECD' (1980) OECD Council Recommendation <<https://www.oecd.org/sti/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm>>.

In accordance with the GDPR, the concept of data quality is no longer viewed as a mere set of non-binding principles or declarations. Failure to adhere to data quality standards is considered a violation of the Regulation and can result in severe penalties for organisations. supervisory authorities have been granted specific powers to ensure that organisations comply with the Regulation and effectively protect individuals' rights and freedoms in regard to the processing of personal data. These powers include, but are not limited to, issuing fines of up to 4% of the organisation's annual global turnover or €20 million, whichever is greater, to controllers and processors who fail to implement PbDD and violate GDPR requirements.⁵⁷⁸

For example, the French regulator (CNIL) imposed a €400,000 monetary penalty⁵⁷⁹ on a real estate service provider for non-compliance with GDPR, namely, for failing to (a) implement appropriate security measures,⁵⁸⁰ and (b) failing to define and apply adequate data retention periods⁵⁸¹ to personal data processed, by keeping 'in an active database the personal data of applicants who did not access the rental for a period exceeding in significant proportions the period necessary to achieve the purpose of the processing, namely the allocation of housing, without any intermediate archiving solution in place',⁵⁸² that is, to not have in place a process or procedure for ensuring data quality.⁵⁸³

⁵⁷⁸ In accordance with Article 83 GDPR.

⁵⁷⁹ Annex 1 offers a visualisation of statistics on GDPR fines.

⁵⁸⁰ In accordance with Article 32 GDPR.

⁵⁸¹ In accordance with Article 5(1)(e) GDPR.

⁵⁸² 'Délibération SAN-2019-005 Du 28 Mai 2019' (Commission Nationale de l'Informatique et des Libertés 2018) 2019-005 <<https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000038552658/>>.

⁵⁸³ The consequences of such deficiencies in data quality can be severe for the organisation, data subjects, and data controllers alike, including loss of trust, reputational damage, and financial penalties for non-compliance with data protection regulations. Consequently, it is essential to recognise the complementary nature of data quality and security in effective PbDD operations.

Furthermore, on October 30, 2019, the Berlin Commissioner for Data Protection and Freedom of Information (Berliner Beauftragte für Datenschutz und Informationsfreiheit) imposed a €14.5 million fine on a German real estate company, Deutsche Wohnen, for keeping personal data for an indefinite period of time⁵⁸⁴ (a violation of the storage limitation principle). Deutsche Wohnen did not establish a GDPR-compliant data retention and deletion procedure for personal data of tenants:

‘[T]he Berlin SA considered retaining data substantially longer than necessary a breach of the GDPR, in three respects: first, the controller did not have a legal ground to store personal data longer than was necessary; second, this was considered an infringement of the data protection by design requirements under Article 25 (1) GDPR; and, finally, it was an infringement of the general processing principles set out in Article 5 GDPR.’⁵⁸⁵

The intersection between security and data quality arises from the fact that data quality is predicated on the confidentiality, integrity, and availability of personal data. If the processing of personal data is not undertaken in a secure manner, it is susceptible to unauthorised access, alteration, or destruction, which can result in data inaccuracies, incompleteness, or errors.

The GDPR adopts a risk-based approach to data processing security,⁵⁸⁶ as articulated in Article 32 of the Regulation. This provision sets out several measures that organisations must implement to minimise the risks arising from data processing activities

⁵⁸⁴ Ritzer and Filkina (n 336).

⁵⁸⁵ *ibid.*

⁵⁸⁶ GDPR, Recital 75.

that may impact the rights and freedoms of data subjects. These measures include pseudonymisation and encryption of personal data,⁵⁸⁷ the implementation of restoration mechanisms to ensure the availability and access to personal data in the event of an incident,⁵⁸⁸ and the deployment of mechanisms for testing, assessing, and evaluating the effectiveness of measures aimed at ensuring processing security.⁵⁸⁹ Ensuring the integrity and confidentiality of data is mainly accomplished through the incorporation of PbDD into businesses' systems and data processing activities.⁵⁹⁰

Regrettably, the GDPR provides limited guidance on how organisations should ensure the security of processing and is silent on information rights management. Article 32 of the GDPR stipulates that measures must be implemented to 'ensure a level of security appropriate to the risk.'⁵⁹¹ However, it offers no specific guidance on which measures to use, beyond pseudonymisation and encryption, or how to assess risk. As these are the only balancing and testing conditions provided by Article 25 GDPR for organisations to rely on during their implementation efforts, 'taking into account... as well as the risks of varying

⁵⁸⁷ *ibid.*, Article 32(1)(a).

⁵⁸⁸ *ibid.*, Article 32(1)(c).

⁵⁸⁹ *ibid.*, Article 32(1)(d).

⁵⁹⁰ Article 32 of the GDPR mandates that organisations must implement specific TOMs to ensure the security of personal data with an adequate level of protection. These measures include: (i) ensuring the pseudonymisation and encryption of personal data; (ii) guaranteeing the confidentiality, integrity, availability, and resilience of processing systems and services on an ongoing basis; (iii) establishing a process to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and, (iv) implementing a process for regularly testing, assessing, and evaluating the effectiveness of TOMs for ensuring the security of the processing.

⁵⁹¹ GDPR, Article 32(1)(a).

likelihood and severity for the rights and freedoms of natural persons posed by the processing,⁵⁹² this issue becomes systemic to PbDD.⁵⁹³

Many organisations have attempted to address this problem by implementing a compliance methodology based on a simple risk matrix,⁵⁹⁴ such as the one shown below:

Severity of impact	Serious harm	Low risk	High risk	High risk
	Some impact	Low risk	Medium risk	high risk
	Minimal impact	Low risk	Low risk	Low risk
		Remote	Reasonable possibility	More likely than not
		Likelihood of harm		

Table 3 - Example of a data protection risk matrix

⁵⁹² GDPR, Article 25(1).

⁵⁹³ In practical terms, the data controller is responsible for ensuring the security of personal data by deploying specific PbDD mechanisms to address critical aspects of data processing. These mechanisms include access control, which minimises the security risk of unauthorised access to physical and logical systems; data integrity, which restricts user authorisations to specific tasks or roles; data pseudonymisation, which replaces personal data with random codes; data encryption, which encodes personal data; data confidentiality, which applies password policies to protect data; data recoverability, which involves implementing data backups that are regularly checked for successful recovery of personal data; data evaluation, which entails conducting periodical reviews of TOMs for their effectiveness and plausibility; and transmission control, which involves implementing secure protocols for the transmission of data, such as SSL certificates for websites (https://) or SFTP (Secure Socket Tunnelling Protocol), designed to secure the online transfer of data.

⁵⁹⁴ This matrix helps identify potential threats to data privacy and security and provides a visual representation of their relative impact and probability. By utilising this matrix, organisations can focus on addressing the most significant risks, allocate resources more effectively, and enhance their overall data protection strategies. The data protection risk matrix is typically structured as a grid, with the likelihood of a risk occurring plotted on the horizontal axis, and the severity of the risk's impact on the vertical axis. The matrix is divided into different zones or quadrants, each representing a level of risk.

Despite being, by conception, a risk-based legal framework (Principles-based Regulation, 'PRB'), it is important to note that, while the GDPR requires organisations to conduct risk analyses and implement risk-based responses, the definition of "risk" remains ambiguous, defined only by reference to aspects of likelihood and severity, which may have a negative impact on individuals' rights and freedoms. Nonetheless, it is clear that the GDPR's definition of risk extends beyond privacy and data protection, as it includes other fundamental rights in its scope of application, such as the right to freedom of expression and non-discrimination. Furthermore, it imposes several ambiguous requirements for certain data processing activities (activities that may pose a high risk to the data subject) without providing a clear risk parametrization - when do specific processing activities pose a high risk?

For example, in the context of conducting a DPIA, Article 35(3) GDPR only provides a non-exhaustive list of when a processing operation is "likely" to result in high risks, namely, when 'a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person'; it involves 'processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10'; or when 'a systematic monitoring of a publicly accessible area on a large scale' applies.⁵⁹⁵

⁵⁹⁵ GDPR, Article 35(3).

In 2017, the WP29 issued guidelines and examples outlining the GDPR's data protection impact assessment requirements.⁵⁹⁶ The WP29 presented three scenarios in which a DPIA is unlikely to be required: (a) processing personal data from patients or clients by an individual healthcare provider or lawyer,⁵⁹⁷ (b) an online magazine using a mailing list to send a daily digest to subscribers, and (c) an e-commerce website displaying ads for vintage car parts, involving limited profiling based on items viewed or purchased on its website. The possible relevant criteria applicable to each scenario are the processing of sensitive data or data of a highly personal nature, data processed on a large scale, and data processed for evaluation or scoring purposes.⁵⁹⁸

Additionally, the WP29 identified several criteria to determine whether a particular processing activity requires a DPIA. These criteria include: (a) a hospital processing genetic and health data, where sensitive data or data of a highly personal nature is processed, data concerns vulnerable data subjects, or data is processed on a large scale; (b) the use of a camera system to monitor driving behaviour on highways, where systematic monitoring of data subjects occurs, and innovative or technological solutions are employed; (c) a company systematically monitoring employees' activities, including their workstation and internet use, where systematic monitoring of data subjects occurs, and data concerning vulnerable data subjects is processed; (d) an institution creating a national-level credit rating or fraud database, where evaluation or scoring algorithms are used, data is processed on a large scale, and data correlation is applied, and sensitive data or data of a

⁵⁹⁶ Article 29 Data Protection Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation' (2017) 2016/679.

⁵⁹⁷ GDPR, Recital 91.

⁵⁹⁸ Article 29 Data Protection Working Party, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation' (n 588).

highly personal nature is processed; and (e) the storage of pseudonymised personal sensitive data concerning vulnerable data subjects for archiving purposes in research projects or clinical trials, where personal sensitive data is processed, data concerns vulnerable data subjects, and processing prevents data subjects from exercising a right, using a service, or a contract.⁵⁹⁹

Apart from the aforementioned scenarios where a DPIA is likely to be required, the WP29 posits that data controllers must establish the appropriate level of security commensurate with the ‘nature, scope, context, and purpose of the processing.’ Practically, this translates into an evaluation of the risks posed by the processing activity and the corresponding security level that effectively addresses the risks of accidental, unlawful, or unauthorised destruction, loss, alteration, disclosure, or access to personal data.⁶⁰⁰

In this respect, the GDPR identifies the high-risk data processing operations as: a) those that use new technologies; b) those that are new and no DPIA has been carried out before; and c) those where a new DPIA has become necessary due to the time that has elapsed since the initial processing.⁶⁰¹ In order to decide the appropriate measures to implement, organisations must consider, *inter alia*, the state of the art, the cost of implementation, the nature, scope, context and purposes of processing, and the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing.⁶⁰² It is important to note, however, that a processing operation may

⁵⁹⁹ *ibid.*

⁶⁰⁰ GDPR, Article 32(2).

⁶⁰¹ GDPR, Recital 89.

⁶⁰² GDPR, Article 32(1).

correspond to the cases listed above while still being deemed by the data controller not "likely to result in a high risk." When this happens, the controller should justify and document the reasons for not conducting a DPIA, as well as include a record the DPO's (and external counsel, if applicable) views.

Therefore, organisations should consider including the following measures⁶⁰³ in their PbDD programme to ensure the protection of personal data:⁶⁰⁴ a) pseudonymisation and encryption⁶⁰⁵ (pseudonymisation is the processing in such a manner that the personal data can no longer be attributed to a specific data subject without using additional information);⁶⁰⁶ b) mechanisms to ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services;⁶⁰⁷ mechanisms to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;⁶⁰⁸ and mechanisms to regularly assessing the effectiveness of TOMs for ensuring the security of the processing.⁶⁰⁹

However, previous research has identified numerous and frequent constraints,⁶¹⁰ namely, in terms of budget allocated to cyber-security⁶¹¹ and scarcity of in-house skills to

⁶⁰³ See, for example, *Z v Finland, App no 22009/93 ECHR 1997-I*. See also, *I. v. Finland, App no 20511/03, (ECtHR, 17 July 2008)* (n 65). The failure to secure, through technical and organisational measures, the confidentiality of patient health data in a public hospital violates Article 8 ECHR.

⁶⁰⁴ Chapter Seven lists several measures that are applicable.

⁶⁰⁵ GDPR, Article 32(1)(a).

⁶⁰⁶ This additional information must be kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person in accordance with Article 4(5) GDPR.

⁶⁰⁷ GDPR, Article 32(1)(b).

⁶⁰⁸ GDPR, Article 32(1)(c).

⁶⁰⁹ GDPR, Article 32(1)(d).

⁶¹⁰ See, for example, Kalle Hjerpe, Jukka Ruohonen and Ville Leppanen, 'The General Data Protection Regulation: Requirements, Architectures, and Constraints', *2019 IEEE 27th International Requirements Engineering Conference (RE)* (IEEE 2019).

⁶¹¹ Andrew Fielder and others, 'Risk Assessment Uncertainties in Cybersecurity Investments' (2018) 9 Games.

promote, develop, and deploy the necessary plans, as well as implement technical measures, to ensure personal information security to GDPR standards. For this reason, it is crucial to go beyond the *lacunae* of the Regulation, and adopt a holistic approach to PbDD, that can clearly identify and fill in the regulative gaps, and on a case-by-case basis.

Regarding information security obligations, the application of insufficient TOMs to ensure information security, resulted in 281 fines issued by EU supervisory authorities, as of January 2023, in a total of €375,648,369.⁶¹² Hence, the PbDD programme should be built on a strategy based on information security, and include the following elements of cyber and risk management: TOMs to integrate security risk assessment in DPIA,⁶¹³ technical security measures (for example, intrusion detection, firewalls, monitoring),⁶¹⁴ TOMs to encrypt personal data,⁶¹⁵ implement procedures to restrict access to personal data, implement a corporate security policy, implement backup and business continuity plans, implement a data-loss prevention strategy, implement regular data security testing (including penetration testing), and obtain a security certification (e.g., ISO 27001).⁶¹⁶

⁶¹² Annex 1 provides a visualisation of GDPR fine statistics utilised in this work.

⁶¹³ See, Recital 76 of GDPR. ‘The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk.’

⁶¹⁴ See, Recital 78 of GDPR. ‘Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations.’

⁶¹⁵ See, Recital 93 of GDPR. ‘In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption.’

⁶¹⁶ See, Recital 100 of GDPR. ‘In order to enhance transparency and compliance with this Regulation, the establishment of certification mechanisms and data protection seals and marks should be encouraged, allowing data subjects to quickly assess the level of data protection of relevant products and services.’

According to the EDPB,⁶¹⁷ the concept of PbDD is mainly based on effectiveness. The requirement to effectively implement the principles means that controllers must put in place the necessary safeguards and measures to protect these principles in order to protect the rights of data subjects. Each implemented measure should thus produce the desired results for the processing that the controller has planned. This observation has two ramifications; firstly, it means that Article 25 does not require the implementation of any specific technical or organisational measures, but rather that the measures and safeguards chosen should be specific to the implementation of data protection principles into the specific processing in question. Therefore, the measures and safeguards should be designed to be robust, and the controller should be able to implement additional measures to scale to any increase in risk.⁶¹⁸ Whether or not measures are effective will thus be determined by the context of the processing in question, as well as an assessment of certain elements that should be considered when determining the means of processing. Secondly, controllers must be able to demonstrate that the principles were followed (accountability). Consequently, the implementation of standard information security (ISMS) models and effective structural design of organisations' information technologies (IT) ecosystems - which include hardware and software capable of guaranteeing the confidentiality, integrity, availability, and resilience⁶¹⁹ of processing systems and services⁶¹⁹ - must be considered as a critical factor in achieving adequate data security, at the GDPR

⁶¹⁷ European Data Protection Board (EDPB) (n 206).

⁶¹⁸ See Article 29 Data Protection Working Party, 'Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks' (2014) 14/EN WP 218 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf>.

⁶¹⁹ GDPR, Article 32(1)(b).

standard (of course, I assume here that the organisation has unrestricted access to the state of the art and that the implementation costs are not a limitation).^{620,621}

The magnitude of challenges that organisations encounter while implementing PbDD measures to tackle data security is immense, and solely for this reason, it can be inferred that integrating GDPR requirements into business operations is far from being straightforward, as Stoica and Ghizlane suggest.⁶²² To provide a broader perspective on the challenge of implementing PbDD in the context of personal data storage, it is important to note that the widespread existence of pre-GDPR data silos in most organisations represents a major barrier to integrating storage limitation principles into business operations. The reason for this is that these silos hold significant amounts of legacy data that are frequently related with vast structured (such as CRM systems) and unstructured data sets (such as loose Excel or Word files). While most of these data sets were legally collected under Directive 95/46/EC, the GDPR now considers any further processing as unlawful unless consent for processing is obtained - irrespective of the fact that, as noted by the ECtHR in the case of *K.H v Slovakia*,⁶²³ unfair processing is defined as the acquisition or processing

⁶²⁰ It is imperative to underscore that a robust data security program cannot solely rely on advanced information equipment and systems; rather, it stems from a harmonised application of these tools in combination with sound data hygiene practices and processes, suitable organisational policies, staff training, and an effective data security awareness program at both the organisational and data subject level. Integrating such a data protection culture into the Information Security Management System (ISMS) ensures that PbDD mitigates security risks, circumvents reputational damage, and precludes potential penalties for non-compliance.

⁶²¹ Recital 83 of the GDPR specifies some high-risk areas of processing that data controllers and processors should take into account while evaluating and implementing organisational security programs to prevent 'accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage'.

⁶²² Liviu Adrian Stoica and Chabbaki Ghizlane, 'Mathematical Approach on the GDPR Complexity' (2020) 16 *Journal of modern accounting and auditing*.

⁶²³ *K.H. and Others (2009)* (n 91).

of personal data in an unfair manner, through deception, or by concealing the process from the data subject.

From a practical standpoint, this also has implications for individuals' rights, such as the right to be forgotten. When an individual exercises their right to be forgotten, an organisation must ensure that all of their personal data is deleted. However, this can be challenging when the individual's data is present in any dataset across the organisation, including legacy data silos. In my opinion, this is one of the most significant challenges posed by the GDPR, and it is not something that PbDD can address independently.⁶²⁴

Addressing this issue may require the re-engineering of many system applications to incorporate security, detection, and process capabilities that can monitor data usage, collect it, link it to consent archives, and enable seamless traceability for Article 17 GDPR requests for data erasure. Such capabilities can help organisations to more effectively manage personal data and ensure compliance with the GDPR's requirements while facilitating the exercise of individuals' rights under the Regulation.⁶²⁵

Another important aspect to consider is the development of process controls to prevent off-purpose processing, which must be deployed as default. The right to erasure, when it comes to data backups is particularly problematic from the technical perspective, and thus very difficult to address by PbDD. Unstructured data, such as text documents and images, will be the primary focus of most erasure requests. Many "backup and restore" software tools back up unstructured data sets as images, rather than individual, easily

⁶²⁴ Blancco Technology Group, 'Locating Customer Data Will Be Half the Battle to Fulfill EU GDPR's "Right to Be Forgotten"' (2017) 47 *Database and Network Journal* 5+.

⁶²⁵ One of the main challenges facing organisations in addressing this issue is the need to redesign almost all of their applications, which can be a costly and time-consuming process.

readable files. Image backups loses individual granularity across backup sessions, making it nearly impossible to search all backups for an individual's specific information.⁶²⁶

It is worth noting that my research indicates that the theme of "non-compliance with general data processing principles" includes concerns regarding storage limitation and data quality. This theme represents the highest total sum of fines issued by supervisory authorities and the second highest number of fines imposed. This section has explored the complexities of data storage by examining the implementation of appropriate TOMs on business systems and processes, emphasising the principles of integrity and confidentiality (security), data minimisation, and storage limitation. I suggest that future research delve deeper into the potential repercussions of poor data retention practices. This could include establishing linkages between data subject rights, data breaches, and emerging technologies, which were beyond the scope of this study.

⁶²⁶ As previously stated, a retention strategy must be developed at the corporate level; however, a right to erasure request will require that the entire data set be erased, invalidating the backup and potentially violating other retention requirements. There is a pervasive belief that backup data is exempt from the erasure requirement because it is unusable until restored. However, neither the EU Supervisory authorities nor the EU state member courts have validated this assumption, which makes compliance with the right to erasure impractical in certain instances.

6.3. PbDD the first line of defence to prevent data breaches

In today's data-driven world, data breaches are becoming increasingly prevalent, and their impacts on individuals, organisations, and society as a whole can be significant.⁶²⁷ Such breaches may result from a variety of intentional or unintentional factors, such as cyberattacks, theft, malware, phishing, or human fallibility. Data breaches are a matter of great concern due to the potential compromise of personal and sensitive information, such as financial records, medical records, intellectual property, or personal data, including names, addresses, national insurance numbers, and passwords. Such information may be exploited for various malicious purposes, including but not limited to identity theft, financial fraud, cyberattacks, and other nefarious activities. In the context of data breaches, PbDD and GDPR play a critical role in preventing them from happening in the first place. PbDD's emphasis on data protection from the outset of system development and implementation is the first line of defence against data breaches.

Nonetheless, PbDD cannot be reduced to a 'one-size-fits-all' mechanism for implementing technical measures, such as pseudonymisation, which is intended to prevent data breaches and is applied during the design and development stages of information systems, and then 'left alone.' While, at first glance, PbDD appears to be purely technological, the truth is that it plays a vital role in nearly all aspects of data protection governance, not just focusing on data loss. Since data loss incidents can have negative consequences for the rights and freedoms of data subjects, both aspects of data protection "by design" and "by default" are relevant in the context of GDPR. The common

⁶²⁷ A data breach refers to an occurrence wherein confidential, sensitive, or otherwise safeguarded information is illicitly accessed or disclosed by unauthorised persons or systems.

denominator between them is the requirement for the implementation of appropriate TOMs. To further explore the role of PbDD in the protection against personal data incidents, this work uses the data breach phenomenon as a case study. Regarding personal data breaches, Recital 85 of the GDPR states:

‘A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.’⁶²⁸

This means that a data breach can cause a variety of negative consequences for individuals. According to Article 4 GDPR a breach of personal data is about more than losing data, rather, it is defined as an incident that affects the confidentiality,⁶²⁹ integrity,⁶³⁰ or availability⁶³¹ of personal data. If such a breach creates a risk of physical, material, or non-material harm to data subjects, for example in situations leading to identity theft, financial loss, damage to an individual’s reputation, or an individual’s loss of control over their

⁶²⁸ GDPR, Recital 85.

⁶²⁹ As only authorised users and processes should be able to access and modify data.

⁶³⁰ For data to be secure, it should not be vulnerable to unauthorised change, whether by accident or on purpose.

⁶³¹ Authorised users should be able to access data whenever necessary.

personal data, then notification and involvement of the supervisory authority is required.⁶³²

Data breach, therefore, not only refers to the principles of data protection formulated in Article 5 GDPR, but is also intrinsically connected to the variables ‘state of the art’,⁶³³ ‘cost of implementation’,⁶³⁴ ‘nature, scope, context and purpose of processing’,⁶³⁵ as well as to the ‘risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing’⁶³⁶ which in Articles 25 and 32 GDPR, represent the elements of the “balancing exercise” that precedes the implementation of any appropriate TOMs. As part of the organisation's breach management process, the

⁶³² GDPR, Article 33.

⁶³³ See European Data Protection Board (EDPB) (n 206). ‘The concept of “state of the art” is present in various EU acquis, e.g. environmental protection and product safety. In the GDPR, reference to the “state of the art” is made not only in Article 32, for security measures, but also in Article 25, thus extending this benchmark to all technical and organisational measures embedded in the processing.’; ‘In the context of Article 25, ‘the reference to “state of the art” imposes an obligation on controllers, when determining the appropriate technical and organisational measures, to take account of the current progress in technology that is available in the market. The requirement is for controllers to have knowledge of, and stay up to date on technological advances; how technology can present data protection risks or opportunities to the processing operation; and how to implement and update the measures and safeguards that secure effective implementation of the principles and rights of data subjects taking into account the evolving technological landscape.’

⁶³⁴ *ibid.* ‘The controller may take the cost of implementation into account when choosing and applying appropriate technical and organisational measures and necessary safeguards that effectively implement the principles in order to protect the rights of data subjects. The cost refers to resources in general, including time and human resources.’; ‘[T]he cost element does not require the controller to spend a disproportionate amount of resources when alternative, less resource demanding, yet effective measures exist. However, the cost of implementation is a factor to be considered to implement data protection by design rather than a ground to not implement it.’

⁶³⁵ *ibid.* ‘In short, the concept of nature can be understood as the inherent characteristics of the processing. The scope refers to the size and range of the processing. The context relates to the circumstances of the processing, which may influence the expectations of the data subject, while the purpose pertains to the aims of the processing.’

⁶³⁶ *ibid.* ‘The GDPR adopts a coherent risk-based approach in many of its provisions, in Articles 24, 25, 32 and 35, with a view to identifying appropriate technical and organisational measures to protect individuals, their personal data and complying with the requirements of the GDPR. The assets to protect are always the same (the individuals, via the protection of their personal data), against the same risks (to individuals’ rights), taking into account the same conditions (nature, scope, context and purposes of processing).’

PbDD strategy should include a risk assessment and a risk assessment matrix to aid in the management of personal data breaches.⁶³⁷

There is little empirical evidence that demonstrates the contribution of PbDD to the realisation of data protection principles⁶³⁸ and how the effectiveness of PbDD depends on the applicability of TOMs. Nevertheless, in this regard, the EDPB Guidelines states:

‘Effectiveness is at the heart of the concept of data protection by design. The requirement to implement the principles in an effective manner means that controllers must implement the necessary measures and safeguards to protect these principles, in order to secure the rights of data subjects. Each implemented measure should produce the intended results for the processing foreseen by the controller.’⁶³⁹

The approach of the GDPR towards data breaches is founded on the principle that prevention is better than cure. By mandating organisations implement appropriate measures to ensure the security of personal data, the GDPR aims to prevent data breaches from occurring in the first place.⁶⁴⁰ In the event that a breach does occur, the GDPR's breach notification requirement is designed to ensure that affected individuals are informed promptly, and that remedial action can be taken to mitigate the risks associated

⁶³⁷ The European Union Agency for Network and Information Security (ENISA) has published guidelines for determining the severity of personal data breaches. See ‘Recommendations for a Methodology of the Assessment of Severity of Personal Data Breaches’ (ENISA) <<https://www.enisa.europa.eu/publications/dbn-severity>>.

⁶³⁸ Spiekermann (n 72).

⁶³⁹ European Data Protection Board (EDPB) (n 206). para. 13.

⁶⁴⁰ Hence, Article 32 of the GDPR requires data controllers and processors to implement appropriate measures to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services. These measures must take into account the nature, scope, context, and purposes of processing, as well as the risks to the rights and freedoms of data subjects.

with the breach. Article 33 requires data controllers to notify the relevant supervisory authority within 72 hours of becoming aware of a personal data breach, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. Data processors, on the other hand, are required to notify the controller of a personal data breach without undue delay. Data subjects also have the right to be informed if a data breach is likely to result in a high risk to their rights and freedoms, under Article 34 GDPR. This notification must be made without undue delay.⁶⁴¹

Data breaches resulting from inadequate implementation of PbDD typically result in hefty fines from supervisory authorities, claims for damages for financial loss and distress caused to individuals (including class actions),⁶⁴² in addition to creating a risk of reputational damage for organisations. Consequently, it is crucial to examine the PbDD "quandaries" within the context of the GDPR to equip data controllers with data protection strategies that conform to the GDPR and offer greater safeguards for the rights and freedoms of data subjects, while mitigating the risk of fines from regulators. As an illustration, the largest fine under the GDPR as of January 2023 was €746 million, which was imposed on Amazon Europe Core S.à.r.l. for non-compliance with general data processing principles. Meta Platforms Ireland Limited, was fined €265 million on 25 November 2021 for failing to implement sufficient TOMs to ensure information security.⁶⁴³

⁶⁴¹ These requirements are intended to promote transparency and enable prompt action to mitigate the risks associated with data breaches. Failure to comply with these requirements can result in significant fines and other penalties.

⁶⁴² Data breaches involving high-profile companies, including Google, Amazon, Meta, British Airways, and Equifax have affected thousands of data subjects. The subsequent group court actions have raised the public's awareness of GDPR rights and how to enforce them.

⁶⁴³ Annex 1 presents a visualisation of the analysis conducted on fines imposed under GDPR.

6.4. Concluding remarks

This chapter has explored the applicability of PbDD within the GDPR framework, addressing key areas such as legacy data clean-up for compliance, storage limitation, and the role of PbDD in ensuring the security of processing. The unique challenges posed by legacy data require a strategic approach, and PbDD emerges as a valuable tool for systematic resolution. The DPPA, in this context, not only facilitates legacy data clean-up but also establishes an enduring framework for data protection.

By integrating data protection measures into the design and default settings of data processing systems, PbDD ensures that businesses not only comply with the security requirements outlined in Article 32 but also adhere to the core principles of the GDPR. This comprehensive approach enhances protection against potential data breaches, which have become increasingly common in today's data-driven world.

As demonstrated, PbDD and GDPR collectively serve as essential tools for preventing data breaches and safeguarding personal data. PbDD embeds data protection and security throughout the system development and usage stages, while GDPR mandates explicit requirements for data controllers and processors, including breach notification obligations.

Transitioning to the next chapter, our exploration will broaden to encompass additional challenges posed by the GDPR. We will navigate through complexities inherent in GDPR such as data security, address concerns related to the lack of clarity that may undermine international data transfers and delve into the considerations surrounding the costs of GDPR implementation.

Chapter 7 – Examining additional challenges arising from GDPR: Data Security, Ambiguity in International Transfers, and Implementation Costs

‘[The GDPR] forces organisations to balance the risk to privacy of data subjects *against the costs of implementation* options, such as TOMs [...] or stopping processing personal data. [...] The GDPR provides no practical guidance about how to balance abstract legal assets, epistemic and technical aspects, and economic costs.’⁶⁴⁴

Introductory notes

My main argument is that GDPR compliance can prove complex, expensive, and disruptive since organisations must devote time and resources to upgrade their systems and processes to meet the security standards mandated by the Regulation. GDPR compliance involves many components that affect organisations in a variety of ways and at all levels.

Several studies have explored the complexities of GDPR. One of these studies even proposed the development of a mathematical method to quantify the GDPR's complexity. In this regard, Stoica and Ghizlane⁶⁴⁵ concluded that GDPR is not overly complex to understand and is relatively simple to implement; however, the costs associated with compliance can potentially negatively impact small business growth. Nonetheless, when this factor is balanced with increased customer trust (brand trust, for example, results in a higher number of customers) the balance between costs and benefits is equilibrated.

⁶⁴⁴ Annika Selzer, Daniel Woods and Rainer Bohme, ‘An Economic Analysis of Appropriateness under Article 32 GDPR Reports: Practitioners’ Corner’ (2021) 7 European Data Protection Law Review (EDPL) 456. (emphasis added).

⁶⁴⁵ Stoica and Ghizlane (n 614).

These findings present a contrasting view to previous studies. The figure below displays the primary challenges for GDPR compliance in the European Union and the United Kingdom in June 2018, unsurprisingly contradicting Stoica and Ghizlane's findings. According to the findings of a survey of IT and legal professionals, the complexity of Regulation was a common issue for 72% of European and 58% of English professionals, respectively.

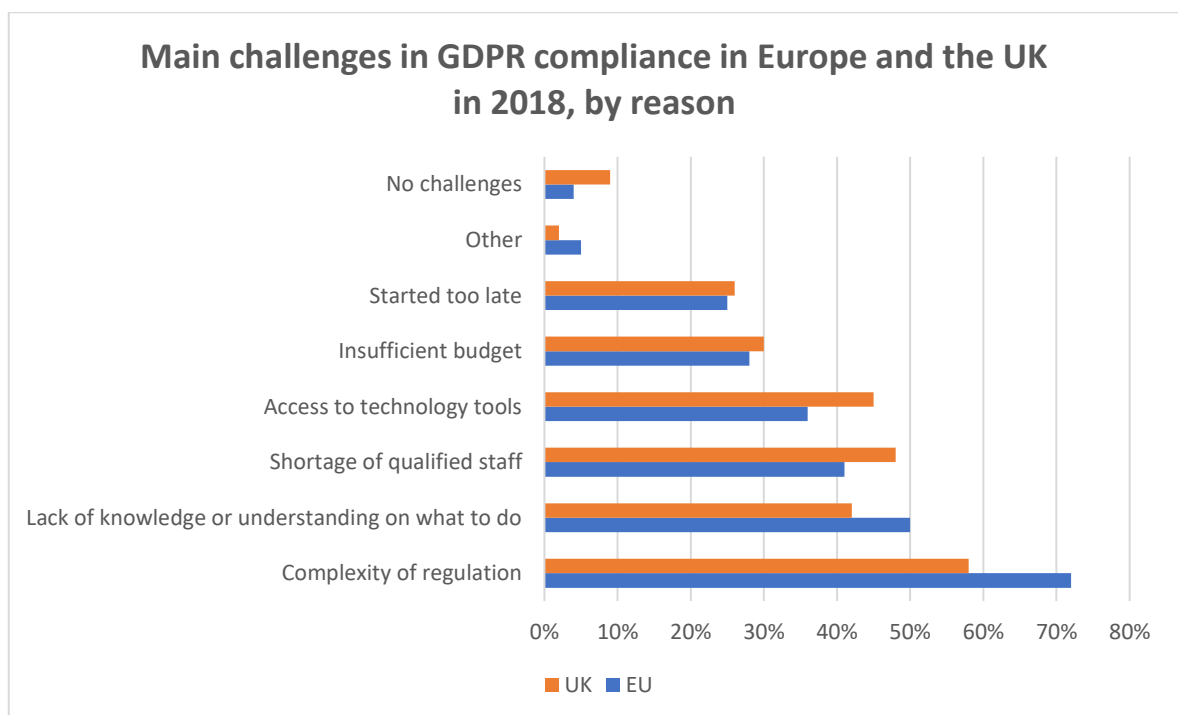


Figure 14 - TrustArc. (July 1, 2018). Main challenges in GDPR compliance in Europe and the UK in 2018, by reason [adapted]. In Statista. <<https://www.statista.com/statistics/1005011/main-challenges-in-gdpr-compliance-in-europe-and-uk/>>.

In this Chapter, I will explore the factors that I believe contribute to the complexity of GDPR from a practical implementation perspective, and also discuss the potential economic impact on organisations.

7.1. Devising a PbDD approach to data security

When discussing the operationalisation of the law, Jonathan Bamford, quoted in Butterworths Data Security Law and Practice, states that '[M]inimising personal information and affording it proper security at the human, organisational, or technical level are essential aspects of the law.'⁶⁴⁶ Additionally, Howard A. Schmidt offers the following insight:

'[I]t is essential that data controllers get to grips with the process of law reform and advancements in types and forms of Regulation. Things are moving very quickly in this area, as the law seeks to keep up with the threats to data and systems, which are constantly evolving and changing in nature.'⁶⁴⁷

Both statements reaffirm my conviction, which I have expressed throughout this work, that achieving data security and protection under the GDPR can be challenging. According to the UK Office of National Statistics ('ONS'), the rise in personal data fraud and computer misuse, as well as criminal cyber-attacks on businesses, continues to accelerate.⁶⁴⁸ The implementation of a preventive cyber-security management mechanism through PbDD, capable of effectively handling various incidents, such as phishing, file hijacking, screenshot

⁶⁴⁶ Stewart Room, *Butterworths Data Security - Law and Practice* (LexisNexis 2009).

⁶⁴⁷ *ibid.*

⁶⁴⁸ Office for National Statistics, 'Overview of Fraud and Computer Misuse Statistics for England and Wales' (2018) Crime and Justice <<https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/Articles/overviewoffraudandcomputer misusestatisticsforenglandandwales/2018-01-25>>.

capturing, ad clicking, hacking, or DDoS attacks, has been a topic of discussion in data protection circles.

As GDPR requires organisations to implement specific TOMs to ensure the security of processing of personal data,⁶⁴⁹ I believe that any data protection strategy must consider the implementation, in parallel with PbDD, of an Incident Response Methodology ('IRM') as it helps organisations to manage the cyber-security aspects in their information systems and IT environments, as well as responding to eventual breaches or criminal cyber-attacks. Depending on the results of a PbDD gap analysis, the characteristics of the organisation and processes involved in the processing of personal data, this could include developing and putting in place an action plan to handle any eventual security incidents, data breaches and cyber threats – Incident Response Plan.⁶⁵⁰ This will guarantee that a mechanism is in place to ensure the effective security of personal data (and compliance with the accountability principle)⁶⁵¹ across the organisation's data ecosystem. Thus, the IRM should be implemented in such a way that it remains active and operational across the whole personal data life cycle.⁶⁵² Although it may be a difficult undertaking, especially given that small and medium enterprises ('SMEs') face numerous and frequent restraints,⁶⁵³ namely in terms of the budget allocated to cybersecurity,⁶⁵⁴ and availability of in-house skills to

⁶⁴⁹ GDPR, Article 32.

⁶⁵⁰ To explore the topic of IRM within the framework of GDPR, see, Gant Redmon, 'Incident Response Under GDPR: What to Do Before, During and After a Data Breach' (*Incident Response*, 27 July 2018) <<https://securityintelligence.com/incident-response-under-gdpr-what-to-do-before-during-and-after-a-data-breach/>>.

⁶⁵¹ GDPR, Article 5(2).

⁶⁵² A factor that must be considered when selecting and deploying PETs.

⁶⁵³ Aneta Ponzewska-Maranda, 'Security Constraints in Modeling of Access Control Rules for Dynamic Information Systems' in Viliam Geffert and others (eds), *SOFSEM 2014: Theory and Practice of Computer Science* (Springer International Publishing 2014).

⁶⁵⁴ Fielder and others (n 603).

promote, develop and deploy the required plans and associated technical measures,⁶⁵⁵ it proves to be an outstanding tool for helping organisations close the cybersecurity gap identified in the GDPR.

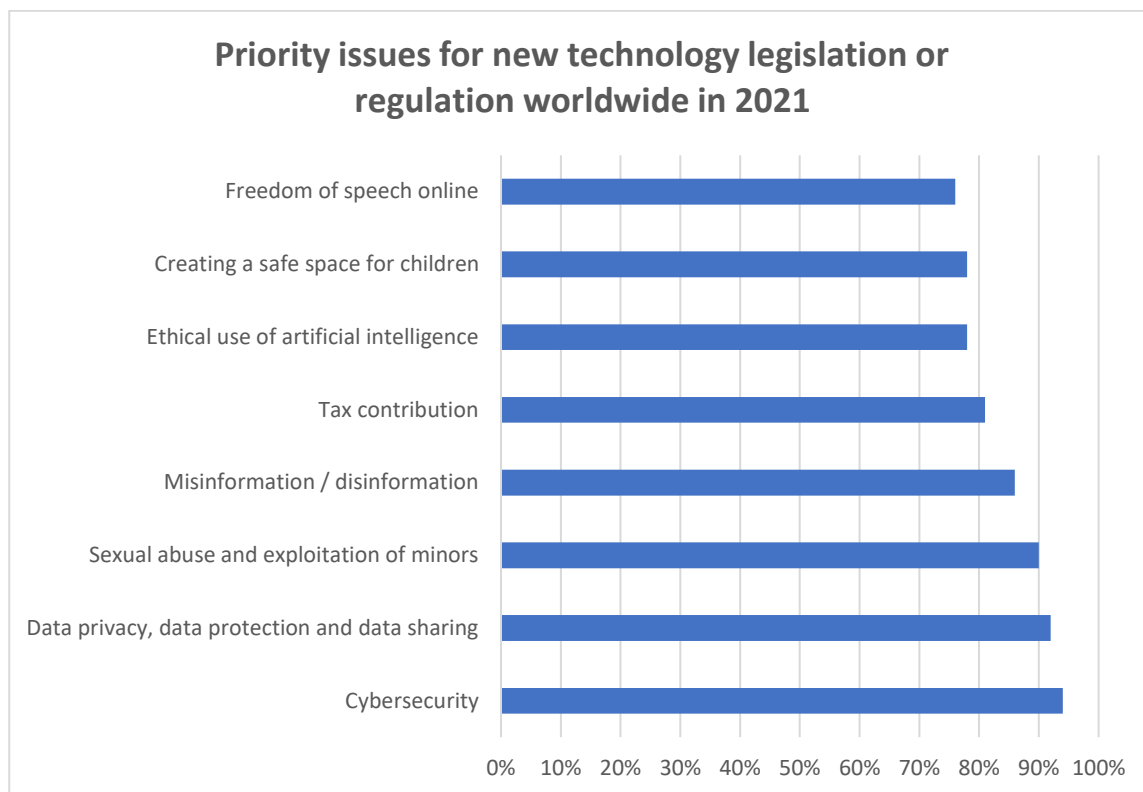


Figure 15 - Clifford Chance, & Milltown Partners. (November 9, 2021). Priority issues for new technology legislation or Regulation worldwide in 2021 [adapted]. In Statista, <<https://www.statista.com/statistics/1279546/new-legislation-priority-issues-worldwide/>>.

Figure 15 shows that 94 percent of respondents in a 2021 study conducted in the United States, which also included data collected in the United Kingdom, Germany, and France, expressed a preference for prioritising cybersecurity⁶⁵⁶ in new legislation or Regulation. In

⁶⁵⁵ Paul Baybutt, 'Cyber Security Vulnerability Analysis: An Asset-Based Approach' (2003) 22 Process Safety Progress 220.

⁶⁵⁶ Cybersecurity is usually defined as the practise of defending computers, servers, mobile devices, electronic systems, networks, and data from hostile intrusions (mainly, unauthorised access to personal data).

addition, respondents cited data privacy, data protection, and data sharing as concerns, with 92 percent indicating that technology companies did not address these matters effectively.

In my opinion, when formulating data protection legislation, policymakers should carefully consider how computer system properties should be incorporated into the law.⁶⁵⁷

A crucial feature of high-end CRMs, such as Microsoft Dynamics,⁶⁵⁸ is the capability to integrate via conversation Intelligence⁶⁵⁹ the organisation retention policy - if a retention time limit is set, the system will retain call recording data for the duration of that time limit. At the trigger point, the system automatically deletes the personal data,⁶⁶⁰ ensuring that the processing poses no further risk to individuals' rights in terms of storage limitation. As we have seen, one of the main challenges for PbDD is to ensure compliance with the storage and time limitation requirements of GDPR, therefore, it is of the utmost importance for organisations to have access to these privacy-enhancing technologies.⁶⁶¹

The effectiveness of “stand-alone PETs” is now a topic of debate in privacy circles,⁶⁶² with the general consensus being that ‘only PETs supportive of PDP [Personal Data

⁶⁵⁷ Dag Wiese Schartum, ‘Making Privacy by Design Operative’ (2016) 24 *International Journal of Law and Information Technology* 151.

⁶⁵⁸ Microsoft, ‘Privacy and Personal Data for Microsoft Dynamics 365’ (2022) <<https://docs.microsoft.com/en-us/dynamics365/get-started/gdpr/>>.

⁶⁵⁹ Microsoft, ‘Data Retention and Access through Privacy Settings’ (2022) <<https://docs.microsoft.com/en-us/dynamics365/sales/data-retention-deletion-policy>>.

⁶⁶⁰ *ibid.*

⁶⁶¹ PETs, for example, are a crucial complement to PbDD in safeguarding personal data, and they are commonly used in contemporary customer relationship management (CRM) systems due to their extensive security capabilities. These features include data encryption, multilevel security, anti-hacking controls, and regular security updates. The majority of these PETs empower businesses to establish roles and access privileges, providing varying levels of user access to guarantee that only authorised personnel can access personal information. Furthermore, these technologies facilitate compliance with the right to erasure by streamlining the identification of an individual's personal data and enabling straightforward updates or deletions of their records, typically with a single click.

⁶⁶² Štarchoň and Pikulík (n 345).

Protection] are not enough.⁶⁶³ By combining the use of PETs with other important PBDD elements, such as policies and procedures, organisations can create a more robust and effective program to protect personal data. Regarding the role of PETs, Damian Tamburri suggests:

‘[S]ystems should be re-designed to make the use of privacy-enhancing technologies as well as security-enhancing approaches or middleware parametric, enacted only wherefore the evidence of their application makes explicit its effectiveness to interested data subjects’.⁶⁶⁴

Notably, PETs cannot be used as a one-size-fits-all solution; their deployment must be duly considered vis-à-vis the categories of data processed, including special categories of personal data, the rights of data subjects and applicable data protection principles. Furthermore, instead of relying on Cavoukian's principle of "full-functionality" as a means to reconcile organisational interests with individual rights (in a positive-sum, non-zero-sum manner), a successful PbDD programme will strive to amplify individual rights without any implicit trade-offs, establish organisational and technological controls, and forestall any risks that may undermine individuals' rights by default.

PETs also play a crucial role in facilitating compliance with the international transfer of data requirements under the GDPR, which imposes stringent conditions on the cross-border transfer of personal data to ensure that individuals' privacy rights are adequately protected, especially when data moves outside the European Economic Area (EEA). PETs

⁶⁶³ *ibid.* (emphasis added).

⁶⁶⁴ Damian A Tamburri, 'Design Principles for the General Data Protection Regulation (GDPR): A Formal Concept Analysis and Its Evaluation' (2020) 91 *Information systems* (Oxford) 101469.

contribute to meeting these international data transfer requirements, namely by incorporate principles of data minimisation, ensuring that only the necessary data is transferred internationally. Utilising encryption as a privacy-enhancing measure safeguards data during its transfer across borders. The GDPR recognises encryption as a security measure, and the use of PETs to encrypt personal data supports compliance with the regulation's data protection principles, particularly those outlined in Article 32. Some PETs include advanced consent mechanisms that empower individuals to control the international transfer of their data. These mechanisms ensure that individuals are informed and provide explicit consent, aligning with GDPR requirements for lawful and transparent data processing. PETs designed for managing cross-border data flows provide organisations with tools to navigate the complexities of international data transfers. These technologies assist in assessing and managing risks, ensuring that organisations adhere to the GDPR's standards for the transfer of personal data outside European borders.

7.2. The lack of clarity in the GDPR undermines international data transfers

Transatlantic cooperation issues also arise from the vagueness of the GDPR, which creates additional barriers to the application of PbDD to processing that involves international transfers of personal data. In this respect, the former US secretary of commerce Wilbur Ross, cited in the Pinsent Masons Set Out-Law Blog,⁶⁶⁵ urged the EU authorities to create

⁶⁶⁵ Pinsent Masons, 'GDPR Lacks Clarity and Threatens Transatlantic Trade, Says Ross' (*Out-Law News*, May 31 2018) <<https://www.pinsentmasons.com/out-law/news/gdpr-lacks-clarity-threatens-transatlantic-trade>>.

clearer rules and a more predictable regulatory environment to support investment and innovation, stating:

‘GDPR creates serious, unclear legal obligations for both private and public sector entities, including the US government. We do not have a clear understanding of what is required to comply. That could disrupt transatlantic co-operation on financial Regulation, medical research, emergency management co-ordination, and important commerce.’⁶⁶⁶

The United States is a good example of the GDPR's lack of clarity and practical guidance regarding international transfers of personal data. Both the Schrems I⁶⁶⁷ and Schrems II⁶⁶⁸ cases are instances where the EU and US data protection frameworks collide. Following the CJEU's ruling in Schrems II,⁶⁶⁹ which invalidated the adequacy decision that underpins the EU-US Privacy Shield Framework, (which more than 5,300 companies relied on for transatlantic personal data transfers), many controllers found themselves in limbo when it came to transferring personal data to the US.

As a result of the CJEU's decision, organisations are under increased pressure to implement additional measures to protect personal data and demonstrate that all aspects of data transfer,⁶⁷⁰ including assessments of compliance with third country data protection laws have been carried out with due diligence. Ewa Kurowska-Tober, Global Co-Chair of

⁶⁶⁶ *ibid.*

⁶⁶⁷ *Schrems [2015]* (n 211).

⁶⁶⁸ *Facebook Ireland and Schrems [2020]* (n 212).

⁶⁶⁹ Emanuel Lobato Cervantes (n 442).

⁶⁷⁰ See Ross McKean, Ewa Kurowska-Tober and Heidi Waem, ‘DLA Piper GDPR Fines and Data Breach Survey: January 2022’ (2022) <<https://www.dlapiper.com/en/uk/insights/publications/2022/1/dla-piper-gdpr-fines-and-data-breach-survey-2022/>>.

DLA Piper's Data Protection & Security Group, stated that 'even for the most advanced and well-resourced organisations', it is difficult to meet the requirements of Schrems II, let alone small and medium-sized businesses.⁶⁷¹ Across the Atlantic, the Office of the US Director of National Intelligence Acting General Counsel Bradley Brooker, Department of Justice Associate Deputy Attorney General Sujit Raman and Department of Commerce International Trade Administration Deputy Assistant Secretary James Sullivan had already urged the EU and the US to start talks on cross-border data flows in order to help clarify this situation. According to these officials, the lack of transparency and guidance from the EU could pose a serious future problem in the transfer of personal data.⁶⁷²

Furthermore, in June 2020, the European Commission published a report on the progress of the Regulation so far, acknowledging the difficulties in implementing the data protection Regulation.⁶⁷³ The existence of a 'very serious to-do list' to enforce the Regulation consistently across the EU was confirmed by Věra Jourová, Commission VP for values and transparency, who stated that 'The European Data Protection Board and the data protection authorities have to step up their work to create a truly common European culture – providing more coherent and more practical guidance, and work on vigorous but uniform enforcement.'⁶⁷⁴ While the report does not translate a *mea culpa* claim, it clearly conveys the idea that to be truly effective, the EU needs to provide clearer compliance guidance that is consistent across countries. As Ewa Kurowska-Tober suggests; '[W]hat is

⁶⁷¹ *ibid.*

⁶⁷² Bradley A. Brooker, Sujit Raman and James M. Sullivan, 'The Need for Clarity After Schrems II' (*Lawfare*, 29 September 2020) <<https://www.lawfareblog.com/need-clarity-after-schrems-ii>>.

⁶⁷³ European Commission, 'Two Years of the GDPR: Questions and Answers' (2020) QANDA/20/1166 <https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_1166>.

⁶⁷⁴ Natasha Lomas, 'GDPR's Two-Year Review Flags Lack of "vigorous" Enforcement' (*TechCrunch+*, 24 June 2020) <<https://techcrunch.com/2020/06/24/gdprs-two-year-review-flags-lack-of-vigorous-enforcement/>>.

really needed is a resolution of the underlying conflict of laws rather than imposing an unrealistic compliance burden onto business and another headwind to international trade (...).⁶⁷⁵

Following the implementation of GDPR, the lack of clarity in the Regulation also hampered important worldwide internet businesses such as domain registrars. In 2018, the Internet Corporation for Assigned Names and Numbers ('ICANN') requested special guidance and a moratorium from European regulators so that they would not face enforcement proceedings while implementing adjustments to comply with the GDPR. ICANN was 'concerned that continued ambiguity on the application of the GDPR to the global WHOIS may result in many domain name registries and registrars choosing not to publish or collect WHOIS out of fear that they will be subject to significant fines following actions brought against them by the European SAs.'⁶⁷⁶

The issues of international data transfers are also intricately linked to the cost of implementing specific TOMs. Implementing specific TOMs is critical for ensuring the security and confidentiality of personal data during international transfers. These measures, while enhancing data protection, may entail significant upfront and ongoing costs. Moreover, the cost of implementing TOMs needs to consider their compatibility with international standards and legal frameworks. Ensuring alignment with the legal requirements of the jurisdictions involved in the transfer may involve additional expenses, such as legal consultations and compliance assessments, as we will discuss in the next section.

⁶⁷⁵ McKean, Kurowska-Tober and Waem (n 662).

⁶⁷⁶ 'ICANN: Clarity Required on GDPR Compliance' [2018] Enterprise Innovation <<https://www.proquest.com/trade-journals/icann-clarity-required-on-gdpr-compliance/docview/2021099454/se-2?accountid=13460>>.

7.3. How does the cost of implementation affect PbDD?

While the GDPR has provided several benefits to both businesses and individuals, it is clear that it has also resulted in a number of unintended consequences. As we have seen, organisations face significant compliance risk as a result of ambiguous legal provisions, uncertainty about how those provisions will be interpreted by supervisory authorities, and heavy fines from regulators for non-compliance. Furthermore, many organisations believe they are spending more money than expected to achieve GDPR compliance.⁶⁷⁷ Understanding the impact of PbDD implementation costs on organisations is critical because it can be a trigger for GDPR non-compliance. I will next examine the effect of the costs of implementation in the implementation and maintenance of a PbDD programme.

In March 2019, in her statement ‘On the General Data Protection Regulation and California Consumer Privacy Act: Opt-ins, Consumer Control, and the Impact on Competition and Innovation,’ before the US Senate Judiciary Committee, Roslyn Layton identified the following major GDPR issues:⁶⁷⁸ (i) GDPR strengthens the largest players,⁶⁷⁹

⁶⁷⁷ See, ‘GDPR Implementation Costs Enterprises More than Expected’ (2018) 55 Security 14. Six months after the GDPR went into force, 41 per cent of organisations respondents to a Verasec survey, stated that they were paying more for achieving compliance with GDPR than anticipated.

⁶⁷⁸ Roslyn Layton, ‘The 10 Problems of the GDPR, The US Can Learn from the EU’s Mistakes and Leapfrog Its Policy’ (2019) <<https://www.judiciary.senate.gov/imo/media/doc/Layton%20Testimony1.pdf>>.

⁶⁷⁹ It is also important to consider that some landmark shifts in the spheres of privacy and data protection law happened due to the action, or lack thereof, from those true “giants” of the world economy. As an example, in the *Google Spain* case, the CJEU produced a decision which almost incorporates a data protection framework in and of itself, namely, in respect to the clarification of legal definitions provided, such as the definition of processing – upheld in the decision in *Lindquist* - and of controller. The Court also made important clarifications in the area of the data subject rights, making it clear that an economic interest cannot justify the potential seriousness of the interference with those rights, and by upholding the right to erasure - which in this case, meant that Google should erase any information and any links to information that appears inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing – created a new privacy paradigm: the “right to be forgotten”.

(ii) weakens small – and medium – sized firms⁶⁸⁰ and, (iii) is cost prohibitive for many companies. I would add that it also increases transaction costs, which in turn increases the prices individuals pay for goods and services. The following figure depicts the outcomes of a 2017 survey of IT decision-makers on the downsides of the GDPR for UK citizens. The findings indicate that fifty-six percent of respondents believed that companies would raise their prices to safeguard themselves from GDPR fines.

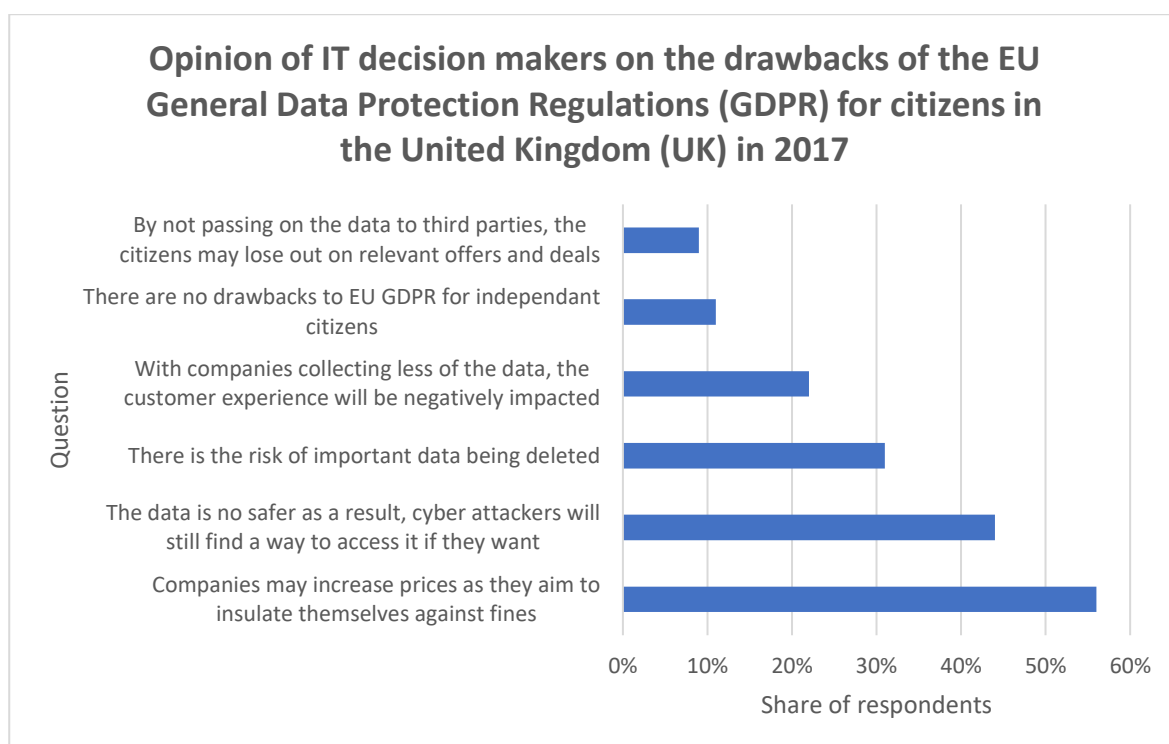


Figure 16 - Varonis. (May 18, 2017). Opinion of IT decision makers on the drawbacks of the EU General Data Protection Regulations (GDPR) for citizens in the United Kingdom (UK) in 2017 [adapted]. In Statista. <<https://www.statista.com/statistics/796083/gdpr-opinion-on-drawbacks-for-citizens-in-the-uk/>>.

It is evident that the GDPR imposes significant compliance costs on data controllers and processors. As per the International Association of Privacy Professionals (IAPP), an

⁶⁸⁰ See James Campbell, Avi Goldfarb and Catherine Tucker, 'Privacy Regulation and Market Structure' (2015) 24 Journal of Economics & Management Strategy 47.

organisation with five hundred employees would require an expenditure of roughly three million dollars (USD 3,000,000) to attain GDPR compliance.⁶⁸¹ However, the degree of both quantitative and qualitative personal data processing is positively associated with the size of an organisation, which implies that large businesses are more likely to allocate more resources toward GDPR compliance than medium and small enterprises.⁶⁸² In terms of the cost of implementation of PbDD, the main factor to consider is that data controllers and processors must comply with several provisions that translate into direct costs, such as implementing TOMs to protect data and incorporating data protection principles and data subject's rights into business operations.⁶⁸³ Another example relates to international transfers of personal data, where Adequacy decisions, standard contractual clauses (SCCs), binding corporate rules (BCRs), and other safeguards are essential for lawful international data transfers. Meeting the GDPR's requirements for international data transfers often requires complex technical solutions. Implementing TOMs that address the intricacies of cross-border compliance, including differing legal standards and local data protection regulations, can elevate the associated costs. Of course, The scalability and flexibility of TOMs are crucial factors influencing costs. Adapting these measures to the evolving landscape of international data transfers may require ongoing investment, particularly as regulatory landscapes change, or new standards emerge.

⁶⁸¹ The International Association of Privacy Professionals and Ernst & Young, 'IAPP-EY Annual Privacy Governance Report 2018' (2018) <https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/financial-services/ey-iapp-ey-annual-privacy-gov-report-2018.pdf>.

⁶⁸² Adam Faihr and Martin Januška, 'Factors Determining the Extent of GDPR Implementation within Organisations: Empirical Evidence from Czech Republic' (2021) 22 *Journal of Business Economics and Management* 1124.

⁶⁸³ Creating a system to gain affirmative consent from individuals to process their data on the website or engaging a data protection officer are examples of PbDD direct costs.

Moreover, in evaluating the adequacy of TOMs, it is imperative to take into account not only the processing circumstances and potential harm to data subjects but also environmental economic factors. Articles 25 and 32 of the GDPR explicitly refer to the "cost of implementation" as a factor to be considered.⁶⁸⁴

The inclusion of such a financial risk for organisations⁶⁸⁵ in the GDPR raises several questions, such as whether the cost of implementation only refers to the costs incurred by the controller when a measure is implemented, and whether this selection criterion for TOMs also takes into account the individual situation of the controller.⁶⁸⁶

This financial risk for organisations should be considered when determining whether the costs of a measure and the risk to data subjects' rights and freedoms resulting from a data processing activity are appropriate and proportionate, based on the following premise: when the risk to data subjects increases, high implementation costs are more likely to be deemed reasonable.⁶⁸⁷ Due to the inherent high risk, data controllers will generally face significant implementation costs when processing special categories of personal data under Article 9 GDPR and personal data relating to criminal convictions and offences under Article 10 GDPR. Furthermore, the EDPB states that 'the state of the art

⁶⁸⁴ Moreover, when implementing the appropriate technical and organisational measures, the 'state of the art' (a term that is not defined in the GDPR), 'and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing', must be considered in tandem with the factor 'cost of implementation'.

⁶⁸⁵ For a high-level discussion of GDPR as a potential (financial) risk for organisations, please see 'The GDPR as a Risk for the Annual Financial Statements | Friedrich Graf von Westphalen' <<https://www.fgvw.de/en/news/archive-2018/the-gdpr-as-a-risk-for-the-annual-financial-statements>>. 'If the auditor notes that the requirements of data protection law are not met in the company, this may result in provisions having to be formed with regard to the costs of implementation and possible fines.'

⁶⁸⁶ Annika Selzer, 'The Appropriateness of Technical and Organisational Measures under Article 32 GDPR Reports: Practitioners' Corner' (2021) 7 European Data Protection Law Review (EDPL) 120.

⁶⁸⁷ Ronald Leenes and others, *Data Protection and Privacy: The Age of Intelligent Machines*, vol 10 (Hart Publishing Ltd 2017) <<https://go.exlibris.link/23sBBF6K>>.

may also be of significance when considering the cost of implementation,⁶⁸⁸ implying that these two factors should always be considered in direct relation to one another. As a result, businesses are expected to devote more time and money to privacy and data protection compliance,⁶⁸⁹ to hire privacy and data protection specialists,⁶⁹⁰ and to pool organisational and technological resources to update their systems and processes to the Regulation's security and functionality standards.⁶⁹¹

Hence, the cost of evaluating the adequacy of TOMs may fluctuate depending on various factors, including the size of the organisation, the intricacy of its data processing activities, and the quantity of measures that must be implemented. The following bar chart illustrates the supplementary expenditure that companies in the European Union and the United States are willing to or have already incurred to achieve GDPR compliance. As per 2018 statistics, the average company is expected to expend \$3 million USD due to GDPR.

⁶⁸⁸ European Data Protection Board (EDPB) (n 206).

⁶⁸⁹ Seo and others (n 87).

⁶⁹⁰ See Eric Lachaud, 'Should the DPO Be Certified?' (2014) 4 *International Data Privacy Law* 189.

⁶⁹¹ See 'Netsparker GDPR Survey: 10 Percent of C-Level Security Execs Say GDPR Will Cost Them \$1M+' *Journal of Engineering* (23 April 2018) 839.

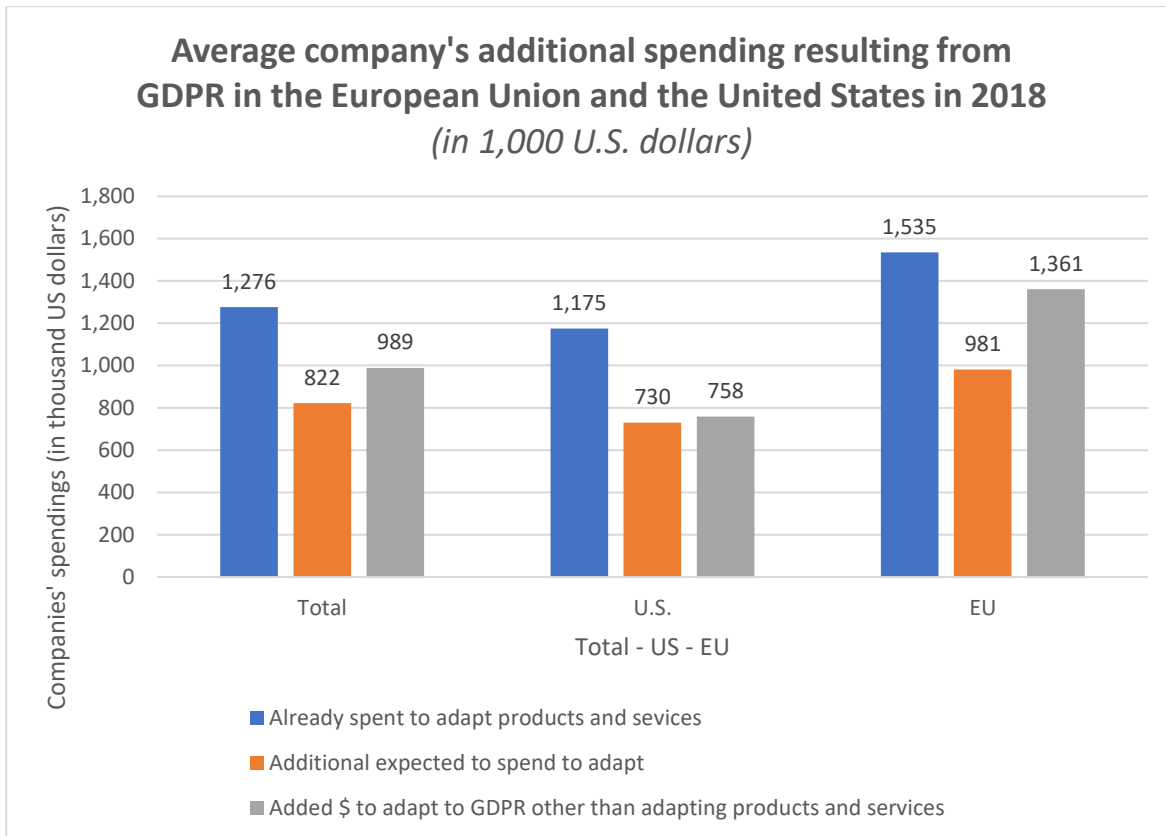


Figure 17 - EY, & IAPP. (May 25, 2018). Average company's additional spending resulting from GDPR in the European Union and the United States in 2018 (in 1,000 U.S. dollars) [adapted]. In Statista. <<https://www.statista.com/statistics/1008320/average-firm-additional-spending-resulting-from-gdpr-in-eu-and-us/>>.

One of the most noticeable implications of the "cost of implementation" aspect in PbDD is that compliance with GDPR requirements can necessitate either a complete overhaul of the organisation's systems and long-standing processes or the costly implementation of additional compliance measures.⁶⁹² These (sometimes very expensive) changes in procedure are particularly drastic in complying with the obligation to keep internal records of data protection activities – data mapping⁶⁹³ (accountability), with the obligation to

⁶⁹² Natalia Daško, 'General Data Protection Regulation (GDPR) – Revolution Coming to European Data Protection Laws in 2018. What's New for Ordinary Citizens?' (2018) 23 Comparative Law Review 123.

⁶⁹³ For a discussion of data mapping requirements (for processing in the area of biomedical research) and the efforts to develop particular tools (technical measures) for compliance with GDPR, see, Regina Becker and others, 'DAISY: A Data Information System for Accountability under the General Data Protection Regulation' (2019) 8 Gigascience <<https://go.exlibris.link/1NfSHBDc>>.

appoint a Data Protection Officer⁶⁹⁴ (only required for some organisations), or, with the obligation to implement appropriate organisational and technical measures to comply, inter alia, with the right to erasure,⁶⁹⁵ to minimise the risk of personal data breaches (cybersecurity strategies and systems),⁶⁹⁶ as well as to uphold the principles governing the processing of personal data (as described in Article 5 of the Regulation).

To evaluate the appropriateness⁶⁹⁷ of TOMs in compliance with both Articles 25 and 32 of the GDPR, the following selection factors should be taken into account: (i) State of the art: Are the measures based on established knowledge? Are innovative technological developments and practical measures suitable? Are the measures already fully developed and ready for technical implementation? (ii) Cost of implementation: What are the initial and ongoing costs of implementing state-of-the-art measures? Is the controller's primary business model based on the processing of personal data? (iii) Nature, scope, context, and purposes of processing: What type of data processing is being conducted? Are special categories of personal data processed? How many individuals' personal data are being processed? Is data processing taking place outside the EU? What are the processing objectives? (iv) Risks to the rights and freedoms of natural persons: Is there a possibility that data processing may result in physical, material, or non-material damage to data subjects? Could data processing lead to discrimination, identity theft, or harm to the data subject's reputation? What is the likelihood of such incidents? (v) Processing risks: Is there

⁶⁹⁴ For a discussion of the DPO role requirements under GDPR, see, Lachaud (n 682).

⁶⁹⁵ See, Timo Jakobi and others, 'The Role of IS in the Conflicting Interests Regarding GDPR' (2020) 62 *Business & Information Systems Engineering* 261.

⁶⁹⁶ See, Jesper Zerlang, 'GDPR: A Milestone in Convergence for Cyber-Security and Compliance' (2017) 2017 *Network Security* 8.

⁶⁹⁷ For a discussion of the GDPR concept of "appropriateness" through the lenses of a risk-based approach, see, Selzer, Woods and Bohme (n 636).

a possibility of accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access to personal data during data processing?

I believe that, by including the cost of implementation as a factor to consider, the GDPR seeks to strike a balance between protecting individuals' data privacy rights and ensuring that organisations are not overburdened by the cost of implementing PbDD. It is challenging to determine conclusively whether the regulators share the same perspective. Although the inclusion of the implementation cost as a consideration in the GDPR indicates that the regulator acknowledges the necessity of balancing these interests, the enforcement actions taken by the supervisory authorities may reflect different priorities. For instance, a regulator may prioritise safeguarding individuals' data protection rights over the cost of implementing PbDD, resulting in stricter enforcement measures and higher fines for non-compliance. On the other hand, a regulator may prioritise supporting businesses in implementing PbDD, resulting in a more lenient approach to enforcement and lower fines. Therefore, it is important to approach this question with caution and consider all the factors that could be affecting their enforcement actions.

The following chart reveals that, in 2020, nearly all German companies that initiated GDPR compliance undertakings encountered difficulties regarding their information obligations, such as informing individuals about how their data is being processed.⁶⁹⁸

⁶⁹⁸ One of the main objectives of GDPR is to ensure that individuals are aware of and comfortable with how their personal information is being used, therefore, transparency and informing the individuals about how their data are being used are two crucial factors of compliance. According to the GDPR, organisations must provide people with information that is: (a) In a concise, transparent, intelligible, and easily accessible form; (b) Written in clear and plain language, particularly for any information addressed specifically to a child; (c) Delivered in a timely manner; and (c) Provided free of charge. The GDPR's Articles 12, 13, and 14 provide helpful guidance, for instance, on how to produce a privacy notice, with an emphasis on making it understandable and accessible.

Similarly, forty-four percent of organisations required a significant amount of effort in terms of resources to meet PbDD requirements.⁶⁹⁹

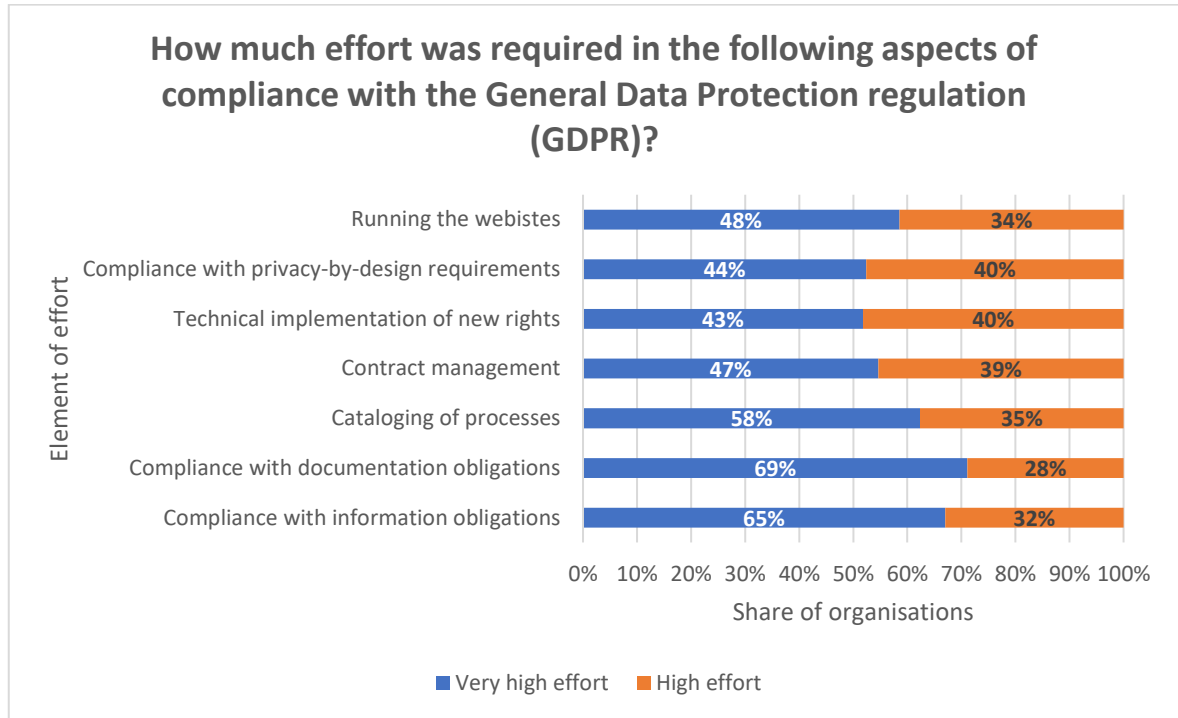


Figure 18 - Bitkom. (September 17, 2019). How much effort was required in the following aspects of compliance with the General Data Protection Regulation (GDPR)? [adapted]. In Statista. <<https://www.statista.com/statistics/1175341/gdpr-compliance-procedures-germany/>>.

The right to access has become synonymous with defending individuals' data privacy rights against abuse by organisations. However, there is no denying that responding to requests within the required thirty days costs businesses a significant amount of time and money.⁷⁰⁰ Many organisations claim that the sheer complexity of some requests, combined with a

⁶⁹⁹ By making the most privacy-friendly option the default, individuals whose data is being collected will have more control over how that data is used by organisations. This means that organisations must have access to the resources needed to develop any new product, system, or procedure that collects and processes the personal (and sensitive) information of data subjects in accordance with GDPR's PbDD requirements.

⁷⁰⁰ PrivSec Report26 May 2020, 'What Is the True Cost of Handling DSARs?' (*GRC World Forums*) <<https://www.grcworldforums.com/data-protection-and-privacy/what-is-the-true-cost-of-handling-dsars/58.article>>.

lack of adequate technology, necessitates a deadline extension, implying a resource increase. Given that some organisations may receive up to five hundred inquiries each month, the cost of responding to them is substantial. Previous research shows⁷⁰¹ that businesses in the UK spend an average of £1.59 million and 14 person years processing data subjects' requests each year. A significant portion of this cost stems from the requirement to manually gather, collate, and redact information. In a simple yet illuminating practical illustration, whenever an individual exercises their right to be forgotten, the organisation must initiate a new process that includes searching for the personal data across the organisation's data sets, analysing these data, deciding on what action to take with the data (such as erasure or anonymisation), and notifying the data subject the erasure of data, or, providing a justification as to why the data could not be erased. These operational tasks will always involve time-consuming procedures that must be completed within a specific timeframe, resulting in additional costs based on the amount of data held by an organisation and, as a result, increased transactional costs.⁷⁰² UK companies also incurred substantial expenses in responding to access requests from data subjects. A survey conducted among privacy experts in 2020 revealed that forty-one percent of them estimated the cost of a DSAR to range from three to six thousand British Pounds:

⁷⁰¹ See, for example, Guardum, 'UK Businesses Expend £1.59 Million and 14 Person Years Annually Processing DSARs Finds New Survey amongst DPOs' (May 2020) 59 <<https://www.globalsecuritymag.com/UK-businesses-expend-L1-59-Million,20200518,98707.html>>.

⁷⁰² For a discussion of the impact of GDPR on the level of transactional costs in the management of medical data in medical organisations, see, e.g., Wojciech Krówczyński and Faculty of Management and Social Communication at Jagiellonian University in Krakow, 'The Influence Of The Regulation Of European Parliament And Council Of The European Union (GDPR) On The Level Of Transactional Costs Of Managing Medical Data In Medical Entities' (2018) 91 *Optimum studia ekonomiczne* 80.

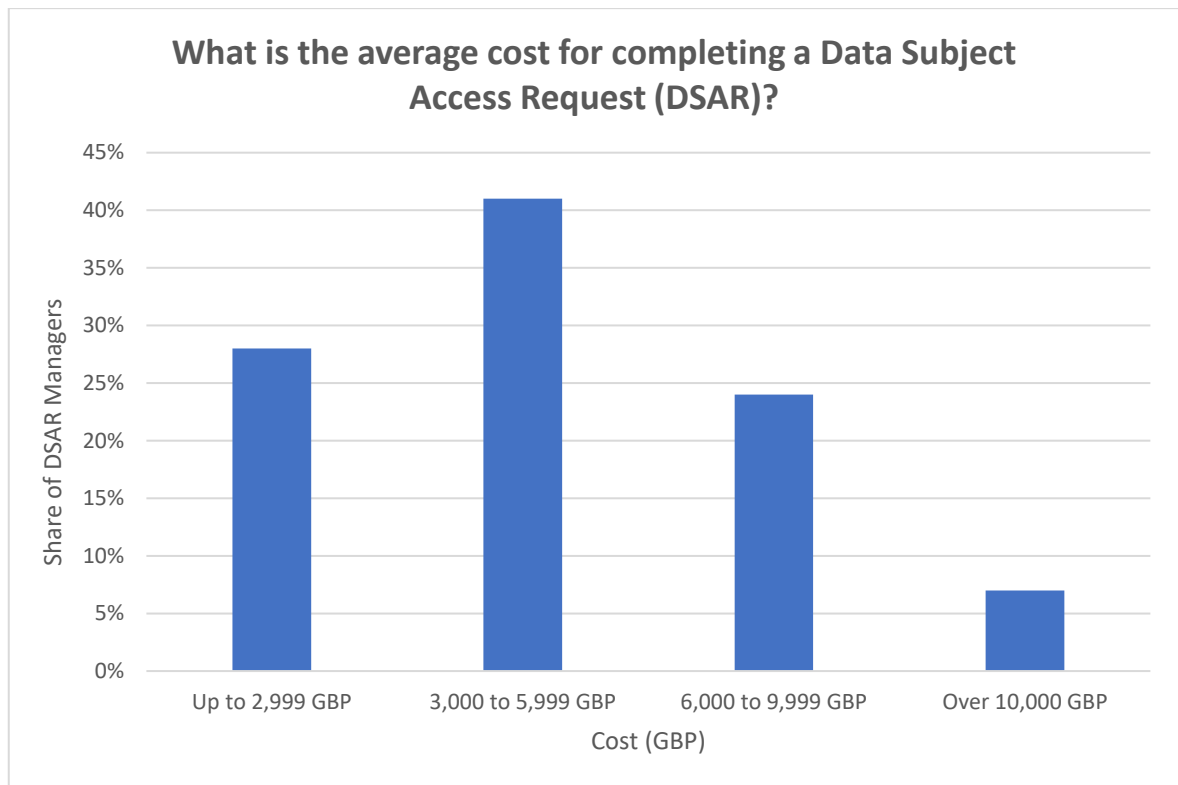


Figure 19 - Guardum. (May 1, 2020). What is the average cost for completing a Data Subject Access Request (DSAR)? [adapted]. In Statista. < <https://www.statista.com/statistics/1177135/average-cost-of-a-data-subject-access-request-uk/>>.

The cost of implementation is a factor that organisations must consider under GDPR in a variety of situations,⁷⁰³ including when implementing PbDD (for example, in the context of implementation of the security measures to ensure the integrity and confidentiality of personal data).⁷⁰⁴ It is noteworthy that by implementing an appropriate PbDD plan, organisations can derive benefits from complying with GDPR. For instance, they can streamline data management by eliminating redundant data,⁷⁰⁵ resulting in significant

⁷⁰³ For a summary of the impact of GDPR implementation costs on organisations in 2022, see, Luke Irwin, 'How Much Does GDPR Compliance Cost in 2022?' (*IT Governance Blog En*, 26 April 2022) <<https://www.itgovernance.eu/blog/en/how-much-does-gdpr-compliance-cost-in-2020>>.

⁷⁰⁴ As required by Article 32 GDPR.

⁷⁰⁵ Rob Perry, 'GDPR – Project or Permanent Reality?' (2019) 2019 *Computer Fraud & Security* 9.

lower data storage and data maintenance costs.⁷⁰⁶ Moreover, the EC estimates a cost reduction for businesses of up to €2.3 billion per year if GDPR is properly implemented.⁷⁰⁷ In the event that organisations take the PbDD "implementation cost" as a business "investment" in privacy and data protection, further benefits may be realised. In this regard, Buckley et. Al. states, that:

‘GDPR has gifted companies a reason to justify investment in modernising their data management processes and security. Companies have cleaner and more up-to-date customer databases. In the absence of GDPR, companies admit they would ask for more information than necessary, use it more frequently, hold it for longer and keep it less securely.’⁷⁰⁸

Despite the potential benefits, it is a fact that complying with GDPR will invariably entail substantial financial costs for organisations, contingent on the quantity of personal data they process and the intricacy of their business activities, rendering compliance with the Regulation excessively expensive for numerous SMEs.

Since 2018, small businesses have committed a significant share of their financial resources to implementing GDPR. In 2019, 6 percent of the surveyed European companies reported spending between 100,000 and 499,000 euros to comply with GDPR:

⁷⁰⁶ Phil Beckett, ‘GDPR Compliance: Your Tech Department’s next Big Opportunity’ (2017) 2017 Computer Fraud & Security 9.

⁷⁰⁷ Ralph O’Brien, ‘Privacy and Security: The New European Data Protection Regulation and It’s Data Breach Notification Requirements’ (2016) 33 Business Information Review 81. ‘The EU hopes that not only will the new legislation improve consumer confidence in the businesses that hold and process their data, it will also reduce costs for businesses that at present have to comply with differing laws in the countries they have operations, customers, and suppliers in. The Commission estimates business a saving of up to €2.3 billion a year.’

⁷⁰⁸ Gerard Buckley, Tristan Caulfield and Ingolf Becker, “It May Be a Pain in the Backside but.” Insights into the Impact of GDPR on Business after Three Years’ <<https://go.exlibris.link/ry3tTcKk>>.

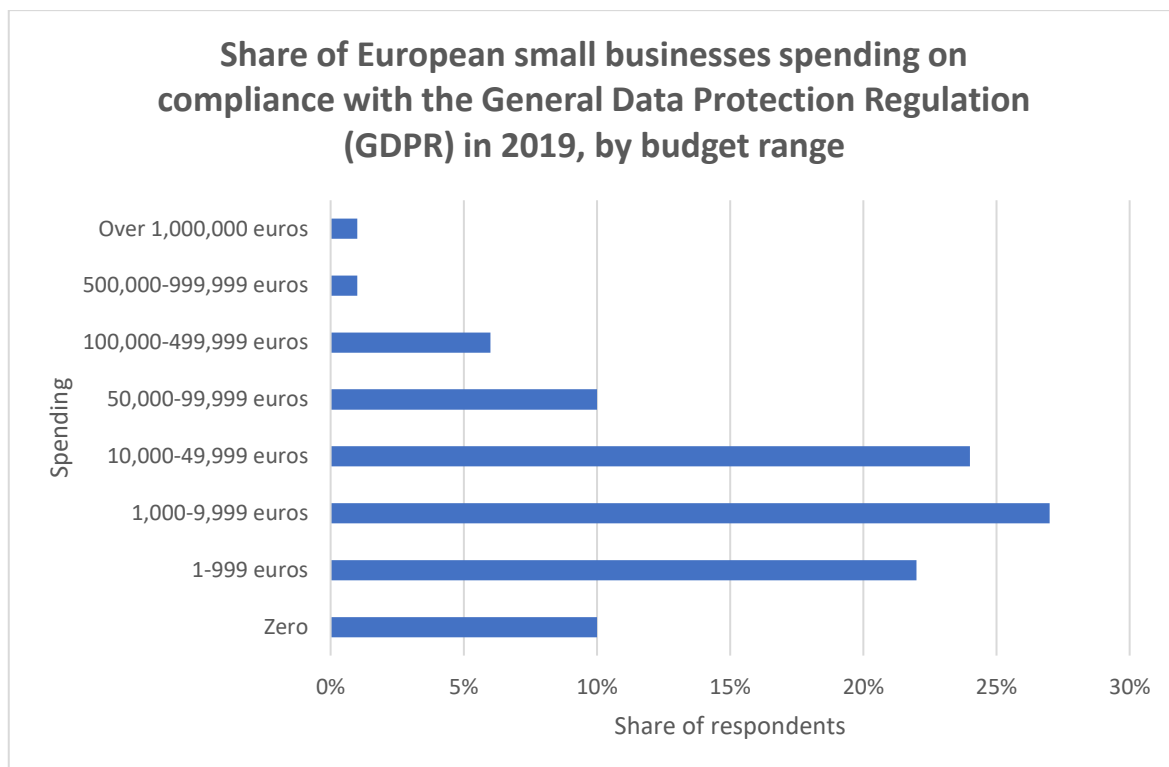


Figure 20 - European Commission (gdpr.eu). (May 20, 2019). Share of European small businesses spending on compliance with the General Data Protection Regulation (GDPR) in 2019, by budget range [adapted]. In Statista. <<https://www.statista.com/statistics/1176050/gdpr-compliance-spending-in-small-businesses-europe/>>.

According to Article 25(1) GDPR, cost of implementation could be interpreted in such a way that economic considerations are limited to the one-off, initial implementation costs of the respective TOMs. So far, it has not been determined whether the term should be interpreted broadly, with some arguing that "cost of implementation" includes the costs of operation, maintenance, and other subsequent follow-up and recurring costs that are directly related to the implementation of a technical and organisational measure - the broad definition of implementation costs in this context is justified by the fact that recurring costs to maintain TOMs can be significantly higher than initial one-time costs. If these costs are not taken into account when selecting the TOMs, a long-term effort may be too high, even if the risk to the rights and freedoms of the data subjects is duly taken

into account. Others, on the other hand, argue that follow-up and recurring costs should not be considered, stating that the GDPR's use of the phrase "cost of implementation" should be interpreted as clearly limited to the costs of initially integrating the measure into the corresponding processing system.⁷⁰⁹

However, the potential budget required to implement GDPR measures tends to multiply significantly with the size of organizations.⁷¹⁰ According to David Coolegem and Adrien Dauchot, the minimum and average implementation cost per employee is consistent across firm size, with implementation costing £300-£450 per employee on average across all sectors. However, as a company grows in size beyond 10,000 employees, the maximum costs seen by a single company decrease significantly,⁷¹¹ leading to the conclusion that the implementation costs of the GDPR may unjustifiably disadvantage small businesses. Furthermore, it is debatable whether the organisations' individual economic circumstances should be considered by the Regulation. Some argue that all in all the factor cost of implementation can only serve to limit the applicability of measures on a theoretical level, therefore, the organisations' concrete financial potential, including its solvency, is irrelevant. However, consideration of costs should protect all controllers and processors from being forced to implement a technical or organisational measure that only marginally reduces the risk to data subjects' rights and is financially ineffective for all of them.⁷¹²

⁷⁰⁹ Selzer, Woods and Bohme (n 636).

⁷¹⁰ I believe that organisations must balance the cost of implementing TOMs with the risks involved in data processing to ensure that they are not overburdened financially. I interpret the GDPR as recognising that some measures may be too costly or impractical for certain organisations and providing flexibility in implementing these measures. However, organisations must still ensure that they have taken appropriate steps to mitigate risks to data subjects' rights and freedoms.

⁷¹¹ Consultancy.uk, 'GDPR Compliance to Cost FTSE100 Firms £15 Million, Banks Face Largest Bill' (News, 21 December 2017) <<https://www.consultancy.uk/news/15101/gdpr-compliance-to-cost-ftse100-firms-15-million-banks-face-largest-bill>>.

⁷¹² Selzer, Woods and Bohme (n 636).

Six months after the GDPR came into effect, many organisations found that the costs of implementing the GDPR were higher than expected. According to a Verasec survey, forty-one percent of respondents said their companies are paying more than expected to comply with Regulations.⁷¹³

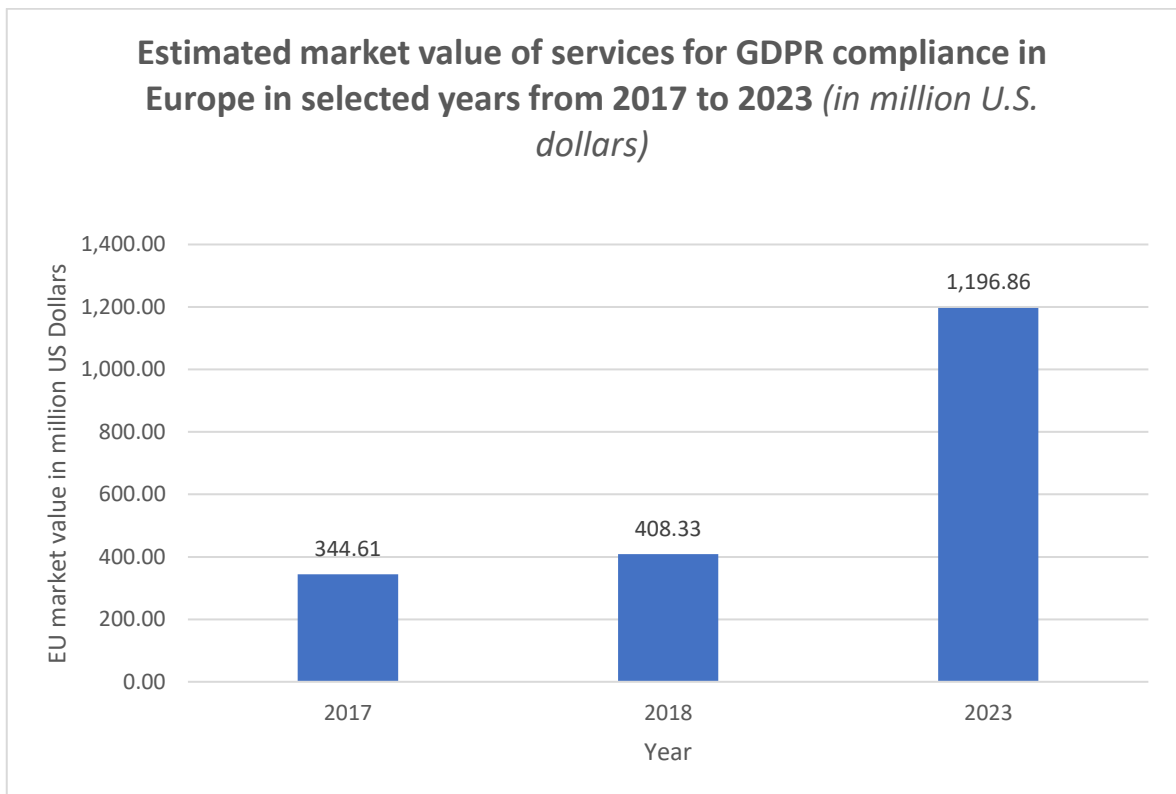


Figure 21 - Statista. (May 8, 2019). Estimated market value of services for GDPR compliance in Europe in selected years from 2017 to 2023 [adapted]. In Statista. <<https://www.statista.com/statistics/1005111/estimated-value-of-gdpr-services-market-in-europe/>>

Figure 22 displays the estimated market value of services for GDPR compliance in the European Union from 2017 to 2018, with a projection for 2023. It is noteworthy that by 2023, the market value of businesses providing services for GDPR compliance is expected to reach 1.1 billion euros, underscoring the economic significance of GDPR compliance services in the EU market. This highlights the other side of the coin, which is the economic

⁷¹³ Anonymous (n 669).

benefits of GDPR in addition to the costs incurred by organisations to comply with the Regulation.

In response to the inquiry regarding the cost of GDPR compliance in 2021, Luke Irwin states that many organisations are still in the process of implementing GDPR requirements, making it premature to estimate the cost of maintaining compliance. However, based on a PwC report, it is expected that GDPR compliance will cost more than \$1 million. In some cases, the cost could be considerably higher; the same report revealed that 13% of respondents were willing to invest over \$10 million in compliance.⁷¹⁴

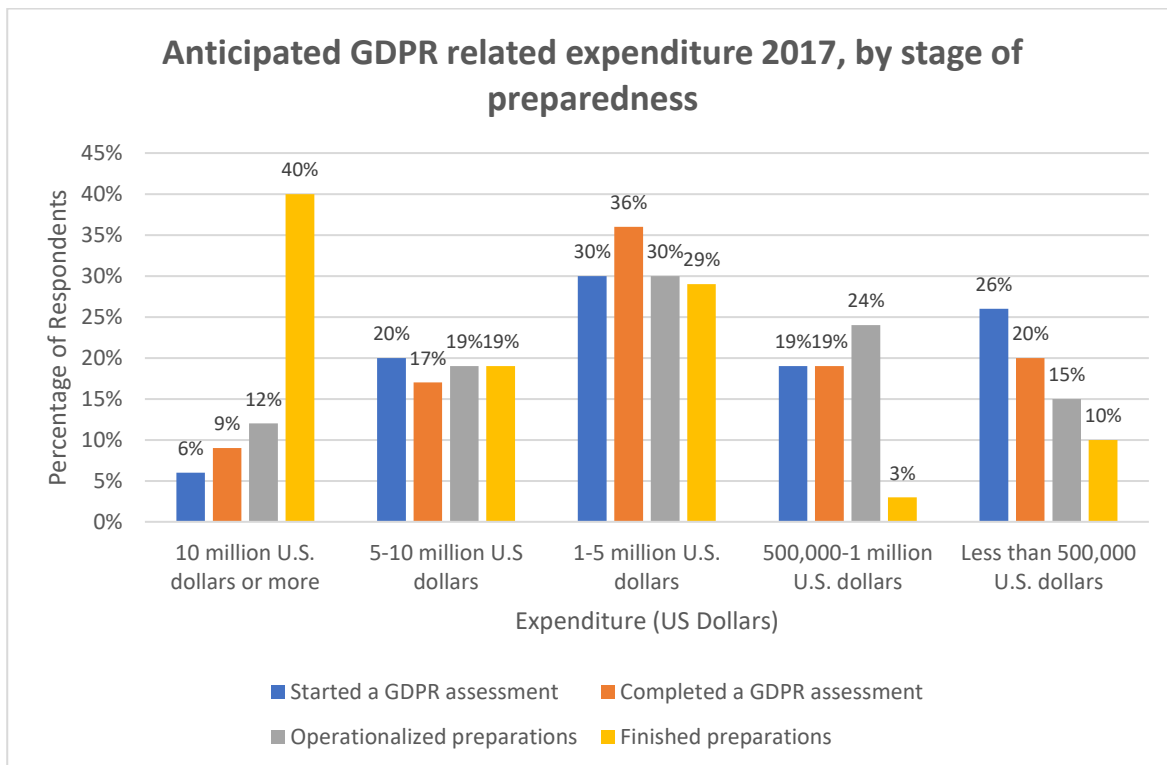


Figure 22 - PwC. (September 13, 2017). Anticipated GDPR related expenditure 2017, by stage of preparedness [adapted]. In Statista. <<https://www.statista.com/statistics/945975/anticipated-gdpr-expenditure/>>.

⁷¹⁴ Luke Irwin, 'How Much Does GDPR Compliance Cost in 2021?' (IT Governance 2021) <<https://www.itgovernance.eu/blog/en/how-much-does-gdpr-compliance-cost-in-2020>>. When it comes to the cost of GDPR compliance, eighty-eight percent of organisations spend more than \$1 million and forty percent spend more than \$10 million, according to the study.

The chart presented in Figure 23 outlines the expected level of GDPR-related spend for companies with a European presence.⁷¹⁵ Eighty-eight percent of those who have completed GDPR preparations expect to spend more than \$1 million on GDPR-related expenses.

Figure 24 illustrates the estimated GDPR implementation costs for FTSE100 companies in the United Kingdom in 2018, broken down by sector. Organisations in the banking sector would face the highest average implementation costs, estimated at sixty-six million British Pounds.

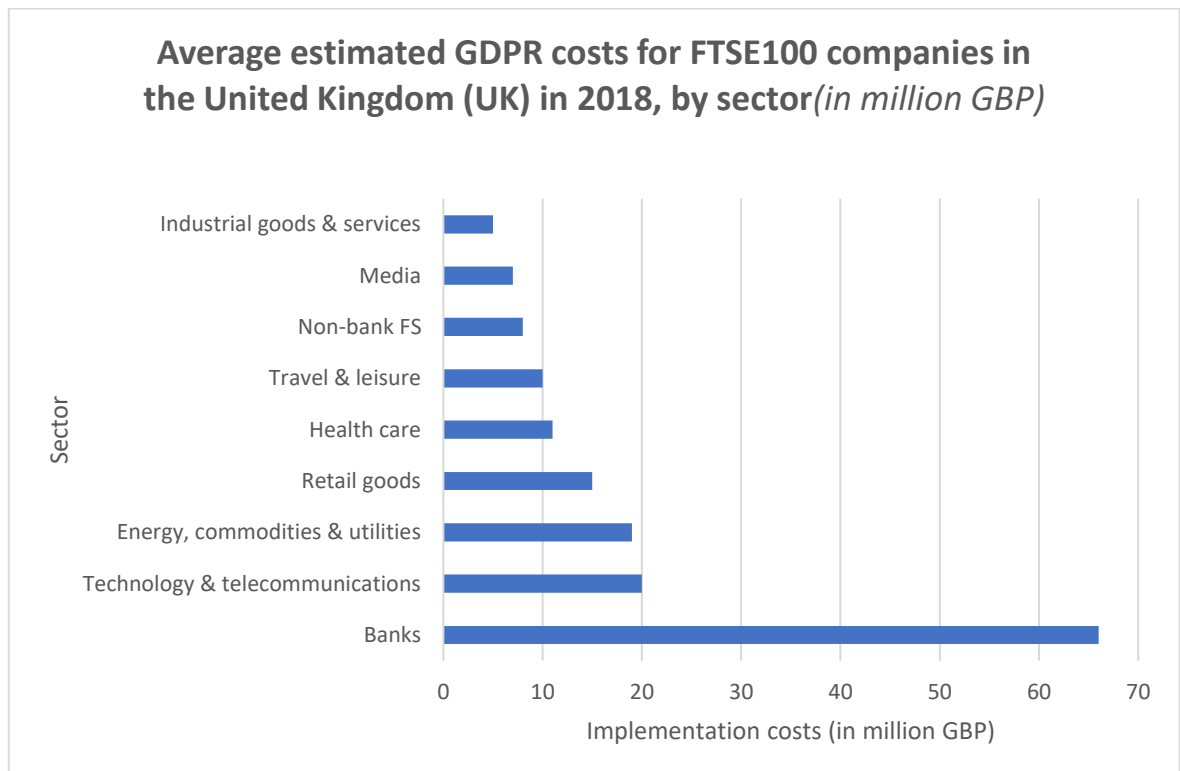


Figure 23 - Sia Partners. (May 1, 2018). Average estimated GDPR costs for FTSE100 companies in the United Kingdom (UK) in 2018, by sector (in million GBP) [adapted]. In Statista. <<https://www.statista.com/statistics/869613/gdpr-implementation-cost-by-sector/>>.

⁷¹⁵ Statistics pre-GDPR (2017).

In accordance with Sia Partners, UK banks have an average GDPR implementation⁷¹⁶ cost of £66 million, the highest of any sector. Non-bank financial services firms have lower costs on average (£8 million), but their implementation cost per employee is unusually high (£719 versus £553 for banks or £271 for the retail sector), which can be attributed to the advanced technological implementation of PbDD needed to ensure the security of online access to banking data. It is important to note that certain costs, such as the need to maintain an up-to-date level of online data security and demonstrate compliance, are expected to persist over the long term.

Another aspect that is inextricably linked to the high implementation costs of PbDD measures concerns data security, prevention and notification of data loss or data breaches. The GDPR introduced the requirement for data breach notification and changes in controller's liability that have a profound impact on the businesses. Not all data breaches must be reported to the supervisory authorities; only those where the individual is likely to suffer some form of harm, such as identity theft or a breach of confidentiality. In addition, where the breach puts individuals' data at risk, data subjects must also be informed. The notifiable data breach must be reported to the supervisory authority as soon as possible, but no later than 72 hours after the data controller becomes aware of it.

These changes underscore the growing importance of integrating business data security into the organisation's PbDD programme. To ensure that all systems are fit for purpose under the new GDPR security regime,⁷¹⁷ regular organisational reviews and audits will be required. The GDPR expressly states that improved data breach investigation,

⁷¹⁶ When GDPR implementation is referred to, all associated costs are captured, including those associated with the implementation of a PbDD program or technical and organisational PbDD measures.

⁷¹⁷ As per the provisions of Article 32 GDPR, security is deeply rooted in the implementation of PbDD.

categorisation, containment, and response infrastructure are required. The PbDD programme must therefore ensure that the appropriate measures are in place to detect, report and investigate a personal data breach. This could include assessing and documenting the types of data stored, which would have to be reported in the event of a breach. Policies and procedures for dealing with data breaches must also be in place. When it comes to data loss and data breaches, in addition to the financial risk for organisations, there is also a reputational risk to consider.

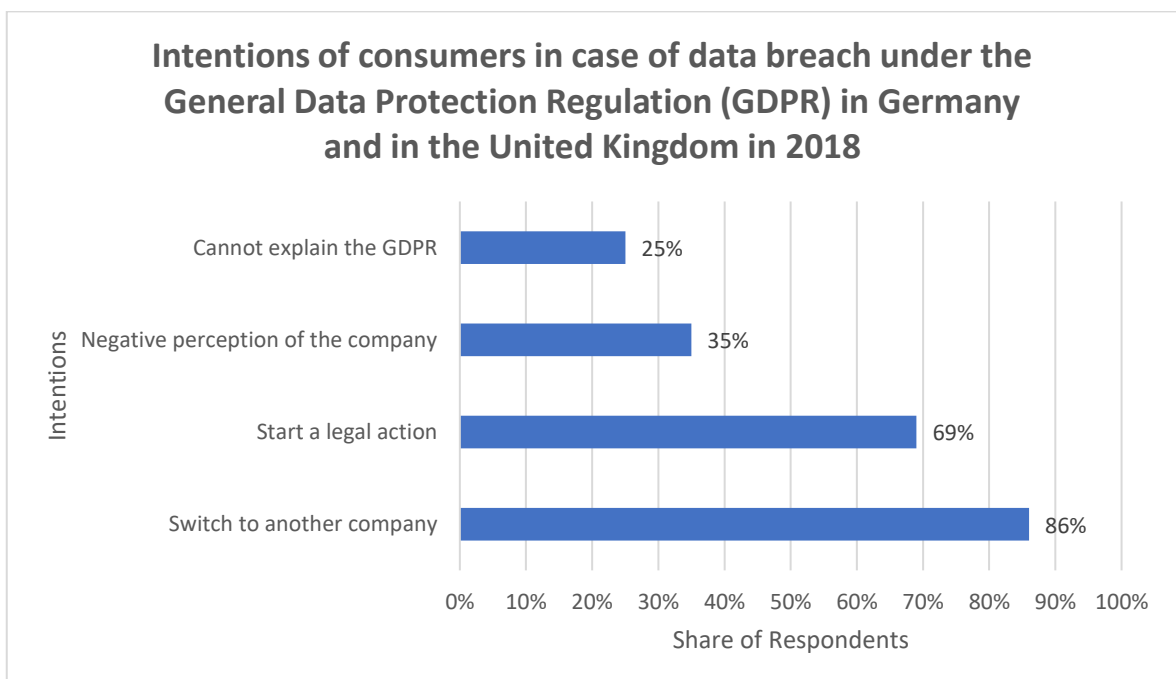


Figure 24 - Thales Group. (November 26, 2018). Intentions of consumers in case of data breach under the General Data Protection Regulation (GDPR) in Germany and in the United Kingdom in 2018 [adapted]. In Statista. <<https://www.statista.com/statistics/1004907/consumers-intentions-in-case-of-data-breach-in-germany-and-uk/>>.

Figure 25 illustrates the results of a 2018 survey on consumer purchase intentions in the event of a GDPR data breach in Germany and the UK; eighty-six percent of respondents said they would switch companies if there was a data breach. The second largest group

(sixty-nine percent) agreed that they could take legal action⁷¹⁸ against a company that does not handle their personal data in accordance with the GDPR.

According to the IBM's annual report,⁷¹⁹ the global shift to remote work as a result of the COVID-19 pandemic has also impacted organisations and their ability to respond to data breaches. The final total of \$4.24 million expenditure per incident in 2021 is the highest since the report began fourteen years ago, according to the IBM-sponsored Ponemon Institute. The figure is a ten percent increase over previous year's total, averaging \$3.86 million expenditure per incident. The report examined 537 breaches from May 2020 to March 2021 and discovered that those organisations who acknowledged that remote work was a factor in their breach, suffered a higher loss - \$4.96 million - than those who did not - \$3.89 million – resulting in a fifteen percent difference.

Ransomware breaches were the costliest of all breach types. On average, these types of attacks cost organisations between \$4.62 million and \$4.69 million, with much of the cost likely due to downtime, lost business, and the cost of rebuilding systems from backups when not even from scratch.

Although the chart presented in Figure 26 represents the average cost of a data breach in organisations worldwide based solely on their security automation level at the time of a data breach, it does not provide a direct correlation to GDPR enforcement actions. However, it can help us understand the importance of deploying appropriate security measures in the context of a PbDD programme, as required by Article 32 of the GDPR.

⁷¹⁸ For a discussion of data protection-related class actions, please see 'The "Tidal Wave" of Data Protection-Related Class Actions: Why We're Not Drowning Just Yet...'
<<https://www.twobirds.com/en/insights/2018/global/tidal-wave-of-data-protection-related-cases>>.

⁷¹⁹ Ponemon Institute, 'How Much Does a Data Breach Cost?' (2021) <<https://www.ibm.com/security/data-breach>>.

The chart highlights that those organisations with higher levels of security automation experience lower average costs of data breaches compared to those with lower levels. This suggests that investing in appropriate security measures can help mitigate the risks associated with data breaches and reduce the potential costs of non-compliance with the GDPR.

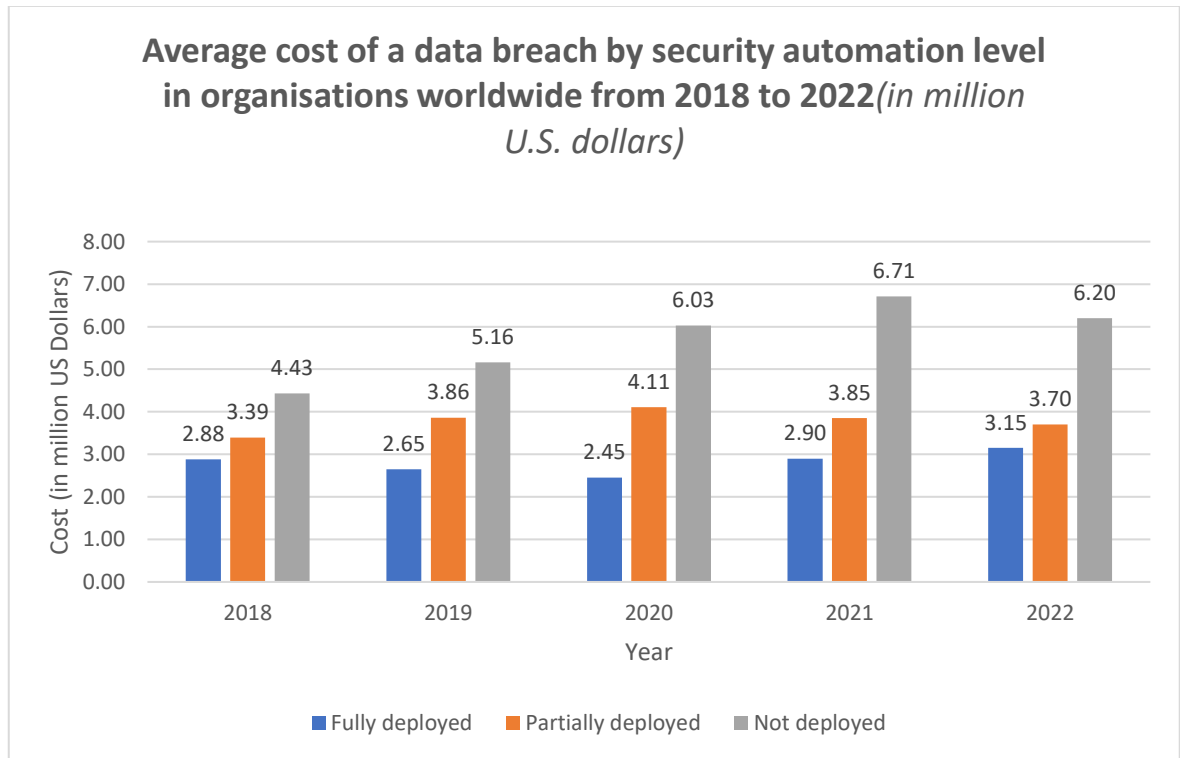


Figure 25 - IBM, & DataEndure. (July 28, 2021). Average cost of a data breach by security automation level in organisations worldwide from 2018 to 2022 [adapted]. In Statista. <<https://www.statista.com/statistics/1176688/data-breach-cost-security-automation-level/>>.

In the context of the GDPR, Figure 27 demonstrates that the average cost of cybersecurity breaches for businesses operating in the UK over the past year stood at £1,200 as of 2022. Notably, this figure tends to increase commensurate with a business's size. The costs incurred because of a cyber-attack, however, extend beyond just monetary considerations and encompass intangible costs, such as the time and resources necessary to recover from the attack. For instance, apart from the financial burden of the attack, a company must allocate significant resources to restoring its systems and data to forestall future security

breaches. Furthermore, a cyber-attack can inflict lasting damage on a company's reputation, thereby jeopardizing its customer base, clients, and investors.

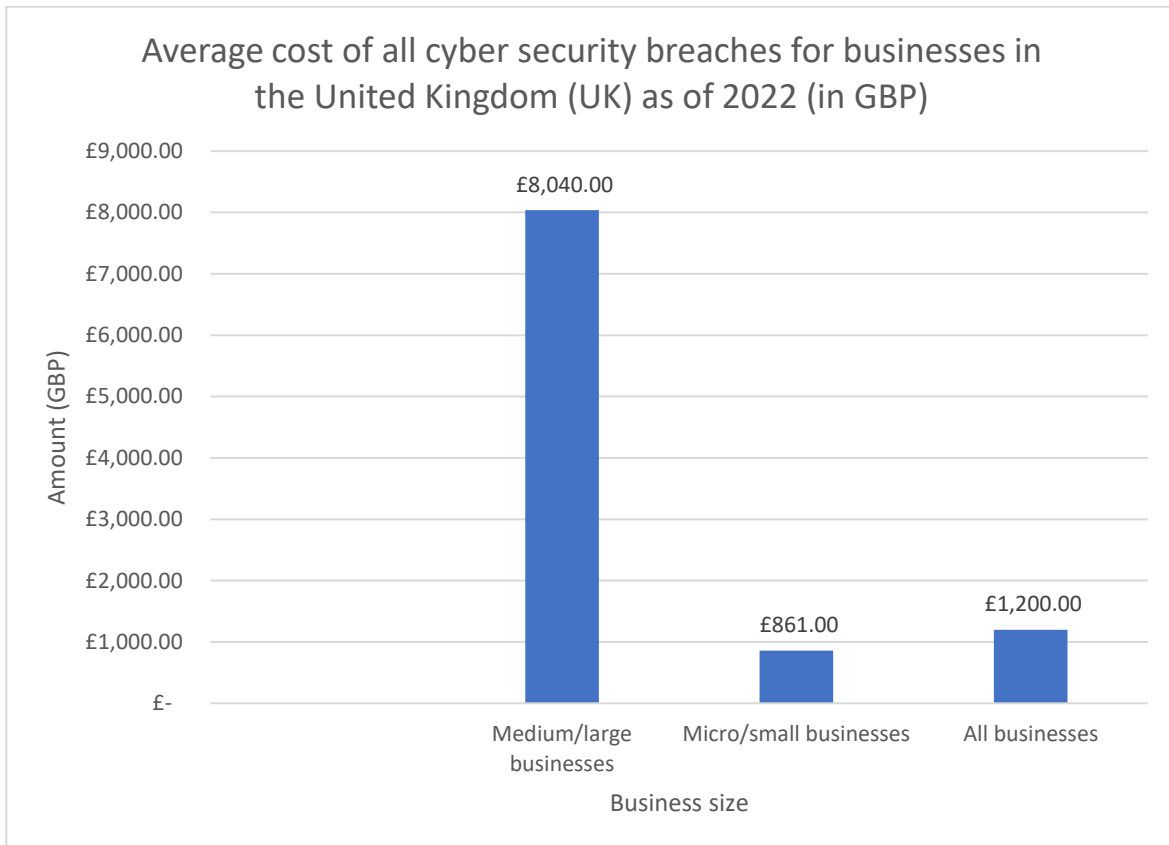


Figure 26 - GOV.UK. (March 30, 2022). Average cost of all cyber security breaches for businesses in the United Kingdom (UK) as of 2022 (in GBP) [Graph]. In Statista. <<https://www.statista.com/statistics/586788/average-cost-of-cyber-security-breaches-for-united-kingdom-uk-businesses/>>.

In conclusion, it is essential to highlight that the current PbDD framework, characterised by a uniform set of requirements, can disproportionately impact small and medium-sized businesses. The absence of provisions for the granularity of applicable TOMs in Articles 25 and 32 of the GDPR can make the cost of implementation unfeasible, particularly for non-profit organisations dedicated to social and humanitarian causes, hindering their ability to achieve their objectives.

7.4. Concluding remarks

Chapter seven has shed additional light on the considerable challenges arising from the lack of clarity and guidance within the GDPR. The examination of these challenges has underscored the complexities faced by organisations striving to conform to GDPR principles. We found that the regulatory ambiguities, pose significant hurdles in the practical application of PbDD, leading to uncertainties in implementation strategies.

Furthermore, the economic implications of GDPR implementation have been thoroughly explored. The chapter has delved into the potential costs associated with ensuring compliance. The substantial investments required for TOMs, staff training, and ongoing monitoring have been weighed against the long-term benefits of enhanced data protection, customer trust, and regulatory adherence.

As we transition to the next chapters, the focus will shift towards the more technical aspects of implementing PbDD. These chapters will delve into the practical application of specific pre-selected TOMs, which form the core of the DPPA. The DPPA, as a comprehensive roadmap derived from the findings of this study, provides a structured framework for the practical implementation of all aspects explored thus far.

By exploring the application of TOMs within the DPPA, I aim to offer practical insights into how organisations can navigate the challenges highlighted in the previous chapters. These technical chapters will provide a detailed examination of the selected measures, offering guidance on their integration. This transition marks a shift from theoretical considerations to a hands-on exploration of implementing PbDD principles in real-world scenarios, contributing to a more pragmatic understanding of effective data protection practices.

Chapter 8 – DPPA (Part I): Operations and implementation of data protection principles

Introductory notes

The quantity of information that individuals generate on a daily basis is unparalleled, and thus far, people have never shared such enormous volumes of their data, whether in return for services or otherwise. The EC recognised this challenge and in January 2012, announced its intention to reform data protection law in the European Union to align it with the digital age. This initiative culminated in the development of the General Data Protection Regulation (GDPR), which comprises 99 Articles and has global implications for organisations.

As we have seen in preceding Chapters, ensuring GDPR compliance is neither a simple nor an easy undertaking. Against a backdrop of global transfers of personal data, threats to the privacy of individuals and increasingly intrusive technologies, the GDPR must ensure that the personal data of individuals in the EU are robustly protected, regardless of where their data is being processed. Although the GDPR strengthens the legal framework that protects individuals' privacy and personal data in the EU, it has become evident that complying with its requirements can be incredibly challenging, or even unfeasible, in practice. Specifically, integrating the fundamental legal obligation of PbDD into technology and modern business processes can pose insurmountable difficulties for some organisations. The GDPR also requires organisations to demonstrate compliance with the Regulation's principles and obligations. According to Article 24 of the GDPR, an organisation's compliance with the Regulation can be demonstrated, *inter alia*, by the

implementation of appropriate TOMs,⁷²⁰ adoption of data protection policies and implementation of PbDD.⁷²¹ Several Articles of the GDPR explicitly demand proof of implementing TOMs to demonstrate compliance, while it is implied in others.

The DPPA provides a practical means for organisations to navigate the challenges of implementing GDPR and maintain compliance. Despite the frictions and technological discrepancies that underpin the DPPA, as discussed in Chapters four, five, and six, it establishes that, in most cases, achieving ongoing conformity with GDPR is feasible by utilising the following framework and maintaining a detailed log of relevant data protection actions.⁷²² The DPPA gives priority to the GDPR requirement that organisations processing personal data of citizens in the EU must do so,

‘[I]n a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).’⁷²³

⁷²⁰ See Recital 74 of the GDPR. ‘The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller’s behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.’

⁷²¹ See Recital 78 of the GDPR. ‘In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default.’

⁷²² Due to the limitations outlined in this work it is impossible to comply with the GDPR in its entirety. The DPPA becomes instrumental in tackling PbDD implementation, significantly contributing to the identification of appropriate technical and organisational measures (beyond those provided by the law) and supporting organisations in identifying the non-compliant areas of personal data processing.

⁷²³ GDPR, Article 5(f).

The DPPA approach to data protection compliance (or data protection management) is anchored on PbDD,⁷²⁴ and therein lies its strength. The ICO defines data protection by design as 'an approach to projects that promotes privacy and data protection compliance from the start',⁷²⁵ and the GDPR expands its scope to include "by default,"⁷²⁶ as an assurance that all projects will take data minimisation and purpose limitation into consideration. The DPPA presents a new way of ensuring compliance with the GDPR that strikes a balance between the requirements of organisations, the data protection principles, and the protection of data subjects' rights and freedoms. While the GDPR mainly applies to processing carried out by controllers or processors within the EU, the DPPA acknowledges that, under certain circumstances and in accordance with public international law, it can also apply to controllers or processors outside of the EU. This makes the DPPA's application universal.

The objectives of the Data Protection Principles Approach (DPPA)

The DPPA framework aims to simplify the operational challenges posed by the complex EU data protection legislation and assist organisations in identifying and implementing appropriate TOMs to ensure data security, maintain trust with individuals and regulators, and achieve ongoing compliance.

The DPPA provides an easy, straightforward and extremely efficient mechanism to implement PbDD, therefore ensuring that the processing activities carried out by the

⁷²⁴ See Recital 78 of GDPR.

⁷²⁵ ICO, 'Data Protection by Design and Default' (n 55).

⁷²⁶ Data protection by default means that user service settings must be data protection friendly by default, and that only the data required for each specific processing purpose should be collected.

organisation are lawful, fair, and transparent for data subjects, in accordance with the GDPR.

My research on the difficulties encountered by numerous organisations in achieving GDPR compliance led to the creation of the DPPA, a tool for organisations to structure their data protection management efforts and effectively implement PbDD, thereby achieving compliance with the Regulation where it is possible to do so.⁷²⁷ The DPPA provides an adaptable "roadmap" for implementing GDPR. This framework is not intended to be viewed as a mere checklist that organisations must complete; rather, it proposes an approach to compliance based on the data protection principles and data subject's rights, by suggesting the implementation of mandatory, observable, and "trackable" TOMs. In essence, the DPPA provides a comprehensive list of data processing scenarios that require the implementation of TOMs to meet the PbDD requirement outlined in Article 25 of the GDPR. It is structured on an "Article-by-Article" basis, ensuring that all relevant provisions of the Regulation are addressed. Since no two organisations have identical PbDD requirements, this methodological approach provides the required flexibility for data controllers and processors planning their PbDD operational actions and is ideal for addressing the risk-based approach inherent to the GDPR from a more stringent perspective. Furthermore, based on the organisation's legal and regulatory compliance needs stemming from a specific personal data processing, appropriate TOMs can be designed and implemented.

This methodology is also intended to assist the DPO in developing an accountability approach to GDPR compliance as it provides a practical-oriented summary of each GDPR

⁷²⁷ This work has presented situations where compliance cannot be achieved due to several factors, including technology (as in the case of blockchain and IoT) which is deemed incompatible, or at least partially incompatible with the GDPR.

Article and maps it to the organisation’s compliance obligations. Another advantage of using this methodology is that it assists the DPO in implementing an audit trail response for GDPR compliance;⁷²⁸ it provides illustrative examples of procedures and mechanisms that can aid in selecting and implementing the required TOMs, as well as a list of examples of evidence demonstrating that the PbDD mechanisms have been correctly implemented and utilised.

The figure below indicates the scope of applicability of the DPPA in the operational theatre of GDPR:



Figure 27 – Scope of applicability of the DPPA

⁷²⁸ An audit trail is a record of all actions that are taken in relation to personal data, from its collection and processing to its deletion or retention. It is a critical tool for ensuring that personal data is processed lawfully and transparently, and for identifying and addressing any security breaches or incidents that may occur.

The DPPA methodology

By mapping and categorising the GDPR Articles that necessitate the implementation of TOMs, I created a simple operational implementation process. The classification is based on the Articles that require evidence of such measures to establish conformity with GDPR. As a result, specific operational circumstances are identified that require the implementation of measures, as well as the appropriate documentation to confirm the organisation's ongoing adherence to GDPR requirements.

In the event that an organisation fails to implement such measures, supervisory authorities are empowered to take action, which can include levying fines for a variety of GDPR violations, including insufficient data protection measures or data breaches.⁷²⁹ The regulator will consider a variety of factors when determining the amount of the fine, including the nature and severity of the violation, the organisation's compliance history, and other relevant factors. Numerous violations were registered between 2018 and 2023, including a record-breaking fine of EUR 743 million,⁷³⁰ which is the highest penalty ever imposed for a GDPR violation. The total amount of fines issued since May 2018 surpassed the milestone of EUR 1 billion in the summer of 2021.

The DPPA gap analysis

The DPPA gap analysis is a rigorous procedure that entails comparing an organisation's current state to an anticipated future state. It identifies the difference, or "gap," between

⁷²⁹ The amount of the fine is based on a tiered system, with the most severe infractions carrying a maximum penalty of €20 million or 4% of the organisation's global revenue, whichever is higher.

⁷³⁰ In its quarterly report, Amazon (US) announced that the Luxembourg Supervisory authority had fined Amazon Europe EUR 746,000,000 for failing to process personal data in compliance with the GDPR. <<https://www.sec.gov/ix?doc=/Archives/edgar/data/0001018724/000101872421000020/amzn-20210630.htm>>

the present and intended state, indicating areas that require improvement or further attention to reach the desired objectives. The initial gap analysis serves a dual purpose by allowing data controllers to evaluate the accuracy and appropriateness of their data usage while also ensuring that personal data is processed solely for its specified, explicit, and legitimate purposes (purpose limitation). This preliminary evaluation also involves determining whether the organisation processes only relevant and necessary personal data for the intended purposes (data minimisation). Furthermore, by providing an overview of the organisational data flows, the gap analysis enables the early identification of appropriate measures to maintain the accuracy of personal data and promptly rectify or erase any inaccurate information (data accuracy). Finally, the analysis helps controllers identify processes to address the requirement that personal data should not be retained for longer than necessary to fulfil its original purpose (storage limitation).

8.1. GDPR requirements must be met via operational PbDD actions

As per Article 24 of the GDPR, organisations are required to implement appropriate TOMs in their data processing systems to comply with the Regulation's provisions and ensure personal data is processed in accordance with the GDPR. Accordingly, this study maps the GDPR Articles that mandate action by the controller to a technical-legal framework (DPPA).

The DPPA not only facilitates the identification of appropriate measures in accordance with the current state of the art, but also enables organisations to demonstrate compliance with Article 5(2) of the GDPR by providing evidence that a specific measure has been applied to the processing activity or system processing the data. To ensure ease of use with the GDPR, the DPPA is structured into five sections, namely, Principles, Rights of

the Data Subject, Controller and Processor, Transfers of Personal Data, and Other Provisions. As a detailed examination of technological aspects is not within the scope of this study, the operational security measures outlined in the DPPA only provide general mechanisms to ensure appropriate data storage (i.e. users must keep personal and confidential data locked away; keep keys to secure filing systems secure; don't save data on laptops, tablets or flash drives; use of organisation's central data server or cloud platform; use system protection mechanisms against unauthorised access, and to allow data to be backed up regularly), access to personal data (i.e. users must keep desks clear; never leave IT assets unattended; use of strong passwords; frequent renewal of passwords - changing passwords regularly can prevent someone who has already compromised an account from continuing to gain access), secure data transfer (i.e. users must use email security tools - emails are easily copied and forwarded, resulting in unauthorised access; mechanisms to allow reviewing the email trail prior to replying, forwarding, or copying on an email; access to guidance on securely transmitting paper copies of personal data), and secure disposal of data (i.e. users must have access to paper shredders, access to confidential waste bins, and IT team to regularly erase files containing personal data from external drives).

Several Articles of the GDPR do not impose any obligations or requirements on data controllers or processors, and therefore do not necessitate the implementation of PbDD measures by the organisation. As such, the following GDPR Articles will not be addressed in the DPPA: Articles 1 to 4, Article 23, Articles 40 to 43, Articles 50 to 88, and Articles 90 to 99. However, these Articles may be briefly referenced, if necessary, to ensure coherence of thought.

8.1.1. Transparency behind PbDD operations

In accordance with the GDPR, personal data processing must be carried out in a transparent manner with regard to the data subject. Transparency encompasses both the information that must be provided to individuals prior to processing and the information that should be accessible to data subjects during processing, as well as the information provided to individuals in response to a data access request.⁷³¹

A1. To ensure transparency: organisations must clearly and concisely provide the following key information to the data subject: (a) all purposes of processing; (b) reliance on the legitimate interest processing ground; (c) the logic in automated decision making, (d) use of third parties to process data; (e) cross-border data transfers; (f) data retention periods; and (g) individuals' rights (access, rectification, objection, etc.).

A1.1. Furthermore, at the outset of PbDD implementation, certain operational actions are necessary. The data controller is required to create a data privacy policy, along with policies and procedures to ensure the quality of data. Additionally, it should establish policies or operational procedures and mechanisms to incorporate data privacy and protection into record retention.

A1.2. A Data Protection Impact Assessment (DPIA) is required for any new programs, systems, or processes, or changes to existing ones.

A1.3. Finally, the data controller must establish an information security policy that incorporates data privacy and protection in relation to all corporate assets, including cloud assets and Software as a Service (SaaS) systems, processing personal data.

⁷³¹ GDPR, Article 12(2).

8.1.2. PbDD: operations focused on TOMs

The presented mapping of GDPR Articles⁷³² will link to specific TOMs that are pertinent to the Article's requirement or obligation, thereby generating a holistic and easily comprehensible practical framework. Within the context of implementing PbDD measures that address the security of processing, 'technical measures' are constructed as controls and safeguards offered to systems and to any technology part of an organisation, including devices, networks, and hardware. Protecting such assets is the first line of defence against data breaches, as they are critical to ensuring the secure processing of personal data. Organisations adopting an ISMS based on ISO 27001, for example, could also map the PbDD TOMs to the ISO 27001⁷³³ Annex A controls.⁷³⁴ Figure 29 depicts some areas of data security that must be considered when devising a PbDD plan.⁷³⁵

⁷³² The GDPR establishes a legal framework for comprehensive data protection and security that encompasses various criteria, such as high standards for managing personal data breaches, protecting personal data, managing third-party involvement, data minimisation, and storage limitation. The GDPR heavily incorporates the principle of "Privacy by Design," as evident from Article 25 GDPR titled 'Data Protection by Design and by Default' and the use of appropriate technical and organisational measures.

⁷³³ In accordance with Article 25(3) GDPR.

⁷³⁴ See isms.online, ISO 27001 – Annex A Controls, < <https://www.isms.online/iso-27001/annex-a-controls/>>. Annex A.5 – Information Security Policies (the objective of this Annex is to manage direction and support for information security in line with the organisation's requirements); Annex A.6 – Organisation of Information Security (the objective is to establish a management framework to initiate and control the implementation and operation of information security within the organisation); Annex A.7 – Human Resource Security (the main objective in this Annex is to ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered); Annex A.8 – Asset Management (the objective in the Annex is to identify information assets in scope for the management system and define appropriate protection responsibilities); and Annex A.9 – Access Control (the objective in this Annex is to limit access to information and information processing facilities).

⁷³⁵ Cybersecurity refers to the protection of computer systems, networks, and data from unauthorized access, theft, damage, or disruption. It involves implementing various measures such as firewalls, intrusion detection systems, and antivirus software to defend against cyber threats. Cybersecurity aims to ensure the confidentiality, integrity, and availability of digital information. See National Cyber Security Centre (NCSC). (n.d.). Cyber Security, < <https://www.ncsc.gov.uk/cybersecurity>>. Physical security focuses on safeguarding physical assets, such as hardware, facilities, and infrastructure, from unauthorized access, theft, or damage. It includes measures like access control systems, CCTV surveillance, security guards, and secure storage facilities. Physical security aims to prevent physical breaches that may compromise sensitive data or disrupt operations. See Centre for the Protection of National Infrastructure (CPNI). (n.d.). Physical Security.

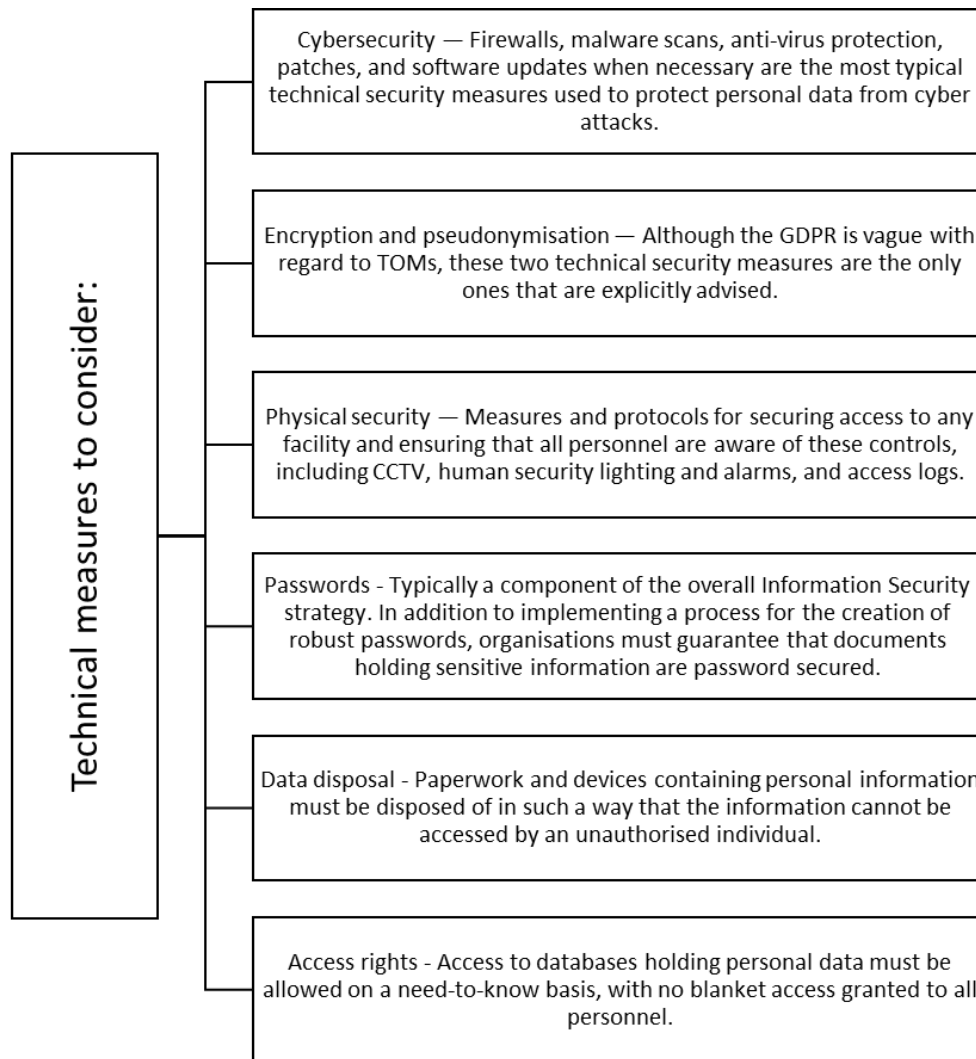


Figure 28 - Technical measures to consider in the PbDD plan.

<https://www.cpni.gov.uk/physical-security>. Passwords are a common authentication method used to protect user accounts and data. They are typically a combination of alphanumeric characters and are kept confidential. Strong passwords should be used, incorporating a mix of upper and lower case letters, numbers, and special characters. See, National Cyber Security Centre (NCSC). (n.d.). Password Guidance: Simplifying Your Approach. <https://www.ncsc.gov.uk/collection/passwords/updated-your-approach>. Data disposal refers to the secure removal or destruction of data that is no longer needed. It is crucial to ensure that sensitive information does not end up in the wrong hands. Secure data disposal methods include overwriting data with random patterns, physical destruction of storage media, or using specialized data erasure tools. Adhering to proper data disposal practices helps to mitigate the risk of data breaches. See Information Commissioner's Office (ICO). (n.d.). Securely Erasing Personal Data. <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/erasure/>. Access rights refer to permissions and privileges granted to individuals or user accounts for accessing specific resources or data within an organization's systems. Access rights are typically assigned based on job roles and responsibilities to ensure that individuals have the necessary level of access required for their tasks. Implementing proper access controls helps to prevent unauthorized access, protect sensitive information, and maintain data confidentiality. See, National Cyber Security Centre (NCSC). (n.d.). Access Control. <https://www.ncsc.gov.uk/collection/access-and-identity-management/using-access-control>.

Moreover, internal policies,⁷³⁶ organisational frameworks or standards, codes of conduct,⁷³⁷ and controls and audits are examples of organisational measures that organisations might use to safeguard the security of personal data, as illustrated in figure 30. The implementation of the following organisational measures will help to ensure consistency in the protection of personal data across the processing cycle.

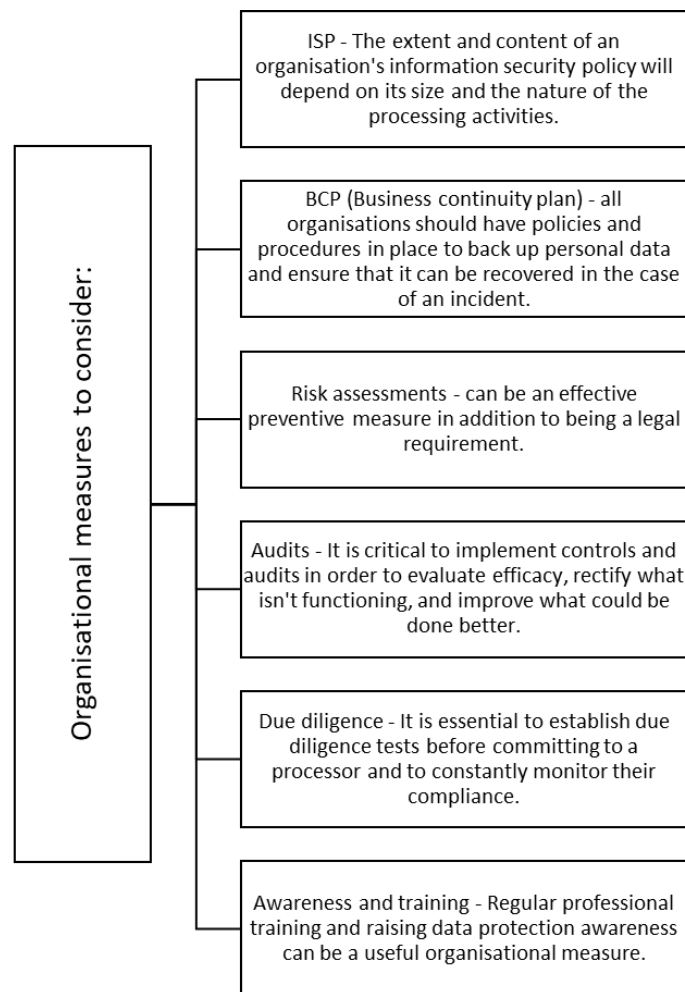


Figure 29 - Organisational measures to consider in the PbDD plan.

⁷³⁶ GDPR, Article 24(2).

⁷³⁷ *ibid.*, Article 24(3).

The organisation is required to incorporate TOMs in compliance with Articles 24, 25, and 32 of the GDPR.⁷³⁸ Such measures must be periodically reviewed for their practicability and state-of-the-art and must be improved whenever possible to enhance their security and protection levels.

A2., A3. The security measures presented below elaborate on examples of TOMs, respectively, that can be implemented within systems and processes⁷³⁹ and, if appropriate, further mapped to ISMS ISO 27001:⁷⁴⁰

7.1.2.1. Data confidentiality

This area can be divided into the following operational actions: implementation of

A2.1./A3.1. Physical access measures⁷⁴¹

A2.1. Technical measures: A comprehensive set of technical measures aimed at minimising the probability of unauthorised access and preserving the integrity of personal

⁷³⁸ Article 24 GDPR emphasises the responsibility of data controllers to incorporate measures that prioritise data protection from the outset of systems and processes. It highlights the significance of considering data protection principles and implementing appropriate safeguards. Article 25 GDPR focuses on the principle of data protection by default. It mandates organisations to establish measures to ensure that, by default, only necessary personal data is processed. Article 32 GDPR underscores the necessity of implementing security measures to safeguard personal data against unauthorised access, loss, or disclosure. See, Information Commissioner's Office (ICO). (n.d.). Guide to the General Data Protection Regulation (GDPR). <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/>>.

⁷³⁹ This is not an exhaustive list of technical and organisational measures currently available to organisations, rather examples of measures based on the current state of the art.

⁷⁴⁰ For a discussion on bridging ISO 27001 to GDPR, please see 'White Paper – IAPP-OneTrust Research: Bridging ISO 27001 to GDPR' <<https://iapp.org/resources/article/iapp-onetrust-research-bridging-iso-27001-to-gdpr/>>.

⁷⁴¹ Technical and organisational measures designed to prevent unauthorised individuals from getting access to data processing systems that process personal data.

data. These measures encompass several physical security mechanisms, including an advanced alarm system capable of identifying and notifying security personnel in real-time of any attempts at unauthorised access. Furthermore, a manual locking system can be deployed to limit physical access to areas where personal data is stored or processed. Biometric access control, such as fingerprint or facial recognition technology, can be utilised as an additional layer of security, ensuring that only authorised individuals are granted access to secure locations. To restrict unauthorised access to sensitive information, smart cards can be issued to individuals with specific clearance levels or permissions. Lastly, Closed-Circuit Television (CCTV) surveillance can be employed as an effective deterrent against potential threats and can also aid in forensic investigations following a security breach.

A3.1. Organisational Measures: Measures that serve to reinforce an organisation's technical measures and promote the effectiveness of its security protocols. These measures encompass a range of procedures, such as the appointment of a receptionist who is responsible for controlling and monitoring access to the organisation's premises, ensuring that only authorised personnel are granted entry. The use of a visitors' book is also recommended, which records the identity and purpose of visitors, thereby enabling the organisation to maintain a record of all individuals who have accessed the premises. Staff and visitors' cards or badges can be issued to authorised personnel, clearly indicating their clearance level, and restricting access to certain areas, thereby reducing the likelihood of data breaches. Additionally, the DPPA emphasises the adoption of an Information Security Policy (ISP) and Standard Operating Procedures (SOPs) as crucial organisational

measures.⁷⁴² An ISP outlines the Regulations, procedures, and rules governing the handling, storage, and processing of personal data, thereby underscoring the organisation's commitment to data protection, and establishing a framework for GDPR compliance (e.g., DPPA). SOPs are also critical, providing specific guidelines and procedures that staff must follow when handling personal data, such as protocols for secure data storage, data breach management, and the disposal of personal data.

A2.2./A3.2. Logical access measures;⁷⁴³

A2.2. Technical measures: Measures aimed at enhancing logical access security, including the implementation of strong passwords, anti-virus software or servers, firewall and intrusion detection systems, encryption of servers, data carriers, smartphones, laptops, and tablets, and two-factor authentication. Strong passwords are a simple yet effective measure to prevent unauthorised access to digital resources. They should be unique, complex, and regularly changed to reduce the risk of password-based attacks. Anti-virus software and servers can detect and eliminate malware that may be introduced into an organisation's digital ecosystem. Firewalls and intrusion detection systems can prevent unauthorised access to networks, applications, and databases, safeguarding digital resources. Encryption is a potent tool referred to in the GDPR to enhance logical access

⁷⁴² Creating comprehensive policies and procedures is vital for organisations to ensure the proper management of personal data and adhere to GDPR requirements. This approach fosters transparency, accountability, and consistency in data handling practices, thereby safeguarding individuals' privacy rights. See, Information Commissioner's Office (ICO). (n.d.). Guide to the General Data Protection Regulation (GDPR). <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/>>.

⁷⁴³ Technical and organisational measures designed to prevent unauthorised users from accessing data processing systems.

security.⁷⁴⁴ Encrypting sensitive data at rest and in transit can prevent unauthorised access even if the data is intercepted or stolen. Encryption can be applied to servers, data carriers, smartphones, laptops, and tablets, providing an additional layer of protection. Two-factor authentication is also gaining popularity as a logical access measure. This mechanism requires users to provide two forms of authentication before being granted access to digital resources, such as a password and a fingerprint, or a password and a token.

A3.2. Organisational measures: Measures to support and reinforce logical access security. These measures include user permission management, central password assignment, the implementation of an ISP, SOPs, and IT user Regulations. User permission management is the process of assigning specific privileges and access rights to individuals based on their job responsibilities and level of clearance. This process ensures that each user only has access to the data and systems they need to perform their duties, minimising the risk of unauthorised access. User permission management can be implemented using credentials, such as usernames and passwords, to provide a granular level of control over access rights. Central password assignment is another critical measure to enhance logical access security. This measure involves the assignment and management of passwords centrally, typically by an IT department. Central password assignment ensures that passwords are strong and unique and are changed regularly to minimise the risk of password-based attacks. The implementation of an ISP and SOPs is also crucial in ensuring effective logical access security. An ISP provides clear guidelines and procedures for the

⁷⁴⁴ For a discussion on the use of encryption schemes, See e.g., Lei Liu, Mingwei Cao and Yeguo Sun, 'A Fusion Data Security Protection Scheme for Sensitive E-Documents in the Open Network Environment' (2021) 16 PloS one e0258464.

handling, storage, and transmission of sensitive information, thereby promoting data privacy and confidentiality.⁷⁴⁵ SOPs outline the specific steps and procedures to be followed by staff when handling digital resources, such as software and databases, reducing the risk of human error or negligence.⁷⁴⁶

Lastly, IT user Regulations, also known as work directives, provide guidance on the acceptable use of digital resources, such as computers and networks, within the organisation. These Regulations outline the specific responsibilities of IT users, including the requirement to report any suspicious activity or potential security breaches, thereby promoting a culture of security and vigilance.

A2.3./A3.3. Authorisation measures;⁷⁴⁷

A2.3. Technical measures: Measures aimed at enhancing authorisation security, including SSH encrypted access,⁷⁴⁸ certified SSL encryption,⁷⁴⁹ physical deletion of data carriers, and file shredder or external deletion of files (in accordance with DIN 66399).⁷⁵⁰

⁷⁴⁵ For a discussion on the application of Information Security Policies (ISP), See e.g., Karin Höne and JHP Eloff, 'Information Security Policy — What Do International Information Security Standards Say?' (2002) 21 Computers & security 402.

⁷⁴⁶ For a practical example of application of Standard operating procedures (SOP), See, e.g., GMH Bollen and MCE Schoordjik, 'HLA Tissue Typing of Family Donors: Respect for Privacy and Wellness' (2009) 43 Bone marrow transplantation (Basingstoke) S310.

⁷⁴⁷ Technical and organisational measures designed to ensure that persons permitted to use a data processing system can only access personal data that is relevant to their role in the organisation, and that personal data cannot be read, copied, modified, or erased without authorisation during the processing and after storage.

⁷⁴⁸ The acronym SSH stands for Secure Shell. The SSH protocol was developed as a secure alternative to unsecured remote shell protocols. It uses a client-server paradigm where clients and server communicate over a secure channel.

⁷⁴⁹ SSL, or Secure Sockets Layer, is an encryption-based Internet security protocol.

⁷⁵⁰ This DIN-norm includes destruction requirements for several media categories. Namely paper, film, optical media, magnetic data media, hard drives and electronic data media.

SSH (Secure Shell) encrypted access is a widely used security protocol for remote login to servers and other digital resources. This protocol encrypts data in transit, preventing unauthorised access to sensitive information. SSL (Secure Sockets Layer) encryption is another potent tool that can be utilised to secure digital communications between servers and web browsers. SSL encrypts data in transit and can provide an additional layer of protection against unauthorised access. Physical deletion of data carriers is a critical measure to ensure that sensitive information is not accessible by unauthorised individuals. When data carriers, such as hard drives or USB flash drives, are no longer required, they should be physically destroyed to prevent any residual data from being accessed. File shredders or external deletion of files, in accordance with DIN 66399, is another measure that can be used to permanently delete sensitive information from digital resources. This method ensures that the data is irreversibly deleted and cannot be recovered by unauthorised individuals.

A3.3. Organisational measures: Measures to support authorisation security,⁷⁵¹ including a minimum number of data administrators, management of user rights and access, the implementation of an ISP, SOPs, and the use of authorisation concepts. The implementation of a minimum number of data administrators is a critical measure to ensure that access to sensitive information is restricted to a select group of authorised individuals. This measure reduces the risk of unauthorised access and ensures that there is a clear chain of responsibility for data security. The management of user rights and access

⁷⁵¹ For a discussion on authorisation security, concepts and models, See e.g., Anton V Uzunov, Eduardo B Fernandez and Katrina Falkner, 'Security Solution Frames and Security Patterns for Authorization in Distributed, Collaborative Systems' (2015) 55 Computers & security 193.

is another crucial measure in authorisation security. It involves the control and monitoring of access rights to ensure that each user only has access to the data and systems they require to perform their duties. This measure can be implemented using credentials, such as usernames and passwords, to provide a granular level of control over access rights. An ISP and SOPs are also pivotal in ensuring effective authorisation security. The use of authorisation concepts is yet another measure that can be used to enhance authorisation security. Authorisation concepts provide a framework for controlling access rights and privileges to digital resources. These concepts can include role-based access control, where access rights are assigned based on job roles, or attribute-based access control, where access rights are assigned based on specific user attributes.

A2.4./A3.4. Separation measures;⁷⁵²

A2.4. Technical measures: Measures aimed at enhancing separation security, including the separation of production and test environments, physical separation of systems and databases, VLAN (Virtual Local Area Networks) segmentation, logical separation of client systems, and multi-tenancy of relevant applications and databases.

The separation of production and test environments is a crucial measure to ensure that changes made to software or systems are fully tested before they are implemented in the production environment. This separation prevents errors or vulnerabilities from being introduced to the production environment, which could lead to data breaches or other

⁷⁵² Technical and organisational measures designed to make it possible to process data obtained for various purposes separately. This can be done, for instance, by physically and logically separating the data sets.

security incidents. Physical separation of systems and databases is another important measure to prevent unauthorised access. This measure involves keeping systems and databases in physically separate locations, or behind secure physical barriers, to prevent unauthorised access. VLAN segmentation is another measure that can be used to enhance separation security. VLANs can be used to partition a network into smaller, isolated segments. This segmentation can help to prevent unauthorised access to sensitive information and can also reduce the impact of a security breach by limiting the spread of any malware or viruses. Logical separation of client systems involves the use of access control measures to ensure that only authorised individuals have access to sensitive information. This measure can be implemented using credentials, such as usernames and passwords, to provide a granular level of control over access rights. Finally, multi-tenancy of relevant applications and databases can be used to ensure that each client or user has their own isolated environment within a shared system. This measure can help to prevent data leakage or unauthorised access between different clients or users, ensuring data privacy and confidentiality.

A3.4. Organisational measures: Measures aimed at supporting separation security, including database rights, the implementation of ISP, data protection policy, SOPs, and security guidelines or instructions for software development.

Database rights refer to the specific permissions and privileges granted to individuals or groups to access databases within an organisation. These permissions and privileges must be granted only to authorised individuals and must be consistent with their job responsibilities. Proper management of database rights ensures that access to sensitive information is limited to only those who require it to perform their duties.

An ISP and data protection policy are crucial in ensuring effective separation security. These policies provide clear guidelines and procedures for the handling, storage, and transmission of sensitive information, thereby promoting data privacy and confidentiality. SOPs outline the specific steps and procedures to be followed by staff when handling digital resources, such as software and databases, reducing the risk of human error or negligence.

Security guidelines or instructions for software development can help ensure that security measures are considered and implemented at every stage of the software development process. This measure can include providing clear guidance on secure coding practices, access control measures, and testing procedures to ensure that any potential vulnerabilities are identified and addressed before software is deployed.

A2.5./A3.5. Pseudonymisation:⁷⁵³

A2.5. Technical measures: Measures aimed at supporting pseudonymisation security, including the separation of the allocation data and storage in a separate system that is encrypted. The separation of the allocation data and storage is a crucial measure in pseudonymisation security. This measure involves keeping the allocation data, which links the pseudonym to the original identity, in a separate system that is encrypted and only accessible to authorised staff. This separation prevents unauthorised access to the allocation data, which could lead to the identification of individuals whose data has been pseudonymised. Storing the allocation data in an encrypted system adds an extra layer of

⁷⁵³ Processing personal data in a way that prevents identification of a particular data subject without the use of additional information, provided that this extra information is kept separately and is subject to the necessary technical and organisational safeguards in accordance with Article 4(5) GDPR.

protection, ensuring that even if the data is accessed by unauthorised individuals, it cannot be read or used to identify individuals. Encryption transforms data into a code that can only be deciphered using a decryption key. This key is only accessible to authorised personnel, ensuring that data remains secure and confidential.

A.3.5. Organisational measures: Measures aimed at supporting pseudonymisation security, including the implementation of an internal directive to anonymise or pseudonymise personal data as much as possible in the event of disclosure to third parties or after the legal retention period has elapsed, the implementation of an information security policy, data protection policy, and guidelines or instructions on cryptography. An internal directive to anonymise or pseudonymise personal data is an essential measure to ensure that personal data is protected and not identifiable after it is disclosed to third parties or after the legal retention period has elapsed. This measure can be implemented using pseudonymisation techniques to protect sensitive information from being identified, even in the event of a data breach.⁷⁵⁴ An ISP and data protection policy are crucial in ensuring effective pseudonymisation security. These policies provide clear guidelines and procedures for the handling, storage, and transmission of sensitive information. They can also include requirements for the use of pseudonymisation techniques to protect sensitive

⁷⁵⁴ Implementing such a directive is essential in safeguarding the privacy and confidentiality of personal data. Anonymisation involves removing or modifying personal identifiers, making it impossible to identify individuals. Pseudonymisation, on the other hand, involves replacing identifiable information with pseudonyms, providing an additional layer of protection. By establishing an internal directive that mandates the anonymisation or pseudonymisation of personal data, organisations can effectively mitigate the risks associated with data breaches, unauthorised access, and misuse of personal information. This ensures that even if the data is accessed or retained beyond the required legal period, individuals' identities remain protected. See, National Cyber Security Centre (NCSC). (n.d.). An Introduction to Pseudonymisation. <<https://www.ncsc.gov.uk/section/information-for/organisations/data-encryption-guidance/encryption-explained/an-introduction-to-pseudonymisation>>.

information and ensure that privacy and confidentiality are maintained. Guidelines or instructions on cryptography can help ensure that pseudonymisation techniques are implemented correctly and effectively. These guidelines can provide clear guidance on encryption and decryption techniques, key management, and other cryptography-related measures to ensure that personal data is effectively pseudonymised.

7.1.2.2. Data integrity

This area can be divided into the following operational actions: implementation of

A.2.6./A3.6. Data transfer measures:⁷⁵⁵

A2.6. Technical measures: Measures aimed at supporting data transfer security, including the use of Virtual Private Network (VPN), encrypted connections, and logging of data access and retrieval. The use of a Virtual Private Network (VPN) is a key measure to ensure secure data transfer. A VPN is a secure and encrypted connection that allows users to access a private network over a public network, such as the internet. VPNs can be used to securely transfer data between different locations or to allow remote access to sensitive information. By using a VPN, organisations can ensure that data is protected from interception and unauthorised access during transfer. The use of encrypted connections is another important measure to ensure data transfer security. Encrypted connections protect data in transit by transforming it into a code that can only be deciphered using a

⁷⁵⁵ Technical and organisational measures intended to ensure that personal data cannot be read, copied, modified, or deleted by unauthorised parties during transfer or storage, and to identify and verify third parties to whom personal data are to be communicated.

decryption key. This measure can be implemented using SSL or TLS protocols to ensure that data is encrypted during transfer. By using encrypted connections, organisations can prevent unauthorised access and ensure the confidentiality of the data being transferred. Logging of data access and retrieval is a crucial measure in data transfer security. This measure involves keeping a record of all data access and retrieval activities, including who accessed the data, when it was accessed, and what was accessed. This information can be used to identify any unauthorised access or suspicious activity and to monitor compliance with data protection Regulations. By implementing logging mechanisms, organisations can detect and respond to any data breaches or security incidents in a timely manner.

A.3.6. Organisational measures: Measures to support data transfer security, including the analysis of routine data retrieval and transmission operations, anonymisation and pseudonymisation guidelines, physical handover of data enclosures included in standard operating procedures, information security policy, and data protection policy.

The analysis of routine data retrieval and transmission operations is a crucial measure in ensuring that data is transferred securely. This measure involves analysing data transfer operations to identify potential vulnerabilities and to develop measures to address them. This analysis can include a review of the types of data being transferred, the frequency of transfers, and the methods used to transfer data. Anonymisation and pseudonymisation guidelines can be used to enhance data transfer security by ensuring that sensitive information is not identified during transfer. These guidelines can provide clear guidance on when and how to use these techniques and can also include requirements for the use of encryption or other security measures. Physical handover of data enclosures included in SOPs is another measure to ensure data transfer security. This measure involves keeping

physical copies of data in secure enclosures during transfer and ensuring that these enclosures are only accessed by authorised personnel. An ISP and data protection policy are crucial in ensuring effective data transfer security. These policies provide clear guidelines and procedures for the handling, storage, and transmission of sensitive information. They can also include requirements for the use of encryption or other security measures during data transfer.

A2.7./A3.7. Data input measures:⁷⁵⁶

A2.7. Technical measures: Measures to support the implementation of role-based access control (RBAC) and the use of strong passwords. RBAC restricts access to data input functions based on job responsibilities, ensuring that only authorised personnel are able to input or modify data. Strong passwords, which are unique and complex, can also prevent unauthorised access to data input functions and minimise the risk of password-based attacks. In addition, the DPPA suggests the use of encryption to protect data during input. Encryption can transform data into a code that can only be deciphered using a decryption key, preventing unauthorised access to sensitive information even if it is intercepted during input. The use of digital signatures, which can be used to verify the authenticity and integrity of data, can also provide an additional layer of security during data input.

⁷⁵⁶ Technical and organisational measures designed to determine retrospectively who entered, edited, or deleted personal data from data processing systems.

A.3.7. Organisational measures: Measures to support data input security, including the mapping of software and systems that can be used to enter, change or delete personal data (assets), use of unique usernames, assignment of rights to enter, change and delete data on the basis of roles, ROPA, ISP, and SOPs. Mapping of software and systems that can be used to enter, change or delete personal data is a crucial measure in ensuring data input security. This measure involves identifying all the software and systems within an organisation that can be used to enter, change or delete personal data, and ensuring that appropriate security measures are implemented for each of them. This can include the implementation of access controls, the use of unique usernames and passwords, and the use of encryption or other security measures. The use of unique usernames is another important measure to ensure data input security. This measure involves assigning unique usernames to personnel who are authorised to enter, change or delete personal data. This ensures that all activities related to data input can be traced back to specific individuals. The assignment of rights to enter, change and delete data on the basis of roles and ROPA is another measure to enhance data input security. This measure involves assigning specific rights to personnel based on their roles and responsibilities within the organisation. For example, staff with administrative roles may be granted more extensive rights to enter, change or delete data than other personnel. An ISP and SOPs are crucial in ensuring effective data input security. These policies and procedures provide clear guidelines and procedures for the handling, storage, and transmission of sensitive information. They can also include requirements for the use of encryption or other security measures during data input.

7.1.2.3. Data Availability and Resilience

This area can be divided into the following operational actions: implementation of

A2.8./A3.8. Availability measures:⁷⁵⁷

A2.8. Technical measures: Measures to protect data from the destructive impact of fire or other disasters. These systems typically comprise fire detection sensors and automatic fire extinguishing systems, which can prevent or minimise damage to servers and other critical equipment that store important data. Server room climatization is another important measure to ensure data availability. This measure involves installing air conditioning and humidity control systems in server rooms to maintain a stable environment for the equipment, which can prevent overheating and damage. In the event of a power outage, the installation of an uninterruptible power supply (UPS) system is a crucial measure to ensure that data remains available. These systems provide emergency power supplies that can keep servers and other equipment running for a certain period of time until power is restored. Hard disk mirroring is another effective measure to ensure data availability. This technique involves creating a copy of data on another hard disk, so that if one hard disk fails, the other can continue to provide access to the data.

To ensure the physical security of servers and other equipment, CCTV and alarm systems are indispensable measures.

⁷⁵⁷ Technical and organisational measures designed to ensure that personal data is protected against accidental destruction or loss.

A3.8. Organisational measures: Measures to bolster data availability. These measures include a personal data backup and recovery process, an ISP, a data protection policy, system integrity testing, and an emergency (and post-mortem) plan. The personal data backup and recovery process is a pivotal measure in safeguarding data availability during system failures or disasters. This process involves systematically backing up personal data and implementing a recovery process to restore data from backups in the event of a system malfunction or catastrophe. By minimising the likelihood of data loss, this measure ensures that authorised staff have access to personal data when required. In addition, ISPs and data protection policies play a crucial role in ensuring effective data availability. These policies provide comprehensive guidance and procedures for handling, storing, and transmitting sensitive information. They may also require regular backups of personal data (backup schedules) and the implementation of recovery processes to further reinforce data availability. Furthermore, system integrity testing is another essential measure to uphold data availability. By conducting regular assessments of all systems and equipment that store personal data, this measure ensures that such systems are functioning correctly and helps to identify potential vulnerabilities or weaknesses that could jeopardise data availability. This guarantees that authorised staff can always access personal data when needed. Finally, an emergency (and post-mortem) plan is a critical measure to ensure data availability during disasters or other incidents. This plan outlines a series of steps to take in the event of an emergency or incident that may impact data availability, including implementing recovery processes, notifying pertinent staff, and identifying potential risks or weaknesses that may affect data availability in the future. The post-mortem phase involves scrutinising the emergency response and identifying areas for improvement to enhance future response capabilities.

A.2.9./A3.9. Recoverability measures: ^{758,759}

A2.9. Technical measures: Measures to bolster data recoverability, including systems for backup monitoring and reporting, as well as automated systems for restorability of personal data. Systems for backup monitoring and reporting are crucial in ensuring the recoverability of personal data. These systems can actively monitor the backup process, issuing real-time alerts and notifications to relevant staff in the event of any failures or issues. This ensures that all personal data is backed up regularly and that the backups are functioning correctly. Additionally, automated systems for restorability of personal data are essential to maintain recoverability security. These systems automate the process of restoring personal data from backups during system failures or disasters. This minimises any downtime and guarantees that authorised staff have access to personal data when required.

A3.9. Organisational measures: Measures to reinforce data recoverability, including a regular testing plan for data recovery, a storage of backup media policy, an emergency plan included in a Business Continuity Plan (BCP), an ISP, and SOPs. A regular testing plan for data recovery is an indispensable measure to ensure the recoverability of personal data. This measure involves conducting periodic tests of the backup and recovery process to confirm that personal data can be retrieved quickly and efficiently in case of

⁷⁵⁸ Technical and organisational measures designed to rapidly restoring the availability of and access to personal data in the event of a physical or technical incident.

⁷⁵⁹ In the context of implementing PbDD, it is essential to differentiate between system availability and recoverability. System availability refers to the system's ability to remain operational, whereas system recoverability pertains to the system's ability to recuperate from technical failures.

system failures or disasters. This helps to reduce the risk of data loss and ensures that authorised staff can access personal data when required. Another critical measure to ensure recoverability security is the implementation of a storage of backup media policy. This measure involves establishing policies for the secure storage of backup media to ensure the recoverability of personal data in the event of disasters or incidents that may affect the primary storage system. These policies may include requirements for the use of secure storage facilities, the implementation of access controls, and regular testing of backup media. An emergency plan included in a BCP is another crucial measure to ensure recoverability of personal data in case of disasters or incidents. This plan outlines the necessary steps to be taken during emergencies or incidents that could impact data availability, including the implementation of recovery processes, notification of relevant staff, and identification of potential risks or weaknesses that could affect data availability in the future. Moreover, an ISP and SOPs are fundamental measures in ensuring effective recoverability security. These policies provide clear guidelines and procedures for the handling, storage, and transmission of sensitive information. They may also include requirements for regular testing of the backup and recovery process, the implementation of secure storage facilities, and the development of an emergency plan included in a BCP.

7.1.2.4. Data Protection Governance and Compliance

This area can be divided into the following operational actions: implementation of

A2.10./A3.10 Operational management measures:

A2.10 Technical measures: Measures to reinforce operational management security, including the centralization of documentation for data protection requirements

and obligations with access granted to employees, data security certification (such as ISO 27001), an annual review of the effectiveness of TOMs, automation of Data Protection Impact Assessments (DPIAs), and implementation of a data protection governance structure. Centralizing documentation for data protection requirements and obligations is an essential measure to ensure effective operational management of personal data. This measure involves gathering all relevant documentation related to data protection requirements and obligations, including policies, procedures, guidelines, and standards, and granting access to all staff responsible for personal data management. This helps to ensure that all employees are aware of their responsibilities and obligations related to personal data management and that the organisation is compliant with relevant laws and Regulations. Data security certification, such as ISO 27001, is another significant technical measure to support operational management security. This certification provides a framework for the implementation of an Information Security Management System (ISMS) to ensure the confidentiality, integrity, and availability of personal data. This demonstrates the organisation's commitment to data protection and can provide assurance to customers, partners, and regulators. Conducting an annual review of the effectiveness of TOMs is another crucial technical measure to ensure effective operational management of personal data. This measure involves regularly reviewing the TOMs implemented by the organisation to ensure that they are effective in safeguarding personal data and that they are in compliance with relevant laws and Regulations. Automating DPIAs is another vital technical measure to support operational management security. Automating the DPIA process can help to ensure that all relevant risks are identified and assessed, and that appropriate measures are implemented to mitigate those risks. Implementing a data protection governance structure is a final important technical measure to support

operational management security. This measure involves setting up a governance structure to ensure effective oversight and management of personal data. This can include appointing a Data Protection Officer (DPO) to supervise data protection activities, creating a data protection policy and associated procedures, and conducting regular training and awareness-raising activities for employees.

A3.10 Organisational measures: Measures to bolster operational management security, including the appointment of a Data Protection Officer (DPO), regular training for employees, the performance of Data Protection Impact Assessments (DPIAs), processes for meeting information obligations under Articles 13 and 14 of the GDPR, processes for handling requests for information from data subjects, and annual monitoring audits. The appointment of a Data Protection Officer (DPO) is a crucial organisational measure to ensure effective operational management of personal data. The DPO oversees the organisation's compliance with data protection laws and Regulations, including the GDPR, providing advice and guidance, and acting as a point of contact for data subjects and regulators. The DPO also monitors the effectiveness of the organisation's TOMs for safeguarding personal data. Regular training for employees is another significant organisational measure to support operational management security. This measure involves providing GDPR and IS training to all employees who have access to personal data or are responsible for its management. Regular refreshers are also necessary to ensure that employees are up to date on any changes to data protection laws or Regulations. Conducting DPIAs is another essential organisational measure to support operational management security. DPIAs assess the risks associated with personal data processing activities and are mandatory under the GDPR for certain types of processing activities.

Establishing processes for meeting information obligations under Articles 13 and 14 of the GDPR is another important organisational measure to ensure effective operational management of personal data. These obligations require organisations to provide information to data subjects about how their personal data is being processed. Establishing processes for meeting these obligations helps to ensure that data subjects are aware of their rights and that the organisation is in compliance with the GDPR. Processes for handling requests for information from data subjects (DSARs) are also a crucial organisational measure to support operational management security. These processes ensure that requests for information from data subjects are handled promptly and appropriately, ensuring that data subjects have access to their personal data and that the organisation is in compliance with the GDPR. Finally, conducting annual monitoring audits is a crucial organisational measure to support operational management security. These audits evaluate the effectiveness of the organisation's TOMs for safeguarding personal data, ensuring compliance with applicable laws and Regulations, and identifying areas for improvement to continuously improve data protection practices.

A2.11./A3.11 Incident response management measures (IRMT):⁷⁶⁰

A2.11. Technical measures: Measures to support incident response management (IRMT), including the use of a Firewall, spam filters, virus scanners, intrusion detection systems (IDS), and intrusion prevention systems (IPS).

⁷⁶⁰ Procedure and support for data breach and security breach response processes.

A Firewall is a fundamental technical measure that serves as a barrier between an organisation's internal network and external networks, such as the internet. Its configuration ensures that only authorised traffic passes through, blocking unauthorised access and safeguarding the organisation's network and personal data against potential security breaches. Spam filters are another technical measure that organisations can use to prevent security incidents involving personal data. By detecting and blocking unsolicited emails and other messages containing harmful content or links, these filters help prevent employees from inadvertently exposing personal data to unauthorised individuals, thereby reducing the likelihood of a security incident. Virus scanners are a third technical measure that can prevent security incidents involving personal data. These scanners are designed to detect and remove viruses, malware, and other malicious software from an organisation's network and devices. Intrusion detection systems (IDS) and intrusion prevention systems (IPS) are additional technical measures that can detect and respond to security incidents involving personal data. IDS are designed to detect and alert on unauthorised access attempts or other security events, while IPS are designed to block unauthorised access attempts or other security events. These measures can help prevent security incidents involving personal data from escalating or spreading, minimising their impact on the organisation.

In addition to these technical measures, IRMT requires appropriate organisational and physical security measures to ensure comprehensive data protection. This may include processes for reporting and responding to security incidents, employee training on incident response, and regular testing and updating of incident response plans.

A3.11. Organisational measures: Measures to bolster IRMT. These measures include a set of documented procedures for detecting and reporting security events and data breaches, the involvement of a Data Protection Officer (DPO) in security incidents and data breaches, the use of a project management tool (PMT) for documenting security incidents and data breaches, post-mortem procedures for data breaches, ISPs, and data protection policies, as well as SOPs for handling data breaches and near-misses. Documented procedures for detecting and reporting security events and data breaches are fundamental to ensuring the effective management of incidents. These procedures provide a clear framework for employees to identify and report security incidents and data breaches promptly, thereby facilitating their timely resolution. By documenting these procedures, organisations can ensure that all employees are aware of their responsibilities and can effectively detect and report incidents and data breaches. Another important measure is the involvement of the DPO in security incidents and data breaches. The DPO can offer guidance and support to ensure compliance with applicable laws and Regulations, as well as identify areas for improvement in incident response management processes. This can enhance the organisation's response to incidents and data breaches. The use of a project management tool (PMT) to document security incidents and data breaches is also a crucial measure. This tool allows organisations to track incidents and breaches, enabling them to manage and resolve them effectively. Additionally, the PMT can be used to record the organisation's remediation efforts, creating an accurate record of its response to incidents and data breaches. Post-mortem procedures for data breaches offer yet another valuable measure to support IRMT security. By reviewing an organisation's response to a data breach, these procedures enable identification of areas for improvement and the implementation of changes to prevent similar incidents from occurring in the future

(lessons learned). ISPs and data protection policies are also critical measures to ensure IRMT security. These policies provide employees with guidance on their responsibilities and the organisation's approach to information security and data protection. Finally, SOPs for handling data breaches and near-misses are an essential measure to ensure a consistent and effective response to incidents and data breaches. These SOPs provide clear guidance on the appropriate steps to take, ensuring that all employees respond to incidents and data breaches appropriately and consistently. By implementing these SOPs, organisations can minimise the impact of incidents and data breaches and maintain the security of personal data.

A2.12./A3.12 PbDD management measures:

A2.12. Technical measures: Measures to support Data Protection by Design and Default (PbDD) management. These measures include ensuring that only necessary personal data is collected, utilisation of data protection-friendly default settings in all software, and a methodology for implementing all necessary measures in the systems and processing activities. To ensure effective PbDD management, organisations must adhere to the principle of collecting no more personal data than is necessary for the intended purpose. This technical measure requires organisations to collect only the minimum amount of personal data necessary to achieve the intended purpose. This measure is vital for protecting the privacy and data subject rights, ensuring that personal data is not processed beyond the scope of what data subjects have consented to. Another critical technical measure for PbDD management is the utilisation of data protection-friendly default settings in all software. This measure requires organisations to configure software

with default settings that protect the privacy and security of personal data. For example, default settings could include minimising data retention periods or ensuring that data is automatically pseudonymised or anonymised.

A methodology for implementing all listed measures (as required) in the systems and processing activities is another essential technical measure for PbDD management (e.g., DPPA). This methodology should ensure that all necessary measures are implemented systematically and consistently across all systems and processing activities. This approach ensures that personal data is processed in a manner that complies with the GDPR and protects data subject rights and freedoms. In addition to technical measures, PbDD management requires appropriate organisational and physical security measures to ensure comprehensive data protection. Such measures may include processes for obtaining and documenting data subject consent, regular review of data retention periods, employee training on PbDD, and regular testing and updating of PbDD policies and procedures.

A3.12. Organisational measures: Measures to support PbDD management. Among these measures, the development and implementation of a data protection policy that incorporates the principles of PbDD, data protection principles, and mechanisms for responding to data subjects' rights is a crucial element. An effective data protection policy that incorporates the principles of PbDD is a cornerstone of PbDD management. This policy should reflect the organisation's commitment to PbDD and outline the principles that will guide the organisation's processing activities. It should also provide guidance on how to implement PbDD measures and foster a culture of privacy and security within the organisation. Furthermore, the data protection policy should include the data protection principles, such as transparency, purpose limitation, data minimisation, accuracy, storage

limitation, integrity, and confidentiality. These principles are fundamental to ensuring that personal data is processed lawfully, fairly, and transparently, while also protecting the rights and freedoms of data subjects. Moreover, the data protection policy should contain mechanisms for responding to data subjects' rights. This includes well-documented processes for addressing data subjects' requests for access to their personal data, rectification, erasure, restriction of processing, data portability, and objection to processing. These processes should be clearly communicated to all employees to ensure that data subjects' rights are protected. Effective implementation of a data protection policy that incorporates the principles of PbDD, data protection principles, and mechanisms for responding to data subjects' rights requires a commitment from senior management and the engagement of all employees. The policy should be periodically reviewed and updated to ensure that it remains effective in protecting personal data and in compliance with relevant laws and Regulations.

A2.13./A3.13 Third party measures:⁷⁶¹

A2.13. Technical measures: Measures to support PbDD management concerning third-party involvement. These measures include the monitoring of external parties' remote access to personal data, monitoring of processors and sub-processors, and the automation of Records of Processing Activities (ROPA) to include international data transfers. Monitoring external parties' remote access to personal data is an essential

⁷⁶¹ Technical and organisational measures designed to ensure that personal data processed on behalf of the controller can only be processed in accordance with the controller's instructions.

technical measure for PbDD management. This measure requires the use of secure virtual private networks (VPNs) or other secure remote access systems and the establishment of clear protocols for granting remote access to personal data. This measure helps to ensure that external parties, such as contractors and service providers, are not given excessive access to personal data. Another important technical measure for PbDD management is the monitoring of processors and sub-processors. This measure requires all processors and sub-processors to meet the same level of data protection requirements as the organisation itself. This measure includes establishing clear protocols for data processing, data protection agreements, and regular audits of processors' compliance with data protection requirements. Additionally, data retention schedules for data processed by processors and sub-processors are also an essential technical measure for PbDD management. This measure ensures that personal data is not retained by processors and sub-processors for longer than necessary and that data is securely and permanently deleted at the end of its retention period. The automation of an audit system for data processors is another critical technical measure for PbDD management. This measure requires the regular audits of data processors' compliance with data protection requirements and the prompt addressing of any issues discovered. Finally, the automation of ROPA to include international data transfers is an important technical measure for PbDD management. This measure ensures that all international data transfers are conducted in compliance with the GDPR and that appropriate safeguards are in place to protect personal data during international transfers.

A3.13. Organisational measures: Measures to ensure comprehensive data protection. Third-party measures are particularly critical to ensuring that all parties with access to personal data, including data processors and sub-processors, are also adhering to

PbDD principles. An essential organisational measure is the establishment of a due diligence process for third parties, which should include an assessment of their data protection practices. This process ensures that third parties meet the same level of data protection requirements as the organisation itself and that they fully understand their responsibilities under the GDPR. Another vital organisational measure is the development of SOPs for the onboarding of third parties with data protection responsibilities. These SOPs should provide clear guidance on the steps to be taken when onboarding third parties, including the establishment of clear protocols for data processing, data protection agreements, and regular audits of the third party's compliance with data protection requirements. SOPs for international transfers of personal data are also essential organisational measures for effective PbDD management. These SOPs should incorporate mechanisms for the protection of personal data, such as Standard Contractual Clauses (SCCs), and ensure that all international transfers of personal data are conducted in compliance with the GDPR. Finally, agreements in accordance with Article 28 of the GDPR are another critical organisational measure for effective PbDD management of third parties. These agreements ensure that all data processors and sub-processors meet the same level of data protection requirements as the organisation itself and establish clear protocols for data processing, data protection, and regular audits of the processor's compliance with data protection requirements.

Important operational note

The aforementioned list (A1-A3) of TOMs aims to assist the data controller in attaining the highest level of compliance with data protection principles, with a specific focus on information security as stipulated in Article 32 of the GDPR. The list is divided into three

categories: A1 (General Governance Measures), A2 (Technical Measures), and A3 (Organisational Measures). A2 and A3 measures align with common Information Security (IS) groups, simplifying the integration of the DPPA with an Information Security Management System (ISMS) such as ISO 27001 through a straightforward checkbox process. Moreover, it serves as a foundation for implementing PbDD. It is important to note that A1, A2, and A3 measures must be incorporated from the outset of the processing activity to ensure full compliance with the requirements of the GDPR.

8.2. Implementing the GDPR principles through PbDD

Article 5 GDPR,⁷⁶² establishes the general principles that must be followed by all personal data processing activities, namely: lawfulness, fairness, and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability. These principles are supported by the following GDPR Articles: Articles 6, 9 and 10 GDPR (Lawfulness); Articles 13 and 14 GDPR (Transparency); Article 6 GDPR (Purpose limitation); Article 32 GDPR (Integrity and confidentiality); and Article 30 GDPR (Accountability).

The following operational actions ensure that data processing activities are consistent with data protection principles:⁷⁶³ (i) Incorporation of effective data protection into processing activities (or systems) through the implementation of TOMs, which includes

⁷⁶² See also Recital 39 GDPR.

⁷⁶³ GDPR, Article 24.

the conduct of a DPIA;⁷⁶⁴ (ii) Conduction of a GAP analysis – the controller compares the current TOMs with its target state (organisation's status quo), in order to determine the applicable mechanisms to (a) incorporating data protection into information security systems and policies; (b) incorporating data protection into data retention practices (including ensuring data quality). Additionally, the controller is accountable for developing or updating data protection policies and documenting data protection actions.⁷⁶⁵

Modus Operandi

The DPPA adopts a question-and-answer (Q&A) approach to facilitate the implementation of PbDD, as demonstrated by the following example:

1. The question posed pertains to a GDPR requirement or obligation, such as whether "all activities involving the processing of personal data are governed by the general principles outlined in Article 5 of the GDPR."

2. A gap analysis is employed to determine the answer, whereby an affirmative response indicates the presence of an organisational-level data protection policy that guides employees in processing and safeguarding personal data. This policy ensures alignment with the fundamental rights of individuals as outlined in the GDPR.

3. In the case of a negative response, the operational task resulting from this exercise entails implementing a technical and organisational measure. In this instance, the corresponding measure involves creating and maintaining a data protection policy to

⁷⁶⁴ As previously discussed, and according to EPBD guidelines, DPIAs are required as part of the development process for new processing or changes to existing processing activities.

⁷⁶⁵ Documentation should be retained to demonstrate compliance and accountability.

establish the necessary framework for data processing and protection within the organisation.⁷⁶⁶

There is, however, no one-size-fits-all approach to applying TOMs. This task depends on various factors, including the type of data processed, the purpose of processing, the means of processing - assets and technology used, and the period of processing, among others.

Consider the following operational example of how the transparency principle can be applied to a company's website:

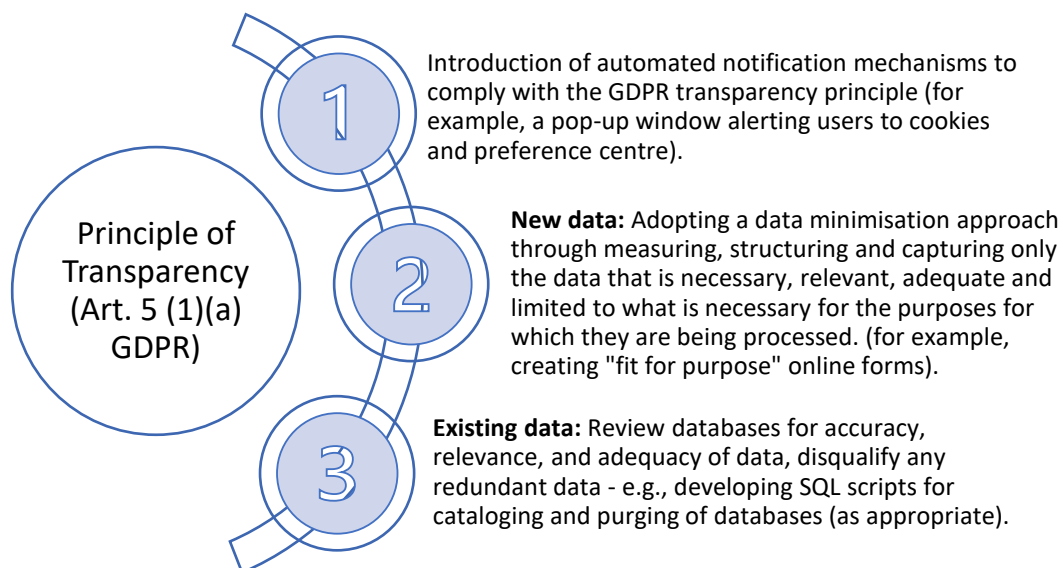


Figure 30 - Operational example: implementing a principle through PbDD

Below are some of the Q&As that will allow the controller to implement the data protection principles via PbDD:

⁷⁶⁶ Compliance evidence examples: A data protection policy that explains how the organisation handles personal information is in place. A strategy for implementing PbDD is in place.

Q: Does the organisation have established policies and procedures for data quality?

An affirmative response indicates that the organisation has implemented robust procedures to ensure the accuracy and currency of its data in accordance with established policies. Should personal data be deemed inaccurate for the purposes of processing, the organisation must act with expediency to rectify or delete said data without undue delay.⁷⁶⁷

Q: Are there policies and procedures in place in the organisation to govern the secondary use of personal data?

An affirmative response indicates that the organisation has established a system or process to aid the controller in implementing policies and procedures that outline how to handle situations where personal data is used for purposes other than those for which it was originally intended. Under Articles 13 and 14 of the GDPR, the secondary uses of data must be disclosed in information notices (with relevance to Articles 6, 13 and 14 GDPR).⁷⁶⁸

Q: Does the organisation possess the requisite policies and procedures to collect valid consent?

An affirmative response signifies that the organisation has implemented a structured system or procedure to enforce policies and protocols that outline the proper processing of personal data in situations where it is utilised for purposes other than those initially intended. In accordance with the provisions set forth in Articles 13 and 14 of the GDPR, any secondary uses of data must be transparently disclosed in information

⁷⁶⁷ Compliance evidence example: Refer to example evidence under Articles 6, 9, 10, 13, 14, 24 and 32 GDPR.

⁷⁶⁸ Compliance evidence example: Preserving an audit trail of the legal justification (legal basis) behind the processing of personal data.

notices, with due consideration given to TOMs that pertain to Articles 6, 13, and 14 of the GDPR.⁷⁶⁹

Q: Does the organisation integrate data protection and privacy considerations into its data retention processes?

A positive response signifies that the organisation has implemented a systematic approach to safeguard personal data and integrate data protection and privacy into policies and processes for record retention. The controller must establish and implement effective policies and protocols to ensure that personal data is retained in a manner that enables the identification of data subjects for no longer than is necessary for the specific purposes for which it was processed, unless it is being archived for public interest, scientific research, statistical analysis, or historical research purposes.⁷⁷⁰

Implementation of the principle of lawfulness of Processing

Regarding the principle of lawfulness of processing, Article 6 GDPR provides the information on legal grounds for processing personal data, as well as how to determine when further processing is compatible with the original purposes for processing.⁷⁷¹

Legal Basis

Justification for the processing of personal data may be found in the data subject's consent or in the legal permission based on necessity. The former condition is specifically

⁷⁶⁹ Compliance evidence example: (a) Evidence indicating that opt-in consent check boxes or buttons are included in web forms. b) Copies of the consent papers that have been signed. (c) Recordings taken from customer service departments.

⁷⁷⁰ Compliance evidence example: Keeping a schedule and policy in place for the retention of personal data.

⁷⁷¹ See also, Recitals 32, 40-50 GDPR.

mentioned in Article 8 CFR as basis for processing personal data,⁷⁷² and described in Article 4(11) GDPR as a ‘freely given, specific, informed and unambiguous’⁷⁷³ indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.⁷⁷⁴ With respect to the latter condition, ‘legal permission’, it holds relevance in the following scenarios: when the processing is necessary for the performance of a contract, when the processing is necessary to comply with a legal obligation imposed on the controller, when the processing is necessary to protect the vital interests of the data subject or another natural person, when the processing is necessary for the performance of a task carried out in the public interest, or when the processing is necessary for the legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, fundamental rights, or freedoms of the data subject requiring the protection of personal data.

⁷⁷² See Charter of Fundamental Rights, Article 8(2).

⁷⁷³ The term ‘freely given’ refers to the condition where the data subject is able to make a genuine choice without any threat of deceit, coercion, intimidation, or significant negative consequences if they choose not to provide consent. It is considered that there is no real choice for the data subject when they are unable to refuse or withdraw their consent without facing harm. The term “specific” denotes that consent should pertain to the purpose of the processing, which must be precisely defined. It is crucial to obtain consent for all processing activities undertaken for the same or multiple purposes. In the case of multi-purpose processing, consent should be obtained for each of the purposes. Regarding research activities, there may be an exception to the requirement for consent, as it may only be necessary for certain areas of research. The term “informed” implies that the data subject is provided with sufficient information to make an informed decision about the processing operations. It is essential that the information is presented in a clear, concise, and comprehensible manner, to ensure that the data subject comprehends the nature, scope, and implications of the consent. The controller is obliged to provide at least the following information: its identity and the purposes for processing, the possibility of occurrence of data transfer abroad, and its consequences, the categories of data stored and the right to withdraw consent. ‘Unambiguous’ means there can be no doubt that the data subject has consented to the processing operations, therefore, the inactivity on the part of the data subject does not imply consent. Silence, pre-ticked boxes or inactivity are insufficient to demonstrate consent. In relation to cookies and similar technologies, the use of a cookie process will not be considered as consent if, for access or storage of information, the access is granted by a cookie previously stored on the terminal equipment of the user and validated by a pre-checked box that the user must deselect to refuse consent.

⁷⁷⁴ GDPR, Article 4(11).

Q: Is there a system or procedure in place to define the legal grounds for processing personal data, as well as how to determine when further processing is compatible with the original purpose?

A positive response to this query indicates the existence of a systematic approach or methodology employed by the organisation to ascertain the legal grounds for processing individuals' personal data and to comprehensively record the rationale behind such a determination.⁷⁷⁵

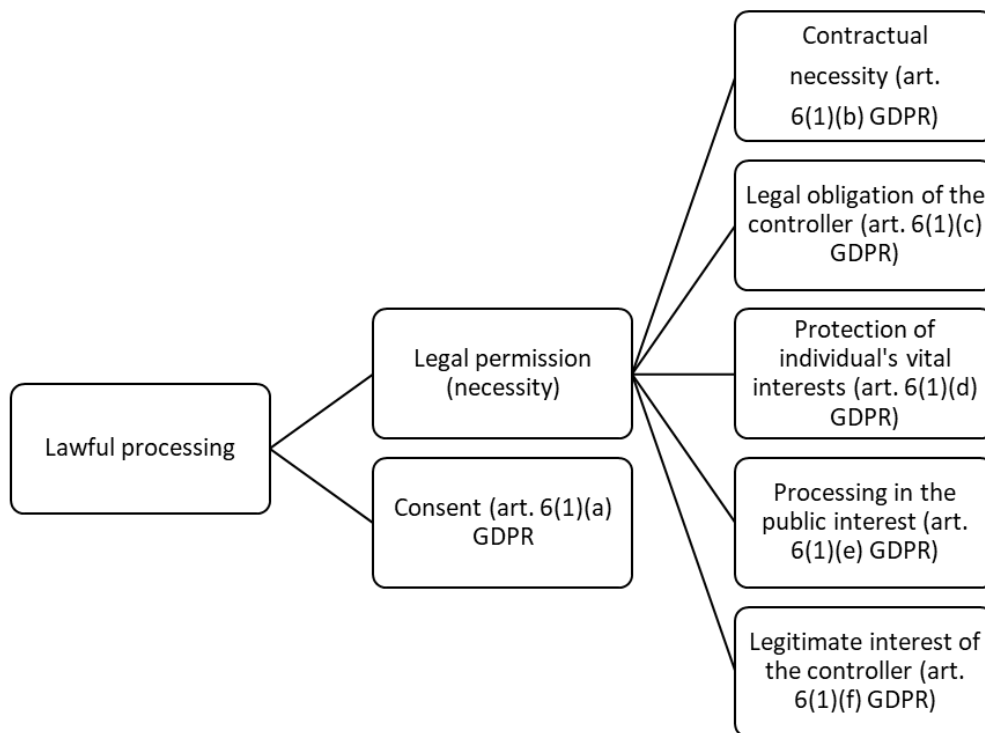


Figure 31 - Lawfulness of processing, Federico Marengo, Data Protection Law in Charts, 2021 (adapted).

Measures

The selection or rejection of suitable TOMs must be contingent upon the evaluation of the processing activity and the relevant legal basis.

⁷⁷⁵ Compliance evidence example: (a) A record of the legal basis for processing personal data, including an explanation of the provided consent, if applicable. (b) DPIAs demonstrating how the data subject's interests or rights and freedoms have been balanced with the data controller's legitimate interests.

In instances where the assessment indicates the employment of consent as the legal basis, due consideration must be given to the consent standard⁷⁷⁶ outlined in Article 7 of the GDPR, which necessitates that consent be demonstrable when utilising it as the legal basis for processing personal data, and explicitly provided when dealing with sensitive personal data.⁷⁷⁷ This requires devising and implementing policies and procedures for obtaining and managing consent, including developing procedures for responding to requests to opt-out, limit, or object to the processing of personal data. For the purpose of accountability, a mechanism should be in place to maintain certain records, such as documentation of opt-in consent, written consent forms, and consent logs in customer relationship management (CRM) platforms. As informed consent must be sought for processing and demonstrated upon request of the data subject or the supervisory authority, it is also necessary to establish a procedure for this requirement, as well as to protect and retain records demonstrating that such consent was collected in accordance with the GDPR standards. TOMs must now be devised and implemented to enable unambiguous consent acquisition, implying that there should be no reasonable doubt regarding the data subject's intention

⁷⁷⁶ See, Article 7(4) GDPR. The presumption of involuntary consent may arise, for instance, when consent is linked to the furnishing of services, and the execution of a contract or the delivery of a service is conditional upon consent. This situation may lead to the processing of personal data that is not indispensable for the fulfilment of the contractual obligations. See also, *Case C-673/17 Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband eV v Planet49 GmbH (Request for a preliminary ruling from the Bundesgerichtshof)* EU:C:2019:801. which interprets consent under the GDPR and ePR to mean that pre-checked checkboxes on consent banners are invalid forms of consent, apart from strictly necessary cookies. Another factor is a clear imbalance between data subjects and controllers; examples include employment - when separate consents for different processing operations are not allowed even though they are appropriate (Recital 43 GDPR). In his Opinion in *Case C-61/19 Orange Romania SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) (Request for a preliminary ruling from the Tribunalul București)* EU:C:2020:901., the Advocate General Spuznar confirms the CJEU's previous position on the strict conditions that must be met in order to use consent as a ground for the processing of personal data under the GDPR.

⁷⁷⁷ See also Recitals 32, 33, 42, 43, 58, GDPR.

to authorise the processing of their personal data.⁷⁷⁸ Where consent is provided as part of a contract, 'safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given'.⁷⁷⁹

Mechanisms for collection of consent

Valid consent may be obtained by oral, written, or electronic means. Written consent must be expressed in an understandable and easily accessible manner, using clear and plain language. If the consent request is part of a document that also contains other matters, the consent request must be clearly distinguishable from the other matters. Any part of such a statement that constitutes a violation of the GDPR does not bind the data subject.⁷⁸⁰

Consent withdrawal and information rights

Moreover, the data subject has the right to withdraw their consent at any time. Thus, before consenting to the processing of their personal data, the individual must be informed that they have this right.⁷⁸¹ Individuals must be able to withdraw consent as easily as they can provide it. In the event of withdrawal of consent, the lawfulness of the processing prior to the withdrawal does not change. The controller may continue to process the personal data of the data subject if they rely on another legal ground for processing, but they must report this situation to the data subject. Furthermore, withdrawing consent implies that the controller can locate and delete the personal information. This can happen during

⁷⁷⁸ It is important to note that inaction on the part of a data subject cannot be construed as consent. For instance, obtaining consent through a privacy policy statement such as "by utilising our service, you provide your consent to the processing of your personal information" will not suffice.

⁷⁷⁹ GDPR, Article 4(11).

⁷⁸⁰ *ibid.*, Article 7(2).

⁷⁸¹ Right also enshrined in Articles 13(2)(c) and 14(2)(d) GDPR.

processing, but it can also happen when data is at rest, such as when it is included in backups and archives. In any case, it is critical to implement appropriate business processes (both technical – e.g., data crawlers, preference centre, and organisational – e.g., SOPs) for validate and execute such withdrawal requests.

Explicit consent

There are certain instances where explicit consent is required, such as when sensitive data is processed,⁷⁸² when personal data is transferred overseas without adequate safeguards,⁷⁸³ or when an automated decision-making process is in place.⁷⁸⁴ The standard is higher than that required for “regular” consent (statement or clear affirmative action). An explicit consent is a form of authorisation that is explicitly stated in writing. In the online setting, this may involve completing an electronic form, sending an email, or providing an electronic signature.

Accountability

A technical and/or organisational measure must be devised and implemented to capture and record consent in a manner that leaves no room for doubt as to whether a data subject has granted consent for the specific processing (e.g., preference centre, consent log). Such consent may be obtained through an opt-in, a declaration, or an active gesture. Although there is no formal requirement for written consent, it is advised due to the controller's accountability. Nevertheless, a distinct scenario emerges concerning children and

⁷⁸² GDPR, Article 9.

⁷⁸³ *ibid*, Article 49.

⁷⁸⁴ *ibid*, Article 22.

adolescents and their consent to the use of information society services. If the data subject is below the age of sixteen, the individual with parental responsibility must provide supplementary consent or authorisation.

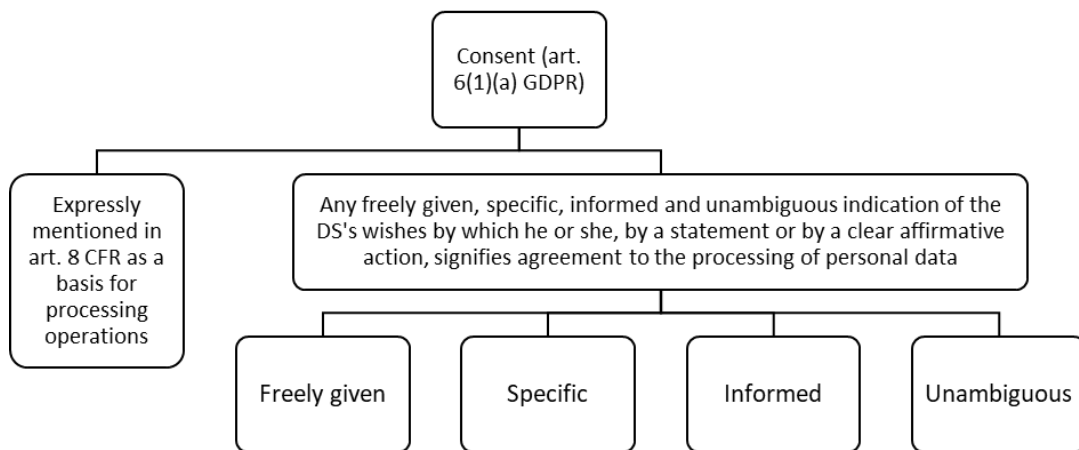


Figure 32 - Consent under GDPR, Federico Marengo, Data Protection Law in Charts, 2021 (adapted).

The following is an example of Q&As that can be used in the gap analysis:

Q: Does the organisation have processes in place to respond to requests to opt-out, restrict, or object to the processing of personal data?

An affirmative response indicates the existence of a mechanism that aids the controller in implementing procedures to verify that records of personal data are used in accordance with any applicable restrictions, including authorisation for uses by the data controller and some limits

for downstream recipients is in place. (Applies to Articles 7, 18 and 21 GDPR).⁷⁸⁵

Q: Does the organisation's use of social media considers the need to protect individuals' personal information and privacy?

An affirmative response to this inquiry indicates the presence of a mechanism that regulates the procedures adopted by the organisation for gathering and disseminating information via social media platforms. With regards to privacy policies pertaining to children and minors, they should encompass the collection and processing of personal data for social networks in adherence to the GDPR's stipulation that the individual possessing parental responsibility for the child must provide consent.⁷⁸⁶

Information society services to minors

Article 8 of the GDPR stipulates that in cases where the legal basis of consent is utilised for providing information society services to minors under the age of 16, consent must be obtained or authorised by the individual with parental responsibility for the child. In addition, the controller must make reasonable efforts to verify the validity of such consent.⁷⁸⁷

⁷⁸⁵ Compliance evidence example: (a) A policy or procedure for responding promptly to requests for restricting the use of personal data. (b) Processes and internal guidelines for analysing and responding to objections from data subjects.

⁷⁸⁶ Compliance evidence example (a) A policy governing the collection and use of personal data as well as listing the measures in place for protecting users' privacy online. (b) The processes that must be followed in order to obtain parental consent and document it. (c) A list of the mechanisms in place to ensure the protection and confidentiality of personal data (d) Guidelines for Social Media Use.

⁷⁸⁷ See also, Recitals 38, 58 GDPR.

Measures

TOMs to incorporate the data protection principles into the organisation's social media practices. This includes the formulation of social network policies that specifically govern the collection and processing of personal data from children and minors, thereby ensuring compliance with the GDPR's stipulation that consent must be obtained from the individual with parental responsibility for the child. A policy and/or procedure to ensure that data subjects receive the necessary specific information when their personal data is collected must also be devised. The scope of the provision specifically refers to the direct provision of information society services to children,⁷⁸⁸ such as marketing or the creation of online personal profiles for children.⁷⁸⁹ It also includes services that are not directly financed by the users, such as those provided by 'free' online services funded by advertising. This provision and requirement were developed on the premise that children require extra protection because they may be less aware of the risks, consequences, safeguards, and their rights in relation to the processing of their personal data.⁷⁹⁰ In general, when selecting the appropriate TOMs, the following guidelines ought to be adhered to: the processing of personal data of a child is lawful if the child is at least 16 years old;⁷⁹¹ for those under 16, such processing is only permitted with the consent or authorisation of the parent or guardian;⁷⁹² if preventive or counselling services are offered directly to a child, the consent of the holder of parental responsibility should not be required;⁷⁹³ member states shall not

⁷⁸⁸ GDPR, Article 8(1).

⁷⁸⁹ *ibid*, Recital 38.

⁷⁹⁰ *ibid*.

⁷⁹¹ GDPR, Article 8(1).

⁷⁹² *ibid*.

⁷⁹³ GDPR, Recital 38.

establish an age for those purposes lower than 13 years old;⁷⁹⁴ and the controller shall use reasonable efforts, based on technology available, to verify that the holder of parental responsibility has authorised or granted consent.⁷⁹⁵

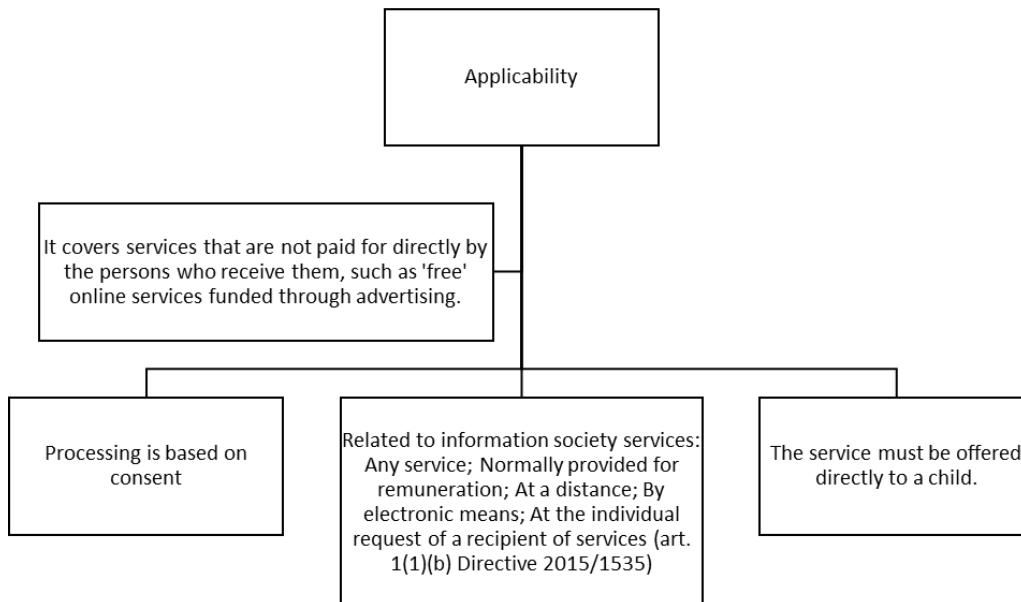


Figure 33 - Conditions applicable to child's consent, Federico Marengo, Data Protection Law in Charts, 2021 (adapted).

Q: Is the organisation's policy and procedure for collecting and using personal data from children and minors in place?

A positive response to this query suggests the existence of a system or process that aids the organisation in guaranteeing that consent or authorisation is provided by the individual possessing parental responsibility.⁷⁹⁶

⁷⁹⁴ GDPR, Article 8(1).

⁷⁹⁵ Article 8(2) GDPR.

⁷⁹⁶ Compliance evidence example: A parental consent policy or procedure, as well as documentation of the technology used to obtain parental consent.

Special categories of data

Sensitive information,⁷⁹⁷ referred to as special category data, encompasses personal information related to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data, data concerning health or sex life, and sexual orientation. Article 9 of the GDPR imposes a broad restriction on the processing of special categories of personal data, accompanied by an enumeration of legal justifications that authorise the processing of such categories of personal data.⁷⁹⁸

Measures

TOMs must be devised and implemented to limit the processing of special category data, except in the following instances: where explicit consent has been obtained; for fulfilling employment, social security, and social protection requirements; to protect the vital interests of a natural person in cases where obtaining consent is impossible; for legitimate activities of non-profit organisations pursuing political, philosophical, religious, or trade union objectives; where the data subject has publicly disclosed the data; for the establishment, exercise, or defence of legal claims; for reasons of substantial public interest; for preventative or occupational medicine, assessing worker capacity, medical

⁷⁹⁷ PbDD places particular emphasis on the handling of special categories of personal data, to such an extent that the Regulation imposes additional obligations on controllers and requires organisations to exercise particular care in managing these sensitive data items. The term "sensitive" was intentionally chosen to emphasise that certain types of data, which do not fall under the category of "special category" as defined by the GDPR, can still pose a significant risk to data subjects due to its sensitive nature. This situation highlights the inconsistency in the classification of personal data. The primary issue at present is whether "sensitive" data should also be considered as "special category" data. The lack of clarity in this regard creates a sense of uncertainty for organisations as they strive to comply with their legal obligations under the GDPR. The data types to which I refer, such as credit card information, social security numbers, passport numbers, national identification numbers, and system access passwords, necessitate a higher degree of safeguarding than ordinary personal data, contingent on the processing context.

⁷⁹⁸ See also Recitals 51-56 GDPR.

diagnosis, provision of health or social care, or managing health or social care systems and services; or for reasons of public interest in areas of public health, scientific or historical research, or statistical purposes. A policy and/or procedure to govern the collection and utilisation of sensitive personal data is necessary. These measures are intended to guarantee that special categories of personal data are exclusively processed in adherence to the legal exceptions outlined in Article 9 of the GDPR. Additionally, the controller must establish mechanisms for documenting the processing of special categories of personal data to ensure accountability, which may incorporate the Records of Processing Activities (ROPA).

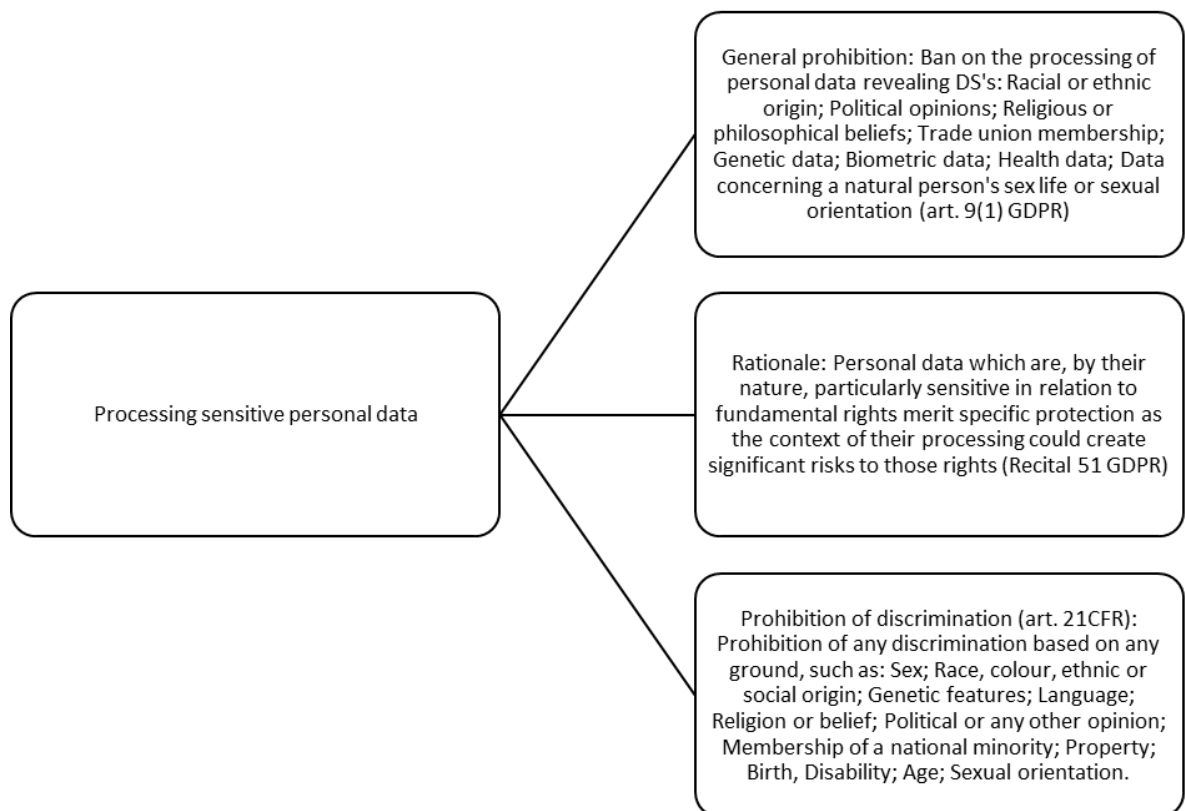


Figure 34 - Processing special categories of personal data, Federico Marengo, Data Protection Law in Charts, 2021 (adapted).

Q: Is the organisation's policy and procedure for collecting and using sensitive personal data up to date?

A positive response to this inquiry signifies the existence of a system or process that aids the controller in devising policies and procedures to ensure that special categories of personal data are solely processed in accordance with Article 9 GDPR.⁷⁹⁹

Data related to criminal convictions and offences

Article 10 of the GDPR outlines the legal bases that justify the processing of personal data pertaining to criminal convictions and offences while also imposing restrictions on such processing. The controller may only process criminal offence data if it is regulated by an official authority or authorised by domestic law. Processing criminal offence data, especially on a large scale, can have consequences for other obligations of controllers, such as documentation, DPIAs, and the designation of a Data Protection Officer (DPO).

Measures

TOMs for documenting the legal basis for processing data associated with criminal convictions and offences. This mechanism should clarify how the organisation determines the legal basis for processing and ensure that a record of this analysis is retained. In this regard, the creation of a personal data inventory and an organisational procedure for

⁷⁹⁹ Compliance evidence example: (a) An organisational policy for the processing of special categories of personal data. (b) A template to assist the organisation in classifying data. (c) A register of consent forms or consent evidence. (d) Collective bargaining agreements outlining how sensitive employee data will be handled. (e) Evidence that certain types of personal information were obtained from a publicly accessible source. (f) A privacy policy outlining how specific types of personal data are handled.

conducting background checks are crucial tasks that require completion. The personal data inventory should encompass details related to criminal convictions and offences, such as the identification of the legal authority, as a matter of accountability. This information can subsequently be incorporated into the organisation's ROPA.

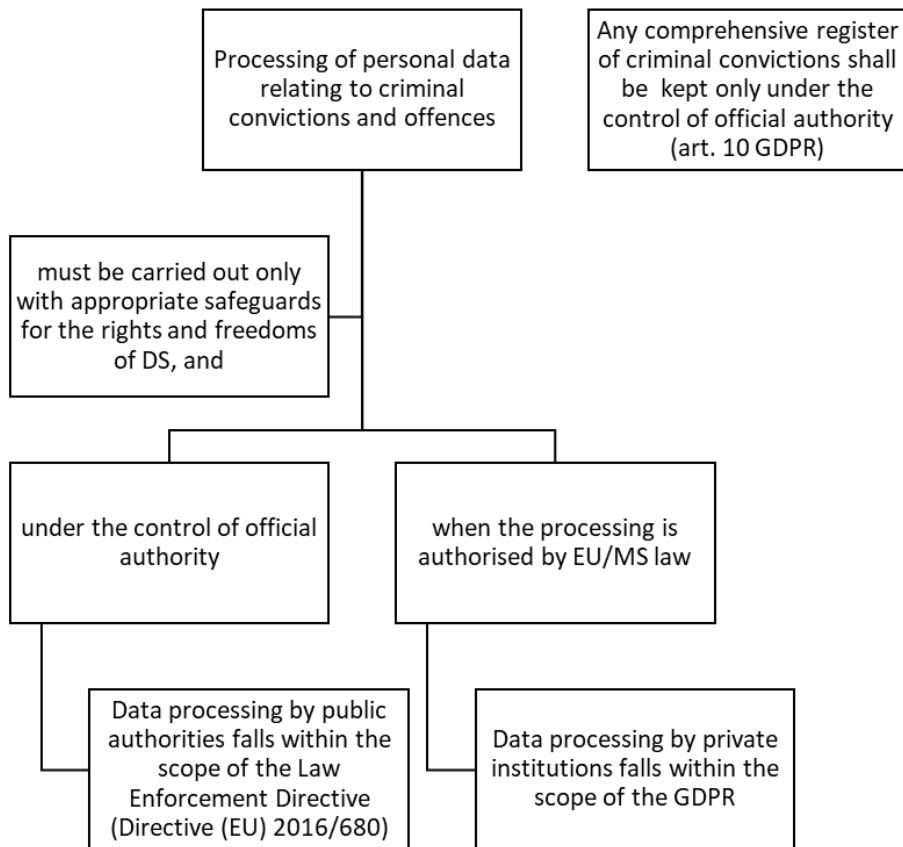


Figure 35 - Processing of personal data relating to criminal convictions and offences, Federico Marengo, Data Protection Law in Charts, 2021 (adapted).

Application of DPPA

This section of the DPPA pertains to Chapter II of the GDPR, which is primarily focused on the implementation of the data protection principles delineated in Articles 5 through 11 of the Regulation. The following Chapter delves into the DPPA measures concerning the rights of data subjects and provides an "Article-by-Article" approach to the implementation of

the GDPR through a detailed analysis of each Article and outlining the necessary measures for compliance.

Chapter 9 – DPPA (Part II): The roadmap for GDPR compliance

Introductory notes

The DPPA presented in this study serves as a useful tool for identifying the specific GDPR Articles that require operational action by the data controller. Furthermore, the DPPA provides a structured approach for the creation of a data protection program, which is based on the effective implementation of data protection principles and mechanisms that uphold data subject rights through PbDD. In addition, provides a list of TOMs that can aid data controllers in demonstrating compliance and accountability.

9.1. Managing data subject rights through PbDD

Transparent information, communication, and modalities for the exercise of the rights of the data subject

Data controllers are obliged to provide information to data subjects in a clear, concise, transparent, and easily accessible manner using simple and understandable language.

An overview of appropriate TOMs⁸⁰⁰

To facilitate data subject rights, TOMs must be implemented, including the ability to respond to requests within a timely manner, verifying the identities of data subjects, and assessing relevant fees if necessary. Privacy notices should include standardised icons to provide an overview of processing activities, and organisations must establish and maintain

⁸⁰⁰ See also GDPR Recitals 58-60.

data protection policies, notices, and procedures. The data protection notice should include a placement log indicating the timing and revisions of the notice to promote accountability. To comply with Article 12 of the GDPR, organisations must have a workflow for responding to requests, templates for communication with data subjects, and policies for collecting and using data from children and minors. Verification mechanisms must be in place for fully or partially automated processing, and notification procedures should be established for individuals affected by a data breach and supervisory authorities. Figure 37 provides a summary of the requirements stipulated in Article 12 of the GDPR.

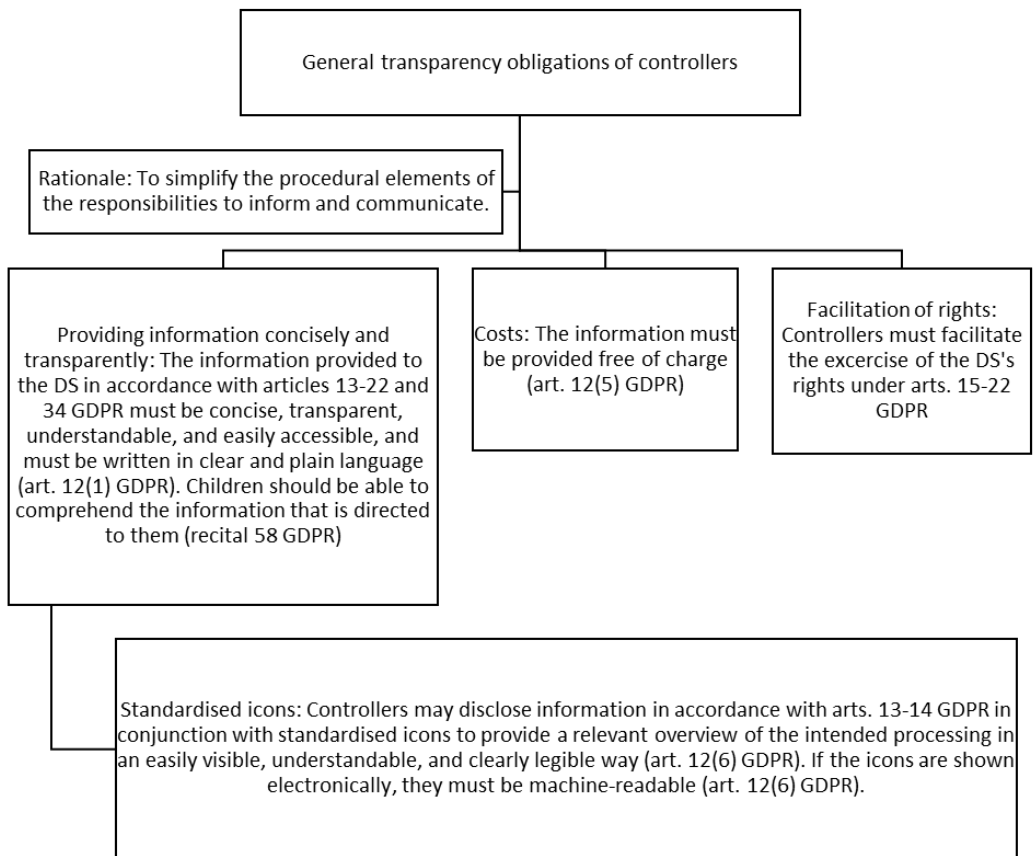


Figure 36 - General transparency obligations of the data controllers, Federico Marengo, Data Protection Law in Charts, 2021 (adapted).

Information to be provided where personal data are collected from the data subject

Article 13 GDPR requires data controllers to provide certain minimum information to data subjects via an information notice. It also sets out the timing requirements for notification and when exemptions may apply.⁸⁰¹

Measures

It is essential to implement TOMs that guarantee data subjects receive the necessary information when their personal data is collected. These measures should include the development of mechanisms that make this information available at every point where personal data is collected, including the provision of a hyperlink to the privacy policy. The privacy policy should contain comprehensive information about the potential secondary use of personal data. To ensure complete coverage, a script should be developed for phone conversations that result in the collection of personal data, such as those conducted by sales departments or customer support, and it should reflect the measures stipulated under Article 12 of the GDPR. The following gap Q&A will aid the data controller in identifying and implementing the most appropriate TOMs:

Q: Does the organisation maintain a privacy notice?

If the answer to this question is yes, it indicates that the organisation has established a system or process that enables them to fulfil their obligations under Articles 8, 13, and 14 of the GDPR. This system or process should ensure that data subjects receive the appropriate information at the time of their personal data collection.⁸⁰²

⁸⁰¹ See also Recitals 60-62 GDPR.

⁸⁰² Compliance evidence example: In addition to a copy of the privacy notice provided to data subjects, documentation demonstrating that the privacy notice complies with legal requirements.

Information to be provided where personal data have not been obtained from the data subject

Article 14 GDPR, requires data controllers provide certain information to data subjects when personal data is not collected directly from them.

Measures

The operational actions required are similar to those described in Article 12 of the GDPR.

To identify the most suitable TOMs, data controllers can address the following gap Q&A:

Q: Is a privacy notice provided at all points where the organisation collects personal data?

Within the context of Articles 13 and 14 of the GDPR, an affirmative response to this inquiry indicates the existence of a system or procedure that governs how organisations provide privacy notices to data subjects during the data collection process. Compliance with both Articles 13 and 14 of the GDPR necessitates a proactive approach on the part of the data controller, and it is not contingent upon a request from the data subject. It is crucial to acknowledge that fulfilling these obligations represents a fundamental aspect of data protection law, as it serves to empower data subjects by providing them with the necessary information to make informed decisions about their personal data.⁸⁰³

⁸⁰³ The ICO recommends that in providing privacy information to individuals, organisations should utilise a number of appropriate techniques, including: a layered approach (Brief privacy notices with additional layers of detail); dashboards (Management tools explain how organisations utilize their data, and allow them to control what happens to that data); just-in-time notices (Privacy information containing relevant and focused information is delivered when the data controller collects specific pieces of personal information); icons (Small, meaningful symbols that signal the existence of a particular type of data processing); and mobile and smart device functionality (A variety of methods are available, including pop-ups, voice-alerts, and gestures on mobile devices).

The diagram presented below serves to depict the responsibilities of data controllers according to Articles 13 and 14 of GDPR in notifying data subjects whether their personal data has been obtained directly from them or not.

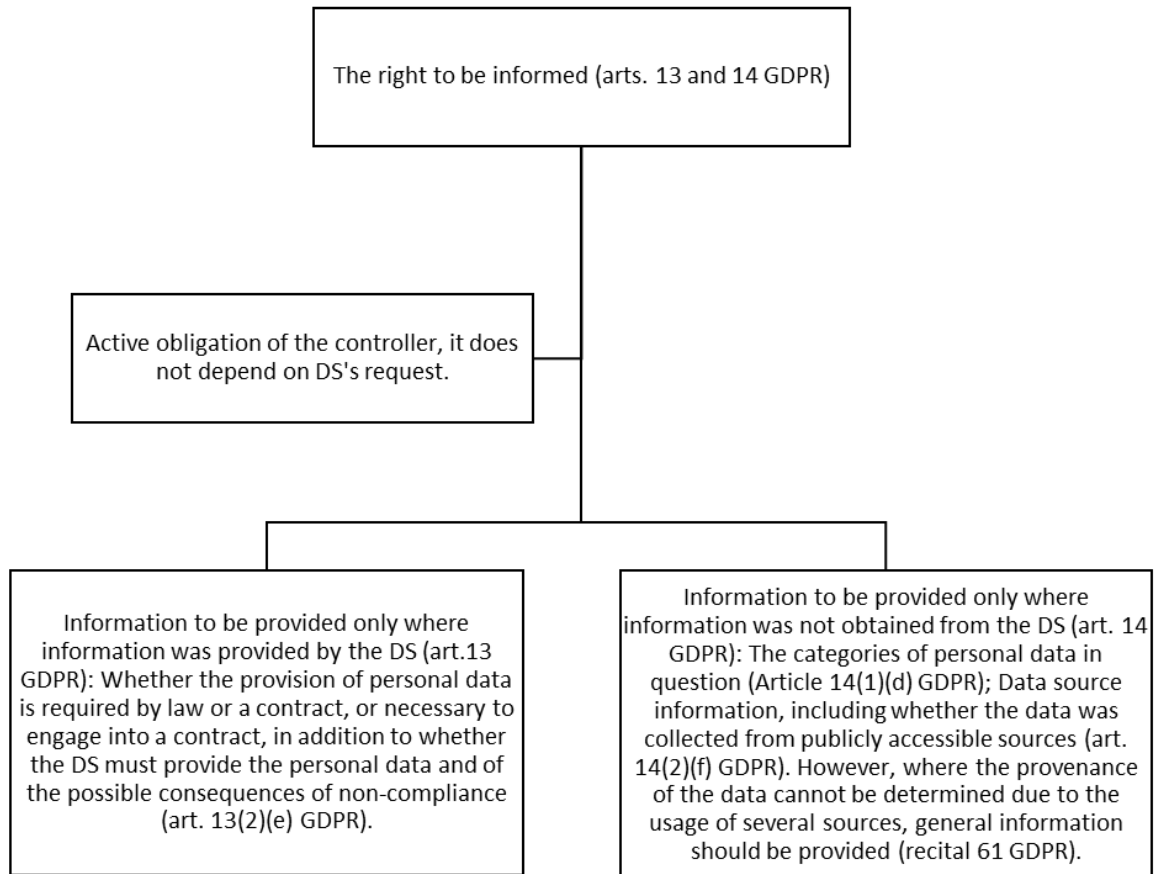


Figure 37 - The right to be informed, Federico Marengo, Data Protection Law in Charts, 2021 (adapted).

The GDPR gives data subjects several rights in relation to their personal data. However, due to variations in the reasons for which data controllers collect personal data, individuals may not always be able to exercise all of the rights provided under the GDPR. Thus, it is necessary to outline specific TOMs within the PbDD plan, and to uphold them throughout the personal data life cycle.

Right of access by the data subject

Article 15 GDPR addresses the right of data subjects to obtain confirmation as to whether or not their personal data is being processed, where it is being processed, and how they can access their data.⁸⁰⁴ It also incorporates a list of supplementary details that ought to be provided to individuals whose data is being processed. These include the objective of processing, the types of data being processed, the recipients of the data, the length of time the data will be retained, the right to rectify and lodge complaints, the sources of the data, the deployment of automated processing (including profiling), the associated rationale, and any safeguards in place for transferring data to third-party countries or international organisations.⁸⁰⁵ This is a fundamental right to personal data protection under Article 8(2) CFR and a critical aspect of data protection law,⁸⁰⁶ which is to be regarded as an active right of the data subject, whereby the controller is obliged to comply with the data subject's request. To that end, measures must be put in place to make access to personal data easy to obtain and granted at reasonable intervals.⁸⁰⁷

The data controller must consider that in relation to the provision of personal data, Article 15(3) GDPR requires organisations to provide a copy of the personal data being processed. When a data subject requests information electronically, the information should be provided in a commonly used electronic form, unless otherwise requested. Furthermore, where possible, the controller must allow direct access to the data subject's personal data

⁸⁰⁴ See also Recitals 63, 64 GDPR.

⁸⁰⁵ Article 12 GDPR also addresses the costs and timeframe for exercising this right.

⁸⁰⁶ See *Joined Cases C-141/12 and C-372/12 YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S* EU:C:2014:2081. See also *Case C-615/13 P ClientEarth and Pesticide Action Network Europe (PAN Europe) v European Food Safety Authority* EU:C:2015:489.

⁸⁰⁷ GDPR, Recital 63.

via a secure system that is accessible remotely.⁸⁰⁸ Responses to individuals' requests are free; however, any additional copies may be charged at a reasonable fee based on the controller's administrative costs.⁸⁰⁹ Nevertheless, such fees should not be greater than the costs of communicating such information.⁸¹⁰

Measures

TOMs must be implemented to verify the identity of a data subject requesting access, particularly in the case of online services and online identifiers.⁸¹¹ Sometimes, access restrictions need to be considered, for example, because the right to obtain a copy of an individual's personal data should not compromise the rights and freedoms of others,⁸¹² this would include trade secrets, intellectual property, and in particular the copyrights protecting software.⁸¹³ However, these considerations should not lead to a refusal to provide all information to the data subject.⁸¹⁴ If the controller processes a large amount of personal information about an individual, it may request that the individual identify the specific information or processing activities to which the request refers.⁸¹⁵ Another aspect to address is how to strike a balance between the principle of storage limitation and the right of access. Data controllers are advised not to hold on to data solely for the purpose

⁸⁰⁸ *ibid.*

⁸⁰⁹ GDPR, Article 15(3).

⁸¹⁰ *Case C-486/12 X, Request for a preliminary ruling from the Gerechtshof te 's-Hertogenbosch EU:C:2013:836.*

⁸¹¹ GDPR, Recital 64.

⁸¹² *ibid.*, Article 15(4).

⁸¹³ *Ibid.*, Recital 63.

⁸¹⁴ *ibid.*

⁸¹⁵ *ibid.*

of fulfilling individual requests.⁸¹⁶ Paradoxically, the right to access should not be excessively curtailed by constraints on time.⁸¹⁷ Consequently, any measures to comply with the requirements of Article 15 of the GDPR must include the implementation of systems, policies, and procedures that cater to requests for personal data access, with particular focus on the following aspects: the deployment of mechanisms and systems for locating and retrieving personal data from an organisation's ecosystem (e.g., crawlers, spiders, SQL scripts, etc.); the establishment and maintenance of internal procedures and systems to manage related activities (e.g., updating website forms, scripts, etc.); and the development and sustenance of suitable communication systems to keep individuals informed of the status of their personal data. Documentation such as an individual's access request log, as well as procedures (and workflows) for responding to data subject requests, should be maintained as proof of compliance and accountability.

Q: Are the organisation's procedures for responding to requests for access to personal data in place and routinely maintained? Can individuals access information from the organisation on how to update or amend their personal data? Does the organisation maintain response processes for these requests?

If the response to the aforementioned inquiries is affirmative, it indicates that the organisation has implemented a system or process to promptly and efficiently respond to data subject access requests. The implementation of such practices represents an effective approach to

⁸¹⁶ GDPR, Recital 64.

⁸¹⁷ *Rijkeboer [2009]* (n 93).

demonstrating a comprehensive understanding and adherence to access rights.⁸¹⁸

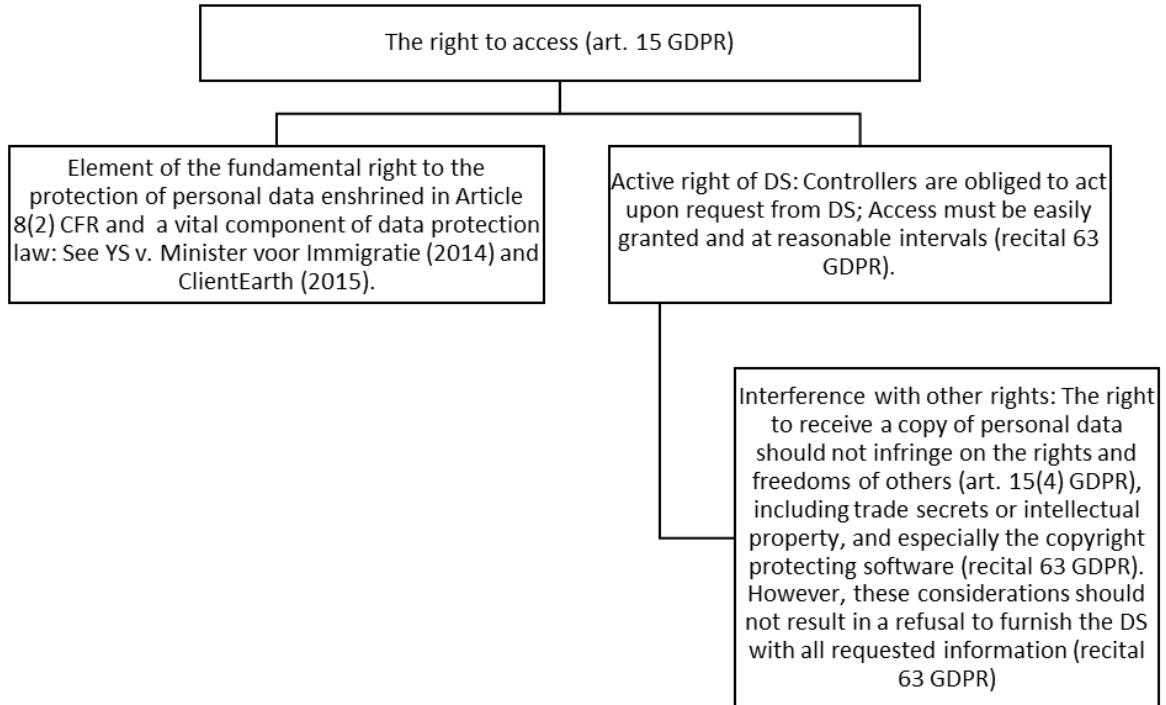


Figure 38 - The right to access, Federico Marengo, Data Protection Law in Charts, 2021 (adapted).

Right to rectification

Article 16 of the GDPR deals with the entitlement of data subjects to request rectification of incorrect data or completion of incomplete data.⁸¹⁹ This right is inherently linked to the principle of accuracy,⁸²⁰ which mandates that personal data must be accurate and up to date, the right to effective legal protection provided by Article 47 of the Charter of Fundamental Rights (CFR),⁸²¹ and the right to access,⁸²² given that access to personal data

⁸¹⁸ Compliance evidence example: (a) A mechanism for promptly responding to access requests. b) A form for collecting extra information regarding the access request. (c) Documentation and logs of access requests.

⁸¹⁹ See also, Recital 65 GDPR.

⁸²⁰ GDPR, Article 5(1)(d).

⁸²¹ *Schrems [2015]* (n 211).

⁸²² GDPR, Article 15.

is a prerequisite for its eventual rectification.⁸²³ The data subject has the right to have their personal data rectified if inaccurate personal data is processed; or completed if incomplete personal data is retained. In the context of operational PbDD actions, it is crucial to acknowledge that it is the responsibility of the data controller to correct inaccurate data or complete incomplete data promptly, and to take all necessary steps to guarantee such rectification⁸²⁴ while communicating solely accurate and complete information about the data subject.⁸²⁵ It is pertinent to note that a supervisory authority has the power to issue an order for data rectification.⁸²⁶

Measures

TOMs must be implemented to establish and maintain mechanisms and procedures to respond to rectification requests and providing a mechanism for individuals to update or correct their personal data (e.g., online portal). These measures may entail the use of technology to meet a range of functional requirements, such as searching, editing, and extending stored data, as well as identifying, authenticating, accessing, and validating information. They must also address backup and archive copies; thus, retaining individual request logs (including online portal access) and internal procedures for responding to data subjects' requests for personal data rectification as evidence of compliance and accountability is essential. Moreover, the controller must communicate any correction or completion of personal data to each recipient to whom the data has been disclosed and

⁸²³ See, *Schrems [2015]* (n 211). See also, *Case C-434/16 Peter Nowak v Data Protection Commissioner EU:C:2017:994*.

⁸²⁴ GDPR, Recital 39.

⁸²⁵ See, *Cemalettin Canlı v Turkey, App no 22427/04, (ECtHR, 18 November 2008)*.

⁸²⁶ GDPR, Article 58(2)(g).

must inform the data subject about these recipients upon request.⁸²⁷ This obligation does not apply if it proves impossible or requires disproportionate effort.⁸²⁸ Hence, it is appropriate to assess disproportionate efforts according to the time, cost, and manpower involved in the completion of the task.⁸²⁹

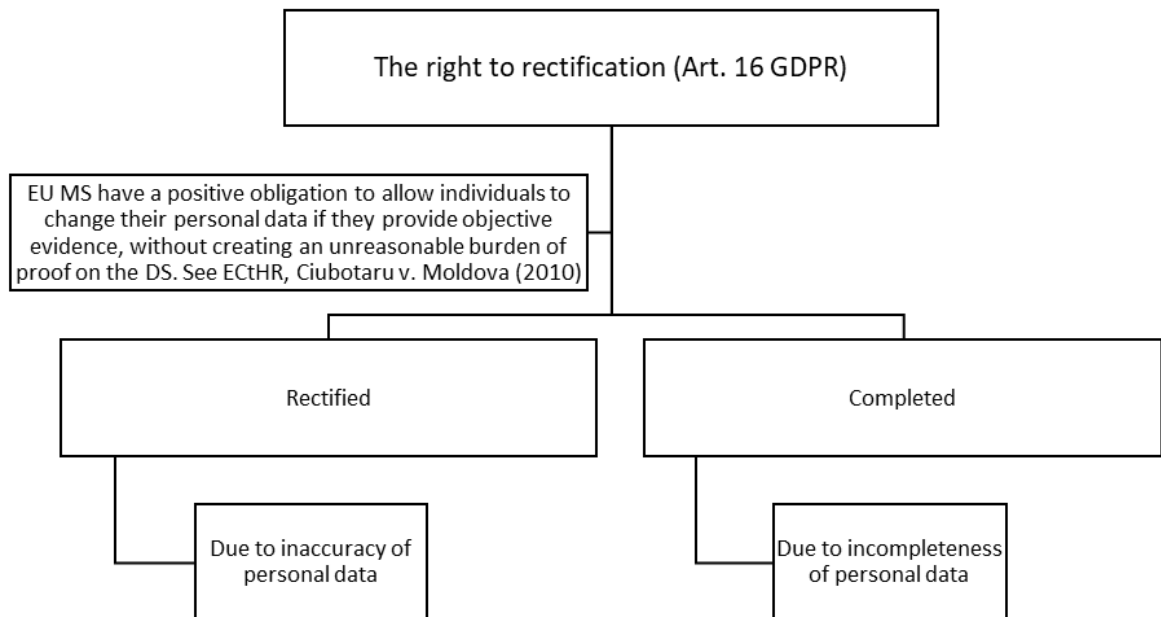


Figure 39 - The right to rectification, Federico Marengo, Data Protection Law in Charts, 2021 (adapted).

Right to erasure ('right to be forgotten')

Article 17 GDPR approaches the right of data subjects to obtain the erasure of their personal data from the data controller on the following grounds: (a) data is no longer required for processing; (b) consent has been withdrawn; (c) there is an objection to the processing; (d) data has been processed unlawfully; (e) as a result of compliance with a

⁸²⁷ GDPR, Article 19.

⁸²⁸ *ibid.*

⁸²⁹ *Breyer [2016] (n 277).*

legal obligation; (f) and where data is collected about children and minors in relation to an information society service.⁸³⁰ It should be noted that there are some exceptions to the right to be forgotten; there are certain circumstances in which the erasure of personal data does not apply, namely, for exercising the right to freedom of expression and information;⁸³¹ where the processing is necessary to comply with a legal obligation imposed by EU or a member state law to which the controller is subject;⁸³² for performance of a task in the public interest or pursuant to the controller's official authority;⁸³³ for reasons of public interest in the field of public health;⁸³⁴ for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, if the deletion of the data would seriously impair the accomplishment of the objectives of the processing;⁸³⁵ and for the establishment, exercise or defence of legal claims.⁸³⁶

Measures

The TOMs must address the implementation and maintenance of mechanisms for responding to requests for erasure of personal data (i.e., data erasure or anonymisation) in a timely and effective manner. This operational action is similar to that applied to the right of rectification and requires the application of various functional requirements, such as identifying stored data, authenticating, accessing, and erasing the data. This process may also impact data in rest, including backups and archive copies of personal data. The

⁸³⁰ See also, Recitals 65, 66 GDPR.

⁸³¹ GDPR, Article 17(3)(a).

⁸³² *ibid.*

⁸³³ GDPR, Article 17(3)(b).

⁸³⁴ *ibid.*, Article 17(3)(c).

⁸³⁵ *ibid.*, Article 17(3)(d).

⁸³⁶ *ibid.*, Article 17(3)(e).

implementation and maintenance of appropriate communication systems to handle requests for data erasure should also be taken into consideration. Data erasure can be achieved through deletion, anonymisation, or in certain cases by "putting data beyond use".⁸³⁷ Individual request logs (including, if applicable, online portal access logs) and procedures for responding to data subjects' requests for personal data erasure should be kept as evidence of compliance and accountability. Another aspect that needs to be considered is the notification obligation regarding erasure of personal data, namely, (i) to other controllers; where the controller has made the personal data public, it is the data controller's responsibility to erase the personal records, as well as to take reasonable steps, including any technical measures (taking into account available technology and the cost of implementing such measures) to notify other relevant controllers of the individual's request, in order to have all links to, or copies of, those personal data erased,⁸³⁸ and (ii) to recipients; controllers must notify each recipient to whom personal data has been disclosed of any erasure of personal data.⁸³⁹ Furthermore, upon request, the controller must inform the data subject about those recipients.⁸⁴⁰ However, this obligation does not apply if it proves impossible or requires disproportionate effort.⁸⁴¹ Again, disproportionate

⁸³⁷ See ICO's guidance on deleting personal data, <https://ico.org.uk/media/for-organisations/documents/1475/deleting_personal_data.pdf>. The process of rendering data 'beyond use' comprises four key elements. Firstly, it involves taking measures to ensure that the organisation will neither use nor utilize the personal data to influence decisions relating to individuals or in any way that might impact the affected individuals. Secondly, it entails refraining from granting any other party access to the personal data. Thirdly, it requires that the personal data is protected at all times using appropriate technical and organisational security measures. Finally, a commitment must be made to delete the personal data as and when this becomes feasible.

⁸³⁸ GDPR, Article 17(2).

⁸³⁹ GDPR, Article 19.

⁸⁴⁰ *ibid.*

⁸⁴¹ *ibid.*

efforts should be evaluated in terms of time, cost, and manpower involved in the completion of the task.

A mention must be made to the right to request delisting or de-referencing; in general, the right to request delisting refers to the Article 17 GDPR right to be forgotten in relation to search engines. This implies that the right to erasure extends to controllers who replicate data on the internet.⁸⁴² If an individual requests the delisting of a particular content, this will result in the deletion of that specific content from the list of search results concerning the data subject when the search is, as a main rule, based on his or her name.⁸⁴³ However, a delisting request does not mean that personal data are completely erased, since the data will not be deleted from the source website nor from the index and cache of the search engine provider.⁸⁴⁴

Q: Does the organisation manage requests for data erasure? (Right to be forgotten)

A positive response to this inquiry indicates that the organisation employs a mechanism or process that facilitates the execution of erasure request evaluation processes, as well as any supplementary actions required upon approval of a request. (This applies to Articles 17 and 19 GDPR).⁸⁴⁵

⁸⁴² *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (2014)* (n 69).

⁸⁴³ Search engine operators are obligated to remove disputed links only from versions of their search engine that correspond to EU member countries, without extending this requirement globally. Therefore, there is no global territorial scope for the removal of such links. See, *Case C-507/17 Google LLC successor in law to Google Inc v Commission nationale de l'informatique et des libertés (CNIL) EU:C:2019:772*.

⁸⁴⁴ EDPB, 'Guidelines 5/2019 on the Criteria of the Right to Be Forgotten in the Search Engines Cases under the GDPR (Part 1)' (7 July 2020) <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-52019-criteria-right-be-forgotten-search-engines_en>.

⁸⁴⁵ Compliance evidence example: A record of the procedure or system used to respond to requests for the right to be forgotten (including communications).

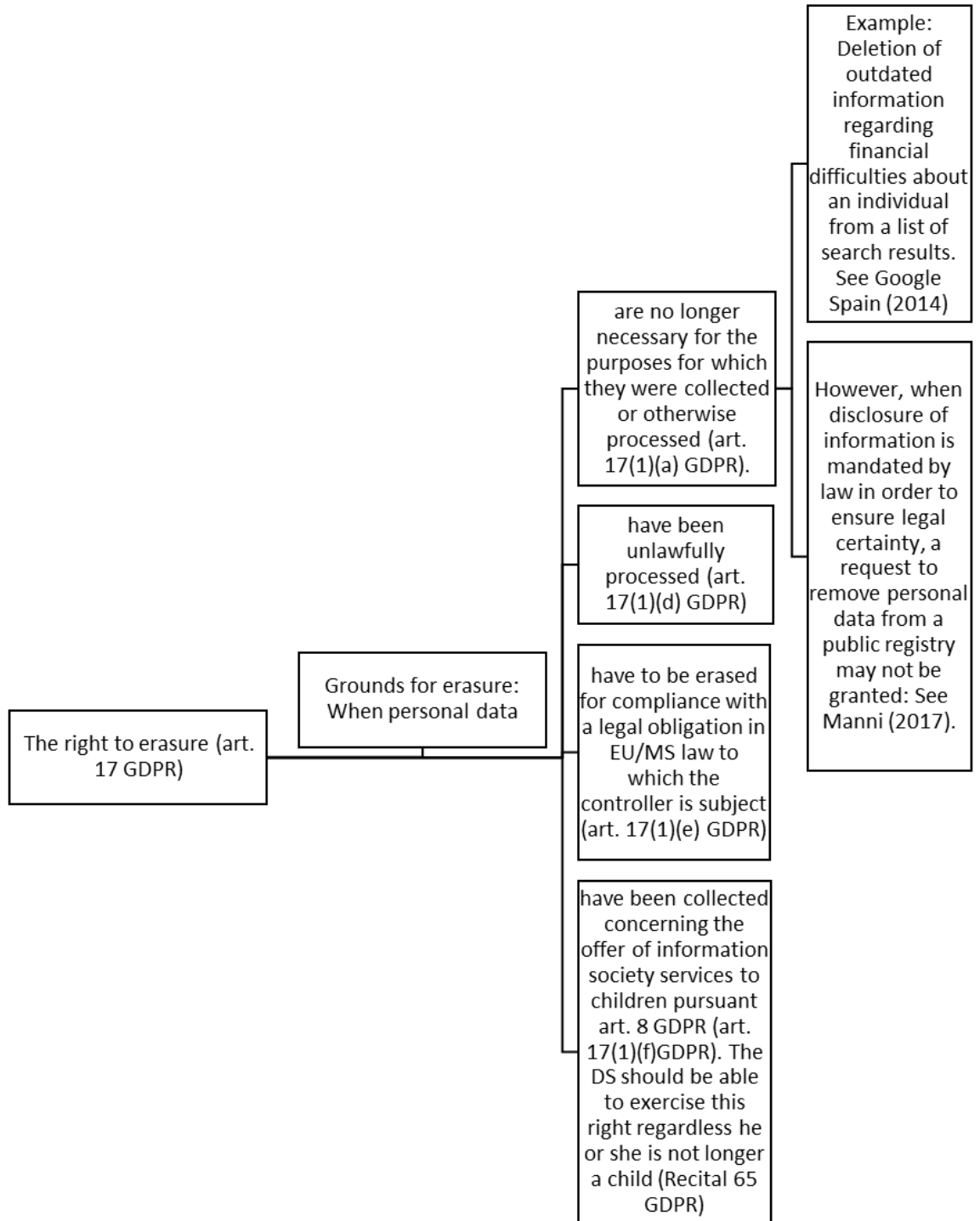


Figure 40 - The right to erasure, Federico Marengo, Data Protection Law in Charts, 2021 (adapted).

Right to restriction of processing

Article 18 GDPR addresses a data subject's right to obtain a restriction (limiting future processing)⁸⁴⁶ on the processing of personal data in situations where, inter alia, a legal basis for the processing is outstanding or the accuracy of the data is contested (as an example, upon withdrawal of consent by the data subject, there is no legal basis for the processing).⁸⁴⁷ It is important to note that there are no overriding legitimate reasons for the processing when the data subject objects to the processing⁸⁴⁸ and it is also possible for a supervisory authority to order the rectification or erasure of data.⁸⁴⁹

Measures

TOMs to address the right to restriction of processing could be, for example, the deployment of technology for address the requests for processing restriction in a timely and effective manner – this PbDD action entails considering the functional requirements, such as identifying stored data as well as authenticating, accessing, and blocking further processing of personal data. This may also impact data backups and archive copies. Processing can be limited by putting data out of use, for example, by changing file attributes at the operating system level. Individual request logs (including, if applicable, online portal access) and procedures for responding to data subjects' requests for processing restriction should be kept as evidence of compliance and accountability.

⁸⁴⁶ See also, Recital 67 GDPR.

⁸⁴⁷ GDPR, Article 17(1)(b).

⁸⁴⁸ *ibid*, Article 17(1)(c).

⁸⁴⁹ *ibid*, Article 58(2)(g).

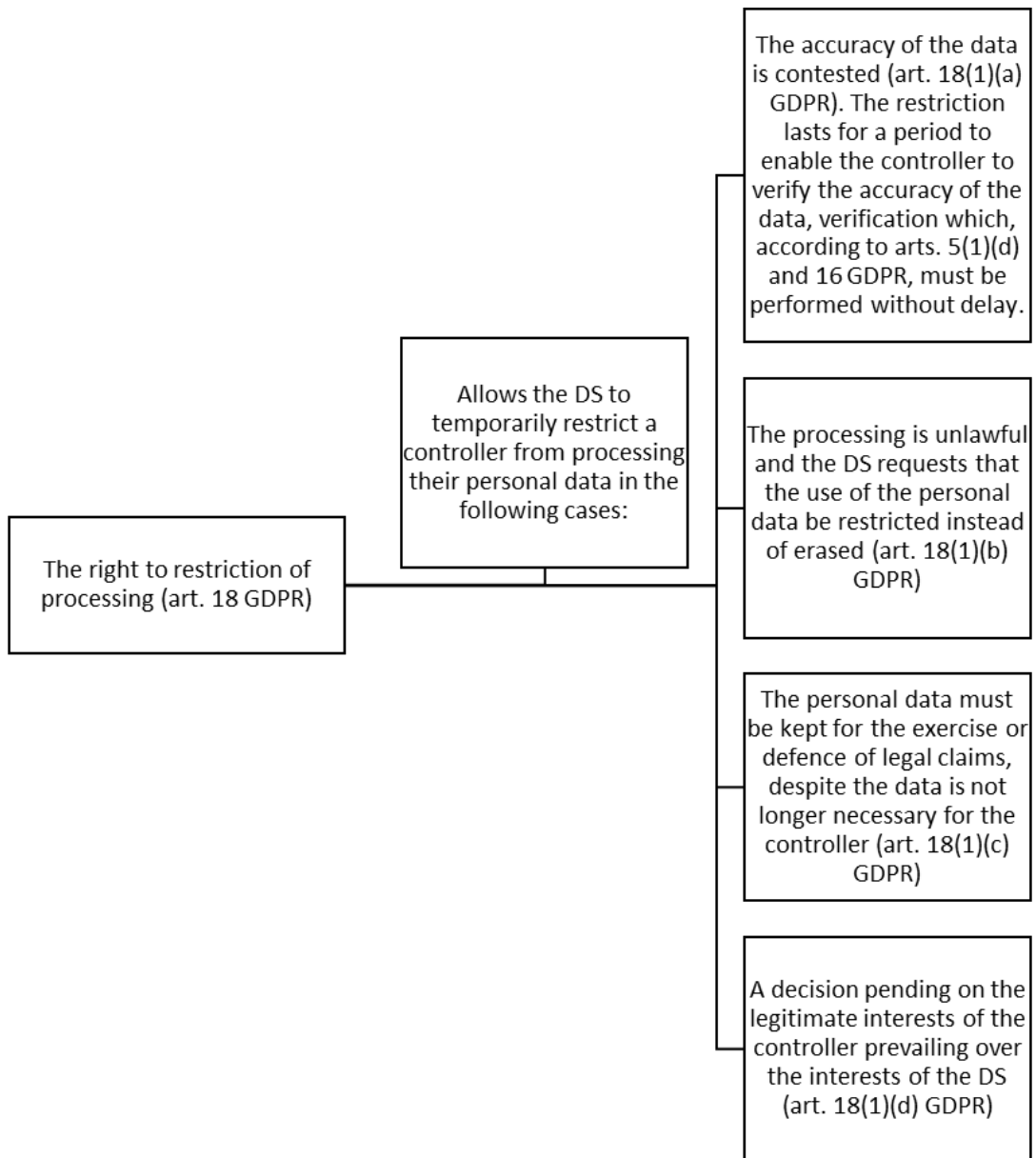


Figure 41 - The right to restriction of processing, Federico Marengo, Data Protection Law in Charts, 2021 (adapted).

Notification obligation regarding rectification or erasure of personal data or restriction of processing

Article 19 GDPR translates into a requirement to notify each recipient to whom personal data has been disclosed of any rectification, erasure, or processing restriction. There is also an obligation to provide the data subject with information about these recipients upon

request. Such notification is not required if it is impossible or requires disproportionate effort.⁸⁵⁰

Measures

TOMs to incorporate and maintain procedures to respond to data subjects' requests, such as providing a mechanism for individuals to update or correct their personal data, enabling timely and effective corrections to personal data records. Additionally, procedures must be in place for responding to requests to opt-out of, restrict, or object to processing. Such procedures will facilitate appropriate corrections to personal data records, including those records held not only by the data controller but also by recipients such as processors or joint controllers. Lastly, procedures for responding to requests to be forgotten or for erasure of data must also be developed and maintained, ensuring that personal data is deleted upon request in a timely and effective manner. To demonstrate compliance and accountability, the controller must also put in place mechanisms that provide accurate data mappings (data inventories) as well as data flow charts, which include transfers of personal data to third parties and countries (for example, ROPA). The establishment of mechanisms for responding to data subject requests, such as an individual's rights portal, and the maintenance of a comprehensive log of communication with data subjects represent essential measures to ensure compliance with GDPR standards.

Right to data portability

⁸⁵⁰ Efforts to be disproportionate should be assessed according to the time, cost and required manpower. Please see *Breyer [2016]* (n 277).

Under Article 20 GDPR, data subjects have the right to receive personal data relating to them in a structured, commonly used, and machine-readable format, and in certain circumstances, to transmit such data to another data controller.

Measures

TOMs must be implemented to allow data subjects to transfer their personal data directly from one controller to another,⁸⁵¹ in a structured, commonly used, and machine-readable format.⁸⁵² Controllers, however, are not required to adopt or maintain technically compatible processing systems.⁸⁵³ The provision of information to a data subject does not mean that the relevant data set will be deleted.⁸⁵⁴ If the data subject also wishes their personal data to be deleted, this must be requested separately.⁸⁵⁵ Specifically, this right applies only to personal data (and not anonymous or aggregated data), and to personal information provided by individuals themselves. The appropriate measure may thus include a technological mechanism to search the data actively and knowingly provided by the data subject (e.g., address, username), as well as data derived from the data subject's actual use of the service or device (e.g., search history). This operation excludes inferred data and derived data, which are data generated by the controller using the data provided by the data subject, as well as personal data that is processed in accordance with consent or contract. In addition, it does not apply to the processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in

⁸⁵¹ GDPR, Article 18(2).

⁸⁵² *ibid*, Article 20(1).

⁸⁵³ *ibid*, Recital 68.

⁸⁵⁴ *ibid*.

⁸⁵⁵ GDPR, Article 20(3).

the controller or where the processing is necessary for the controller to comply with a legal obligation. TOMs must pay special attention to the implementation of technological mechanisms and systems (for example, a software converter for the csv format) to respond to data portability requests. Because this seems such an unlikely (low risk) scenario in practise, it is best dealt with manually processes rather than using automated software functions if the organisation's purpose allows for it. It is important to note that data extraction must be limited to identified and authenticated individuals and must be communicated securely, if possible, encrypted. Furthermore, this task can also imply that the data must be erased or restricted, which must be confirmed prior to the data operations.⁸⁵⁶ In these circumstances, the provision of personal data to the data subject should have no negative impact on the rights and freedoms of other individuals,⁸⁵⁷ especially when more than one individual is involved in a single personal data dataset.⁸⁵⁸ From the standpoint of accountability, TOMs must include the implementation and maintenance of policies and procedures for responding to requests for data portability. To respond to these requests, the data controller must consider the implementation and maintenance of an appropriate communication system with the data subject, and documentation must be kept as evidence of compliance and accountability. It is also worth noting that the right to data portability only applies to personal data processed by automated means; it does not apply to personal data processed manually.⁸⁵⁹

⁸⁵⁶ See, Articles 17, 18 and 19 GDPR.

⁸⁵⁷ GDPR, Article 18(4).

⁸⁵⁸ See, Recital 68 GDPR.

⁸⁵⁹ GDPR, Article 20(1)(b).

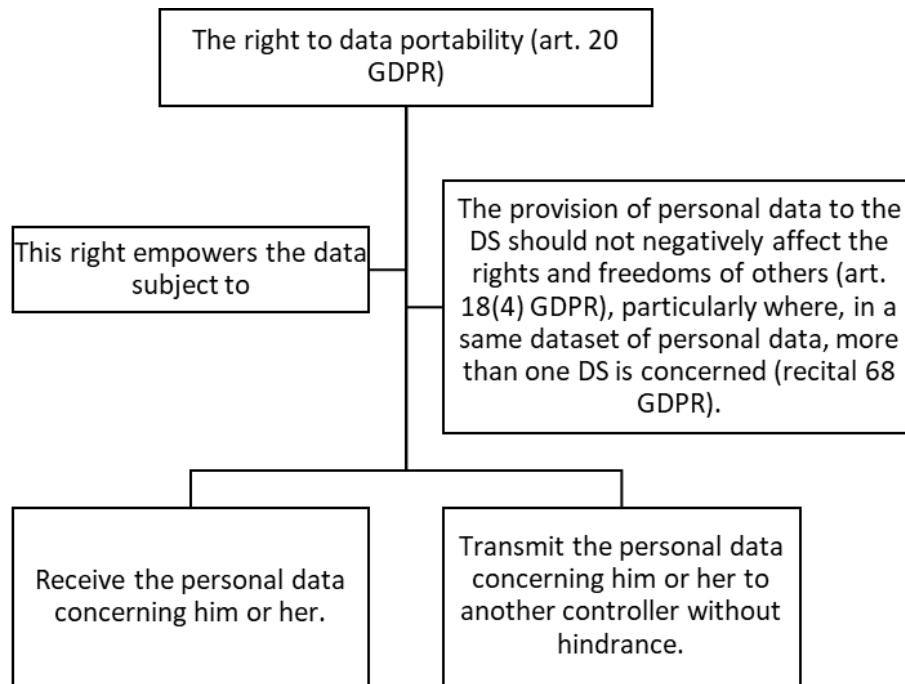


Figure 42 - The right to data portability, Federico Marengo, Data Protection Law in Charts, 2021 (adapted).

Q: How does the organisation respond to requests for data portability?

An affirmative answer to the above question implies that a system or technique that enables data portability is implemented in all systems and processing activities of the organisation.⁸⁶⁰

Right to object

Article 21 GDPR addresses the right of a data subject to object to the processing of his or her personal data. This right only applies to specific legal grounds of processing, namely, to the controller's performance of a task carried out in the public interest or in the exercise of official authority vested in the controller,⁸⁶¹ and when the processing is based on the

⁸⁶⁰ Compliance evidence example: Logs of the procedural or technical process for handling data portability requests.

⁸⁶¹ GDPR, Article 6(1)(e).

controller's legitimate interests.⁸⁶² A controller may reject the request and continue to process the personal data in question if there are compelling legitimate grounds⁸⁶³ for the processing that outweigh the interests, rights and freedoms of the individual,⁸⁶⁴ or if the processing is necessary for the establishment, exercise or defence of a legal claim. Moreover, the right to object to processing does not apply if the processing is necessary to perform a task of public interest.⁸⁶⁵ Following the data subject's request, the controller must immediately cease all processing operations, pending an assessment of the compelling legitimate grounds for the processing that override the rights of the data subject.⁸⁶⁶ Controllers are no longer permitted to process personal data after verifying the request. The controller must also consider the right to object to processing of data for direct marketing purposes.⁸⁶⁷ The data subject has the right to object to the processing of his or her personal information when the processing is conducted for direct marketing purposes, including profiling related to direct marketing.⁸⁶⁸ This right can be exercised at any time and without charge,⁸⁶⁹ and it can pertain to the initial or further processing.⁸⁷⁰ Furthermore, the right to object for scientific or historical research purposes or statistical purposes, applies if personal data is processed for such purposes.⁸⁷¹ It is important to mention that the processing for archiving purposes in the public interest is not included in

⁸⁶² *ibid.*, Article 6(1)(f).

⁸⁶³ See, Recital 68 GDPR. 'It should be for the controller to demonstrate that its compelling legitimate interest overrides the interests of the fundamental rights and freedoms of the data subject.'

⁸⁶⁴ GDPR, Article 21(1).

⁸⁶⁵ *ibid.*, Article 21(6).

⁸⁶⁶ *ibid.*, Article 18(1)(d).

⁸⁶⁷ GDPR, Recital 70.

⁸⁶⁸ *ibid.*, Article 21(2).

⁸⁶⁹ See, Article 21(2) GDPR. See also, Recital 70 GDPR.

⁸⁷⁰ GDPR, Recital 70.

⁸⁷¹ GDPR, Article 21(6).

this right, as the exercise of this right is determined by the individual's particular situation.⁸⁷² Moreover, the right to object to processing does not apply if the processing is necessary to perform a task of public interest.⁸⁷³ Finally, consideration must be given to the right to object to processing by automated means in the context of the provision of information society services. A data subject may object to the automated processing of personal data relating to him or her where personal data are processed in the context of information society services.⁸⁷⁴ The controller of these services is required to implement appropriate technical specifications, arrangements, or procedures to ensure that the data subject can exercise their right using automated means. There are also information obligations associated with the right to object, namely, at the time of the first communication between the controller and data subject, the data controller must inform the data subject of the existence of this right. In such cases, the information must be presented clearly and separately from all other information.⁸⁷⁵

Measures

TOMs to respond to opt-out, restriction, or objection requests to processing, the integration of automated mechanisms for data privacy into direct marketing practices, the provision of a data privacy notice at all points where personal information is collected, and the integration of mechanisms and systems to ensure data privacy in research practices. With respect to organisational measures, data controllers should pay special attention to

⁸⁷² *ibid.*

⁸⁷³ *ibid.*

⁸⁷⁴ GDPR, Article 21(5).

⁸⁷⁵ *ibid.*, Article 21(4).

the implementation and maintenance of policies and procedures in response to requests for opt-outs, restrictions, or objections to processing. Direct marketing and research practices and processes should also be incorporated into data privacy policies. As a result, management and operational activities should include the implementation and maintenance of an appropriate communication system to respond to requests for the right to object, as well as the documentation necessary to demonstrate compliance and accountability.

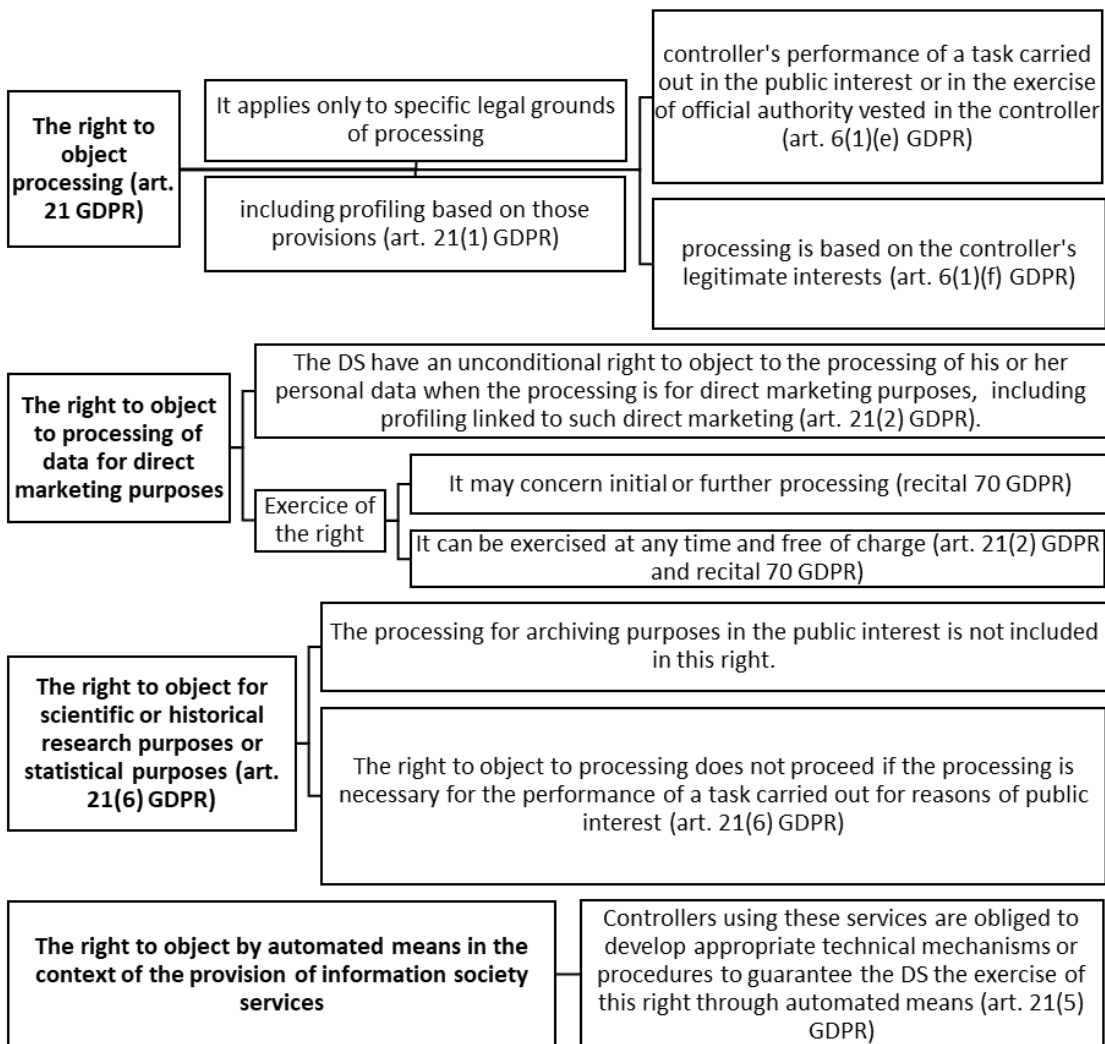


Figure 43 - The right to object processing, Federico Marengo, Data Protection Law in Charts, 2021 (adapted).

Q: Are Data protection and privacy integrated into the company's direct marketing practises?

If the answer to the above question is yes, it means that the organisation has established a system or process to address how it ensures that direct marketing practices comply with the right to object to direct marketing. This system or process shows the organisation's dedication to safeguarding data subject rights and complying with GDPR Regulations.⁸⁷⁶

Q: Is data protection included into the organisation's research procedures (for example, scientific and historical research)?

If the response to the aforementioned question is affirmative, it indicates that the organisation has implemented a mechanism that supports compliance with research practices, including obtaining informed consent, de-identifying data, and preserving research data used for scientific, historical, or statistical purposes.⁸⁷⁷

Automated individual decision-making, including profiling

Article 22 GDPR addresses the data subjects' right not to be subjected to decisions based solely on automated processing where such decisions would have a legal or significant impact on him or her. It also specifies when the right does not apply (for example, when a contract or the data subject's explicit consent is required) and states the application of appropriate safeguards. It also prohibits the use of special category data in automated decision making unless (a) the processing is done with the data subject's explicit consent

⁸⁷⁶ Compliance evidence example: Internal guidelines or procedures for data subject objection analysis and response.

⁸⁷⁷ Compliance evidence example: Internal policies or procedures governing the use of research data for scientific, historical, or statistical purposes.

(but, unless prohibited by MS law) or (b) the processing is necessary for reasons of substantial public interest under Union or MS law.⁸⁷⁸ This right is intended to avoid any detrimental effects on the ability of individuals to control automated decision-making processes, to avoid abdications of human responsibility and to support human dignity, as well as to limit the reach of potentially deficient decisions and reduce the possibility of unfair discrimination.

Measures

It is important to note that this right, although applicable to the processing of personal data that is solely based on automated means,⁸⁷⁹ requires both a technology-based and a people-based approach. An automated decision-making process comprises decisions taken without meaningful human involvement and carried out by someone who has the authority and competence to alter the decision. In this context, "automated processing of personal data" refers to any type of processing that uses personal data to evaluate certain personal aspects of an individual. Specifically, it can be used to analyse or predict aspects pertaining, inter alia, to a person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location, or movements.⁸⁸⁰ Profiling falls under the GDPR rules that regulate the processing of personal data, including the legal basis for processing and the principles of data protection.⁸⁸¹ In order to ensure fair and transparent processing, the controller must implement appropriate measures to ensure

⁸⁷⁸ See, Recitals 71 and 72 GDPR.

⁸⁷⁹ This provision does not apply to manual processing of personal data.

⁸⁸⁰ Article 4(4) GDPR provides the definition of automated processing of personal data.

⁸⁸¹ GDPR, Recital 72.

that factors contributing to inaccuracies are corrected and the risk of error is minimised. To that end, it must consider the specific circumstances and context of personal data processing, as well as the use of mathematical or statistical profiling techniques, to ensure that personal data is protected in a way that takes into account any potential risks to data subjects' rights and prevents, for example, discrimination against natural persons based on racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or which result in measures having such an effect.⁸⁸² Controllers must implement appropriate safeguards when decision-making is based on explicit consent or contractual necessity, ensuring that the data subject is able to obtain human intervention before a decision is made, express his or her viewpoint, and contest the decision.⁸⁸³ Further mandatory safeguards include the provision of specific information to the data subject and the provision of an explanation of the decision reached following an assessment.⁸⁸⁴ Therefore, the controller must implement measures to address the obligation to notify of the existence of automated decision-making; there is a requirement to disclose to the data subject whether automated decisions, including profiling, are being made, as well as the significance and anticipated consequences of these decisions in relation to the data subject.⁸⁸⁵ In addition, measures must be implemented at both technical and organisational level, including mechanisms to prevent automated processing and profiling decisions from having legal consequences for the data subject, with the following exceptions: (a) a data processing operation is required to perform a contract

⁸⁸² GDPR, Recital 71.

⁸⁸³ Under Article 22(3) GDPR, these are mandatory safeguards.

⁸⁸⁴ GDPR, Recital 71.

⁸⁸⁵ GDPR, Articles 13(2)(f), 14(2)(g) and 15(1)(h).

between the data subject and the controller - this processing is authorised by law and is subject to security controls to protect the data subject's rights, freedoms, and legitimate interests; (b) the processing is based on the explicit consent of the data subject; (c) system decisions involving special categories should not be based on automated processing or profiling unless the subject has expressly consented, or the processing is required due to significant public interest. Moreover, a PbDD mechanism must be in place to ensure that individuals have the right to request that key decisions based on automated processing of their personal information be reviewed or reconsidered manually. Data controllers must keep evidence of any manual intervention or human revision of an automated decision-making process, as well as the reasoning used in selecting a legal basis for such processing, for accountability purposes.

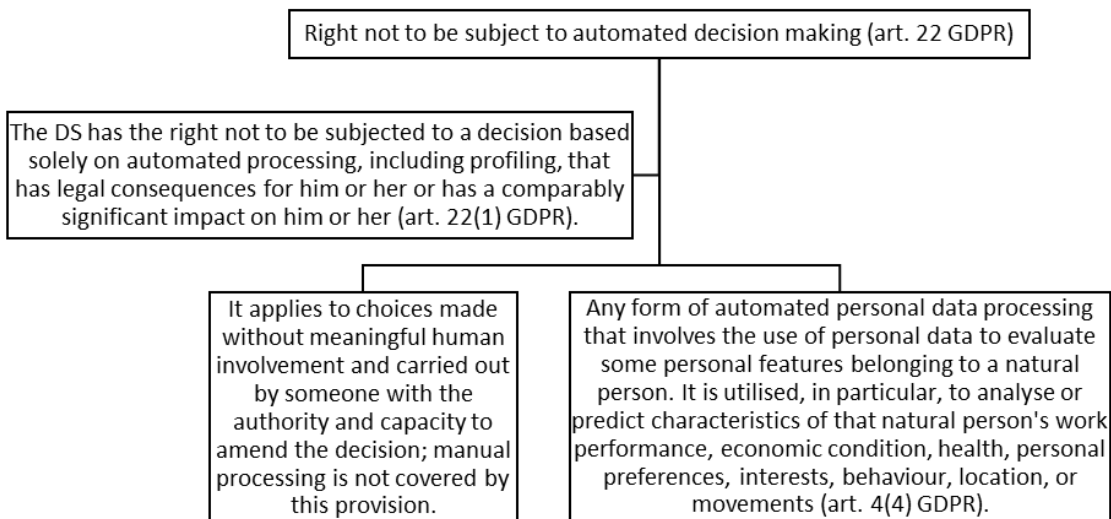


Figure 44 - The right not to be subject to ADM, Federico Marengo, Data Protection Law in Charts, 2021 (adapted).

Q: Are there policies and procedures in place to review processing that is entirely or partially automated?

If the answer to the above question is yes, it means that the organisation has established a system or procedure that allows the controller to identify whether their processing activities are subject to limitations on automated decision-making and provides options to ensure compliance. In addition to measures that protect the rights, freedoms, and legitimate interests of individuals, the organization must also consider the requirements outlined in Article 12 of the GDPR, such as allowing individuals to express an opinion. The measures implemented should be clear, timely, and appropriate, ensuring that the organisation meets GDPR standards and demonstrates its commitment to protecting the rights of data subjects.⁸⁸⁶

This section of the DPPA pertains to Chapter III of the GDPR and outlines the approach to implementing procedures for processing data subjects' rights as stipulated in Articles 12 to 23 of the Regulation. It is important to note that the PbDD plan should include TOMs to ensure that the system processing personal data has adequate safeguards in place to override initial processing mechanisms associated with data subject rights, either on the advice of the DPO or as directed by official authorities. As per Article 23 of the GDPR, Union or Member State law may impose limitations on data subject rights and data controller obligations. However, such limitations must comply with the requirements outlined in the Charter and the ECHR.⁸⁸⁷ While the Charter no longer applies to the UK, as it was not

⁸⁸⁶ Compliance evidence example: (a) Policies and procedures governing decision-making automation. b) An inventory of data that describes automated data processing and specifies the legal basis for such processing. (c) Proof of human intervention in the decision-making process.

⁸⁸⁷ GDPR, Recital 73.

included in law as part of the European Union (Withdrawal) Act 2018, the ECHR remains applicable.

9.2. Implementing PbDD measures to address the responsibilities of controller and processor

This section will explore DPPA measures related to the data protection responsibilities of data controllers and processors.

Responsibility of the controller

Article 24 GDPR requires the data controller to put in place appropriate TOMs to ensure and demonstrate GDPR compliance. The appropriateness of these measures is determined by a risk assessment that considers the nature, scope, context, and purposes of the processing, as well as the risks of varying likelihood and severity to individuals' rights and freedoms. There is a specific reference in the GDPR that data protection policies must be implemented where they are proportionate to the processing activities.⁸⁸⁸ As a result, any data processing system that processes, stores, or transfers personal data must be subject to a transparent risk assessment in order to determine associated risk and proportionate security controls to ensure the confidentiality, integrity, and availability of personal data. Article 24 GDPR serves as a formal reminder that an appropriate, comprehensive mesh of organisational measures, including policies and procedures, as well as technical, physical, and other measures and controls addressing information risk and compliance obligations,

⁸⁸⁸ GDPR, Recitals 74 to 77.

must be implemented. The magnitude of this PbDD operational task typically requires a structured, systematic approach, to which the current DPPA model may contribute significantly. Given the frequent overlaps, it usually makes sense to integrate, or at least align and coordinate, data protection measures with ISO27001 (or similar information security framework) and other tools of data security and governance, including business continuity management.

Measures

TOMs must include the implementation of robust mechanisms and systems for conducting enterprise privacy risk assessments and self-assessments of privacy management. Additionally, controllers should maintain policies and procedures for these assessments, seek relevant certifications, accreditations, or data protection seals, and uphold a comprehensive data protection policy. Furthermore, controllers must implement and maintain appropriate data governance mechanisms, such as audit systems and controls, to review processes involving personal data processing and assess risks associated with such processing. These mechanisms are crucial in demonstrating compliance to regulators and individuals alike.

Q: The organisation conducted a global data protection risk assessment? Are data protection management self-evaluations or audits undertaken by the organisation?

The DPO must prioritise resources to mitigate risks based on their likelihood and impact on the organisation. This measure applies to risk assessments conducted at the highest level of the organisation, not to specific endeavours such as projects or processing activities (DPIA). A system or activity must be in place (such as a gap analysis) to help the

DPO establish a procedure to demonstrate that appropriate TOMs have been implemented for GDPR compliance. (Applies to Articles 24 and 39 GDPR).⁸⁸⁹

Q: Does the organisation maintain documents that demonstrate compliance or accountability?

An affirmative answer to the above question implies that a process is in place to assist the organisation in creating documentation of the TOMs it has taken to demonstrate compliance with the GDPR.⁸⁹⁰

Data protection by design and by default

Article 25 GDPR Introduces new responsibilities for data controllers and makes data protection by design and default mandatory in the organisation's systems and processing activities involving personal data. To meet the GDPR requirements, data controllers must implement appropriate TOMs, when determining the means of processing as well as when further processing personal data, to incorporate the data protection principles enshrined in Article 5 and the necessary safeguards into the systems and processing activities involving the use of personal data. Moreover, data controllers must implement data protection by default, to ensure that, by default, only personal data necessary for the specific purpose for which was collected is processed. As previously discussed, the "necessity" element informs (a) the amount of data collected, (b) the extent of processing,

⁸⁸⁹ Compliance evidence example: (a) implementation of a comprehensive risk assessment (or gap analysis) for the organisation that takes data protection and privacy into account. (b) The development of a strategy or methodology for evaluating and mitigating potential risks to individuals' privacy. (c) Evaluations of preparedness and performance. (d) A scorecard for data protection and privacy accountability.

⁸⁹⁰ Compliance evidence example: Records of all data processing activities within the organisation, including interpretations of the applicable legal provisions and reasons for the processing (purposes).

and (c) the retention and accessibility of data. Controllers must also ensure that by default, personal data are not made accessible to an indefinite number of individuals. Adherence with an approved certification mechanism⁸⁹¹ may be used as an element to demonstrate compliance with these requirements.⁸⁹²

There are certainly business reasons for a data controller to invest appropriately in data protection, such as information risk detection, evaluation, and mitigation, as well as GDPR compliance requirements. As we have seen, such implementation necessitates organisational approaches to PbDD with varying costs, challenges, and benefits; elaborating on these appears to be a good way to secure management support and involvement, as well as to provide and allocate the funding and resources required to design, deliver, implement, and maintain the appropriate TOMs. Data protection ‘by design’ and ‘by default’ are two GDPR requirements that guide the specification, design, development, operation, and maintenance of privacy-related IT systems and processes, including third-party relationships and contracts. As a result, a methodology for operationalising data protection principles and implementing the necessary safeguards to protect data subjects' rights is critical to the data controller's compliance efforts; technical measures, such as the implementation of mechanisms, systems, and processes to integrate PbDD into system and product development (for example, mechanisms for conducting DPIAs for new programs, systems, and processes or mechanisms for conducting DPIAs for changes to existing programs, systems, or processes), necessitate a methodological approach, such as that provided here by the DPPA framework. Due to the complexities

⁸⁹¹ As described in Article 42 GDPR.

⁸⁹² GDPR, Recital 78.

involved in bridging GDPR legal requirements into the personal data operations theatre, any attempt to implement PbDD in a non-structured, holistic form, will render such compliance impossible. Furthermore, a data protection methodology will provide a valuable means of demonstrating accountability to a supervisory authority, in addition to the data privacy policy, ROPA and retention schedule, data de-identification tools, and information security assessments.

The figure below illustrates the novel implementation strategy that underpins the DPPA model:



Figure 45 - DPPA framework: approach to PbDD implementation

The implementation of PbDD through the DPPA

The DPPA PbDD implementation process starts by determining the status of existing processing activities and related TOMs that meet the GDPR requirements and comparing

them with the desired or expected outcome in relation to the legal requirements and obligations based on the GDPR (gap analysis). This exercise provides the identification and attribution of the organisations' processing activities, the corresponding data flows and the assessment of the legal basis for processing, leading to the fulfilment of the requirement expressed in Article 30 GDPR for the existence of a ROPA. Documentation required for accountability purposes may be added to the PbDD plan contained in the DPPA on an ongoing basis. Adhering to the DPPA compliance approach allows data controllers to embed accountability measures and foster a data protection culture across the organisation, while building trust with individuals and mitigating enforcement actions. The DPPA offers a dynamic approach to compliance, allowing organisations to regularly review and update as necessary the TOMs implemented in accordance with ongoing GDPR requirements. Therefore, accountability under the DPPA model cannot be viewed as a one-off exercise.

According to Article 5 GDPR, compliance must be ensured through various means and at various appropriate times, throughout the entire lifecycle of the personal data, and integrated into the products and services used by data subjects. Mechanisms and systems must thus evolve in tandem with and adapt to technological advancements, and should be as thoroughly integrated into the product, service, process, and technology as possible.

As a practical example, data controllers can use push-pull mechanisms and other specific tools to provide transparency in online activities. Privacy policies, detailed notices, and notifications can be delivered to individuals at the appropriate time, via websites, dashboards, control panels, and user interfaces. In many cases, interactive tools are a good option - the goal is not to force users to understand icons, but rather to develop

transparency technology that understands the user and responds appropriately,⁸⁹³ two examples are user-friendly chat boxes and chatbots. However, while machine learning can help with transparency, human interfaces should not be overlooked.

The DPPA has Article 25 GDPR and PbDD at its core, hence the key Q&A in this model is the following:

Q: Is data protection by design and by default incorporated into the organisation's data processing operations?

An affirmative answer to the above question implies that a system, control, or process is in place that assists the DPO in building a framework for the practical implementation of legal requirements and aids engineers, IS/IT managers, and application developers in designing and implementing essential processing operations that adhere to privacy and data protection standards and Regulations.⁸⁹⁴

Joint controllers

Article 26 GDPR provides that two or more controllers, are joint controllers when they jointly determine the purposes and means of processing personal data. The data controllers must regulate their respective obligations for GDPR compliance in a transparent

⁸⁹³ See, Recital 60 GDPR. 'That information may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing. 'Where the icons are presented electronically, they should be machine-readable.'

⁸⁹⁴ Compliance evidence example: (a) The specifications for new IT/IS tools (software and hardware) must demonstrate the inclusion of data protection and privacy criteria. (b) Data Protection Impact Assessments confirming that the required and sufficient safeguards have been integrated into the processing. (c) Incorporating data protection by design into IT systems, governance and accountability processes, physical design, and network architecture. (d) Methodologies, procedures, policy guidelines, and more strategies for managing anonymised or pseudonymised data.

manner through an agreement between them.⁸⁹⁵ The essence of the arrangement must be made available to the data subject, and data subjects may exercise their rights against either data controller, regardless of any arrangements to the contrary.

Measures

TOMs to manage relationships with business partners while ensuring that data protection as well as other aspects of information security are not neglected or ignored. This includes, for example, investigating and resolving data protection incidents, data breaches, or access requests collaboratively, achieving and maintaining an assured level of GDPR compliance, and adhering to the consented purposes for which personal information was initially collected, regardless of where it resides or is being processed. In addition to the requirements in Articles 12 and 15 GDPR relating to transparency and providing information to data subjects, and Articles 15, 16, 17, 18, 19, 20, and 21 GDPR relating to the mechanisms for responding to requests exercising data subject rights, a data protection policy that provides transparency around the joint controller relationship and identifies a point-of-contact for data subject requests must be in place.

Representatives of controllers or processors not established in the Union

Article 27 GDPR determines that when a non-EU data controller or data processor offers goods or services (paid or free) to EU data subjects, or monitors data subjects' behaviour within the EU, they must designate, in writing, a representative in the EU. EU

⁸⁹⁵ Where organisations are jointly responsible for determining and fulfilling data protection requirements collaboratively, they must clarify their respective roles and responsibilities.

representatives are legal or natural persons who represent the controller, or processor, in relation to their GDPR obligations and must be based in the same MS as the data subjects being monitored or offered goods or services. It is important to mention that exceptions will apply if the data controller or processor is a public sector body, processes only on occasion, does not process large amounts of special data, and the processing is unlikely to result in a risk for the rights and freedoms of individuals.⁸⁹⁶

In terms of measures to address accountability, the controller must: have a written contract or agreement with the representative; conduct an assessment or request a legal opinion on whether a representative must be appointed as a result of the processing activities carried out; issue a written mandate for the representative to act on behalf of the controller or processor; and keep documentation of the representative's communication, for example, via the data protection policy or via a specific notice on the organisation's website.

Q: Does the organisation assign an individual responsibility for data protection and privacy? (Applies to both the roles of DPO and EU Representative).

An affirmative answer to the above question implies that a process is in place to assist the organisation in assigning operational responsibilities for a data protection program to a natural or legal person.⁸⁹⁷

⁸⁹⁶ GDPR, Recital 80.

⁸⁹⁷ Compliance evidence example: (i) The controller or processor must give the EU Representative written authorisation to act on their behalf. (ii) The public has easy access to information on how to contact the EU Representative, such as in a privacy notice or on a website.

Processor

Article 28 GDPR creates an obligation for data controllers to only outsource the processing of personal data to entities that offer sufficient guarantees to implement appropriate measures to ensure GDPR compliance. Furthermore, it determines that a contract or binding act governing the relationship is required and specifies its terms. Article 28 GDPR also limits processors' ability to subcontract without the data controller's consent and specifies the guarantees that must be included in the agreement.⁸⁹⁸

Measures

The data controller must implement measures to facilitate the conduct of due diligence on potential processors' data protection and security postures to ensure that processing is only performed by organisations that can provide sufficient data protection guarantees. In addition, it must develop and maintain a list of data protection requirements for processors that takes into account the specifics of the processing activity to help determine what data protection safeguards are required to include in contracts with data processors. The applicable measures must therefore include a mechanism to ensure that data processing agreements are in place with all data processors and embedded in the organisation's procurement process. To ensure compliance with Article 28 of the GDPR, it is imperative to implement measures that focus on maintaining accountability documentation. These measures include copies of processor agreements; data procurement policy, including data protection requirements; processor self-evaluation, assurance report and due diligence; templates for standard contractual clauses and data transfer agreements. Following the

⁸⁹⁸ GDPR, Recital 81.

CJEU's Schrems II decision, the controller must also conduct and maintain up to date a risk assessment in relation to personal data transfers to third countries. Similarly, any system that acts as a data processor (including cloud or SaaS) must be governed by a contract or other legal act that defines the operational aspects of the processing engagement.⁸⁹⁹ This requirement also applies to internet service providers (ISPs) and communication service providers (CSPs), as well as outsourced data centres and other commercial services where the data controller transfers personal data to third parties for purposes such as marketing, payroll, tax, pension, or medical services for employees.

Q: Is data protection and security-related vendor and processor due diligence undertaken by the organisation?

If the answer to the above question is yes, it indicates that the organisation has implemented a process that ensures that data processing is carried out only by entities that provide sufficient data protection guarantees.⁹⁰⁰

Q: Is the organisation's data privacy policy applicable to third parties (such as customers, vendors, and processors)?

If the answer to the above question is affirmative, it suggests that the organisation has a robust system or process in place that enables it to make informed decisions regarding the necessary data protection

⁸⁹⁹ The agreement must provide for: 1. Processing duration; 2. Processing nature and purpose; 3. Personal data types and categories; 4. Data Controller obligations and rights; 5. States that the processing is defined and authorised by the Data Controller (including transfers); 6. States that persons authorised to process personal data are subject to appropriate confidentiality agreements; 7. Security controls that satisfy Article 32 are implemented; 8. Regulatory flow down to data sub-processors is declared and agreed; 9. Encourages the data controller to respond to data subject rights requests; 10. Processor will delete or return data sets at the request of the data controller; and 11. Processor will make all information required to demonstrate regulatory compliance available to the data controller.

⁹⁰⁰ Compliance evidence example: (a) A list of screening questions for prospective vendors and processors. (b) A questionnaire for vendors. (c) An evaluation of the vendor's data protection risks.

requirements to apply to contracts entered into with third-party entities authorised to receive and process personal data.⁹⁰¹

Processing under the authority of the controller or processor

Article 29 GDPR determines that processors and employees of controllers and processors, must only process personal data as instructed by the data controller, or in case such processing is required by Union or MS law.

Measures

The controller must have in place mechanisms and procedures to execute contracts or agreements with all data processors, or third parties involved in the processing of personal data. Processors, like controllers, must keep all personal data they handle secure. Because processors are frequently controllers for personal data on their employees, they should have all necessary data protection measures and protection mechanisms in place (including a plan for implementation of PbDD); it will then be a matter of extending them to cover client (controller) data and managing data protection within client relationships (for example, determine how to handle data breaches and data incidents when data is processed on behalf of the data controller).

⁹⁰¹ Compliance evidence example: (a) Evaluation of potential suppliers and other processors. (b) Data protection, privacy, and security clauses in contracts. (c) Data protection questionnaire for outsourcing personal data processing. (d) A scorecard for evaluating vendor data security risks. (e) A list of contractor data protection requirements. (f) Proof of the processor's adherence to a code of conduct or certification mechanism. Contracts with contractors or vendors that contain standard contractual clauses.

Q: Is the organisation following the proper procedures for executing contracts or agreements with all processors?

An affirmative answer to the above question implies that a system or process that ensures written or electronic contracts with data processors are in place.⁹⁰²

Records of processing activities

Article 30 GDPR lists the information that must be maintained as records of processing activities, carried out by and on behalf of the controller, as well as the obligation to make the records available to data subjects and supervisory authorities upon request.⁹⁰³

Measures

TOMs to ensure that all processing processes are defined in sufficient detail by the controller to support the maintenance of an electronic ROPA. The PbDD plan must be designed to allow registration of the following information: a) Purpose of processing; b) Description of the data subjects and associated categories of personal data; c) Description of all recipients of the personal data; d) Transfers of personal data to any third countries or international organisations; e) The time limits for erasure for each of the categories of personal data; and f) Description of security controls protecting personal data. This task requires the implementation of mechanisms and systems to maintain an inventory of

⁹⁰² Compliance evidence example: (a) Contracts or agreements demonstrating legal compliance and privacy risk management activities. (b) Evidence of the processor's adherence to an approved code of conduct or certification mechanism. (c) Standard contractual clauses between the data controller and the data processor.

⁹⁰³ GDPR, Recital 82.

personal data holdings (what personal data is held and where), as well as the implementation and maintenance of appropriate systems and controls that enable effective recording of the organisation's processing activities. This record cannot be viewed as a static document; rather, it must evolve in response to the organisation's data processing activities. As a result, periodic assessments of the organisation's data processing activities must be performed and the ROPA updated accordingly, so that all processing activities are included in the personal data inventory.

Q: Is an inventory of personal data or processing activities (ROPA) kept by the organisation?

An affirmative answer to the above question implies that a system or process is in place that assists the controller in developing an inventory of processing activities and address the information that must be kept and for how long (for example, privacy management software or spreadsheets).⁹⁰⁴

Security of processing

Article 32 GDPR Requires data controllers to implement TOMs⁹⁰⁵ to ensure an appropriate level of security, based the state of the art, the costs of implementation and the nature,

⁹⁰⁴ Compliance evidence example: Maintenance of lists of data categories, data subjects, the purposes for which the data was collected, recipient categories and countries, and other information specified in Article 30 GDPR.

⁹⁰⁵ The GDPR mentions some examples of technical and organisational measures (such as encryption, anonymisation, and resilience) that cover data confidentiality, integrity, and availability, as well as assurance measures and employee compliance (implying a requirement for implementation of policies and procedures, data protection awareness and training, compliance enforcement and audits).

scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of data subjects.

Measures

Following are some examples of TOMs that should be included in the PbDD plan depending on the level of risk presented by the processing activity: a) the pseudonymisation and encryption of personal data; b) a process leading to the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; c) a process leading to the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; d) a process for regularly testing, assessing and evaluating the effectiveness of TOMs for ensuring the security of the processing. In terms of technical measures, the data controller must consider the implementation of mechanisms and systems to integrate data protection into an information security policy; to maintain technical security measures (for example, intrusion detection, firewalls, active network monitoring); to maintain measures to encrypt personal data and the implementation of mechanisms and systems to restrict access to personal data (for example, role-based access to data sets and systems, segregation of duties).⁹⁰⁶ In terms of organisational measures, the data controller must implement and maintain procedures for performing regular testing of data security and cybersecurity (for example, penetration testing), procedures for incorporating data protection risk into data security risk assessments, and procedures for devising and maintaining data protection

⁹⁰⁶ Article 32 GDPR also requires anyone with access to personal data to only process such data in accordance with the data controller's instructions.

requirements for third parties (for example, clients, vendors, affiliates, and processors). Industry certifications such as ISO certification, SOC 2/3 certification, or ITIL certification can be used to demonstrate GDPR compliance as well as accountability. The ISO27001 ISMS series, for example, provides a coherent, comprehensive, and structured framework for assisting in data protection management, in addition to other information risk and security controls, and can be an excellent tool for aligning the data protection measures suggested by PbDD application with the organisation's information security requirements. The DPPA approach to security is elaborated upon in 6.1.2.

Q: Does the organisation consider data protection and privacy risks when assessing security risks?

If the answer to the question is yes, it means that the data controller has established a process or system that helps them consider data protection in security risk assessments.⁹⁰⁷

Q: Is the organisation integrating data protection and privacy into its information security policy (ISP)?

An affirmative answer to the above question implies that a procedure or mechanism is in place that assists the controller in ensuring that data protection is incorporated into the information security policy.⁹⁰⁸

⁹⁰⁷ Compliance evidence example: Incorporating security risk assessments into DPIAs helps demonstrating that technical and organisational measures were chosen based on a risk assessment.

⁹⁰⁸ Compliance evidence example: Incorporating data protection and privacy into ISP indicates that due consideration was given to areas of data security and cybersecurity, namely that the choice of technical and organisational measures was based on a relevant assessment. This is especially helpful when demonstrating compliance with the Regulation.

Q: Does the organisation keep adequate internal and external technical security measures for its information technology and information systems (such as firewalls and intrusion detection)?

An affirmative answer to the above question implies that a process is in place that helps the controller evaluate whether the appropriate technical security measures are in place to ensure an appropriate level of security according to Article 32 GDPR.⁹⁰⁹

Q: Does the organisation keep encryption measures for personal data up to date?

An affirmative answer to the above question implies that a system or process are in place to ensure the controller maintains an appropriate level of security across the organisation's data processing assets and helps establishing encryption practices as appropriate TOMs.⁹¹⁰

Q: Does the organisation have protocols in place to restrict access to individuals' personal information, such as role-based permissions and separate areas of responsibility?

An affirmative answer to the above question implies that a system or procedure are in place that assists the controller in addressing how employees and other users gain access to personal data based on legitimate business needs.⁹¹¹

Q: Are there routine audits or assessments of the system's security that are carried out by the organisation?

⁹⁰⁹ Compliance evidence example: A description of the technical security measures in place, as well as a policy for their periodic assessment and update.

⁹¹⁰ Compliance evidence example: A map of internal (or cloud based) encrypted assets.

⁹¹¹ Compliance evidence example: (a) Contracts are in place that bind employees and contractors, limiting how personal data is treated. (b) A list of employees and contractors with access to IT systems and data is available. (c) Audits of personal data access to establish whether present procedures are adequate in light of the purpose and nature of access are periodically conducted.

An affirmative answer to the above question implies that a measure designed to aid the controller in implementing a control over the technological or organisational safeguards in place to ensure the security of the processing of personal data is in place.⁹¹²

Notification of a personal data breach to the supervisory authority

Article 33 GDPR makes it mandatory to notify supervisory authorities in the event of a data breach occurs that poses a "risk of harm" for the rights and freedoms of data subjects.⁹¹³

The notification is expected without undue delay and where feasible within 72 hours of the event. Note that the point at which the clock begins to tick is not explicitly defined; it may be appropriate to gather and evaluate the available information and evidence prior to determining whether a reportable incident has occurred, for instance, the clock may not start until the incident is deemed authentic and not a false alarm. Detailed content requirements are set out by the GDPR for the notification letter and the circumstances of the data breaches must be documented. It is important to note that if data is strongly encrypted, losses or thefts of IT devices containing personal data are probably not required to be reported.

Measures

⁹¹² Compliance evidence example: A list of technical and organisational measures (which can be included in the ROPA).

⁹¹³ See also, Recitals 85, 87 and 88 GDPR.

The controller must implement measures leading to the appropriate and proportionate monitoring into the processing operation or data processing system processing personal data, as well as devise procedures to detect data incidents and breaches that must be reported to the supervisory authority within 72 hours of detection. This should include mechanisms and systems to maintain a log to track and handle data protection incidents and breaches, and organisational measures such as maintain a data privacy incident and breach response plan as well as maintain a breach notification procedure (to affected individuals) and system reporting protocol (to regulators, credit agencies, law enforcement).

In the context of notification of a breach to the supervisory authority, the following Q&A will aid the controller in identifying the appropriate TOMs:

Q: Does the organisation have a plan for responding to data protection incidents and breaches? Is an incident register kept by the organisation to track data protection breaches?

An affirmative answer to the above query implies that a process or system are in place that will enable the organisation to develop a breach response architecture to facilitate compliance with the specific requirements outlined in Article 33 GDPR. These requirements concern notification protocols, timing, and notification content. In addition, a mechanism must be implemented to ensure that the information that is necessary for accountability purposes is recorded.⁹¹⁴

⁹¹⁴ Compliance evidence example: (a) The procedure that should be followed when dealing with data loss events and breaches. (b) Information on how to get in touch with the breach response team. (c) Models of breach notification letters to be used in the event that a violation occurs. (d) A log of incidents to document any violations of data protection. (e) A form for compiling a summary of incidents. (f) The report on the loss of information and the form for managing the loss of information.

Communication of a personal data breach to the data subject

Article 34 GDPR requires notification to data subjects of breaches that result in a "high risk" for the rights and freedoms of individuals.⁹¹⁵ In addition to the legal and ethical considerations and guidance emanated from supervisory authorities, the timing and nature of disclosure present significant business concerns and challenges that must be addressed in the PbDD plan. This would typically be part of an integrated incident management process for serious or significant incidents, involving senior management, specialists, and consultants. One of the strongest arguments for making data protection an organisation's top priority and investing adequately in appropriate preventive breach measures is to avoid this situation and the associated business costs, disruption, and aggravation.

Measures

TOMs to establish a process for informing data subjects of any breaches impacting them and to ensure that communication is carried out using plain language. In addition, the processes that are used to handle a breach of personal data need to include mechanisms that can be used to assess the potential risk to the data subject, the implementation and ongoing maintenance of appropriate breach response mechanisms and procedures, as well as appropriate mechanisms to address external information and communication with data subjects, regulators, law enforcement and press in the event of an incident.

⁹¹⁵ See also, Recitals 86, 87 and 88 GDPR.

Q: Does the organisation have breach notification procedures (which are directed to individuals who have been affected) as well as reporting protocols or procedures (which are used to alert regulators, agencies, law enforcement, and the press) in place?

An affirmative answer to the above query implies that a system or mechanism is in place that will assist the organisation in selecting the appropriate timing, content, and communication channels for notifications to be sent to data subjects. (Applies to Articles 12, 33 and 34 GDPR).⁹¹⁶

Data protection impact assessment and prior consultation

Article 35 GDPR requires data controllers to conduct an impact assessment on the protection of personal data whenever there is a probability that the processing will result in a high risk for the rights and freedoms of data subjects.⁹¹⁷ In order to properly carry out the DPIA, the controller is required to consult with the DPO (when designated). Additionally, the resultant risks identified following the DPIA must be recorded and duly approved by the organisation's assigned risk owner. The assessment must include, at a minimum: (a) a description of the processing, including its purpose and legitimate interests; (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes; (c) an assessment of the risks to the rights and freedoms of data subjects; and (d) security controls demonstrating compliance. Data protection and privacy risks, including potential impacts, must be evaluated, particularly when new technologies, systems, assets, or arrangements with third parties are being considered, or in any other

⁹¹⁶ Compliance evidence example: (a) Contact details for the incident response team. (b) Letters and templates for notification in the case of a violation. (c) Protocols for notifying supervisory authorities and data subjects where there is a significant risk of damage.

⁹¹⁷ See also, Recitals 75, 84, 89, 90, 91, 92 and 93 GDPR.

situation where the risks may be significant, such as when the processing includes profiling of individuals (as defined in Article 4 of the GDPR). As we have seen, in addition to GDPR requirements, there are also sound business and ethical reasons to identify, assess, and treat information risk (including privacy and data protection compliance risk). Privacy and data protection risk should be included alongside other business risk in corporate risk registers. GDPR also suggests incorporating the evaluation of data protection risk into routine risk assessment activities for business change projects and new IT system developments.

In this context, the following gap Q&As will aid the controller in identifying the appropriate TOMs:

Q: Does the organisation keep DPIA standards, guidelines, and template documents up to date?

An affirmative answer to the above question implies that a system or activity are in place to provide guidelines for analysing personal data processing and assessing risk to personal data as part of the DPIA process (for example, risk matrixes, audits, policies, and guidelines for risk management). When developing their processing programs, organisations should ask questions about the available technology, the cost of implementation, the nature, scope, context, and purposes of the processing, as well as possible measures to protect the rights of data subjects (such as pseudonymisation).⁹¹⁸

⁹¹⁸ Compliance evidence example: Templates for DPIAs covering content requirements, such as a guide, policy, or assessment on when DPIAs are required; a report that shows the extent to which affected populations were consulted; assessments and reviews of processing activities based on new or changed risk information; and guidance and policies for assessing risk minimization through consultation with the Supervisory authority.

In relation to the duty to undertake a DPIA, Articles 6, 25, and 35 of the GDPR should be questioned as follows:

Q: Does the organisation conduct DPIAs for new programs, systems, or processes? Does the organisation perform DPIAs for changes on programs, systems, or processes? Is the organisation involving external stakeholders (for example, individuals, community groups, and privacy advocates) in the DPIA process? Is the organisation tracking and addressing data protection and security vulnerabilities discovered during DPIAs?

An affirmative answer to the above questions implies that a system or activity are in place to identify when a DPIA is needed as part of the development process or for a new processing activity. Also, a process or system are in place that ensures the organisation addresses comparable data protection concerns consistently, allowing the lessons learnt from prior DPIAs to be used to future DPIAs and ensuring that the organisation treats similar data protection issues consistently.⁹¹⁹

⁹¹⁹ Compliance evidence example: (a) DPIAs that certify to the use of relevant safeguards. (b) Documentation from DPIAs demonstrating the balance that was reached between the legitimate interests of the organisation and the rights and freedoms of the individuals whose data was being controlled. (c) Guidelines or evaluations regarding the circumstances in which DPIAs are required. (d) Documentation demonstrating that the DPIA procedure took into account the advice and opinion of the DPO. (e) Evidence that affected communities or their representatives were consulted. (f) Evaluations and reviews of the processing activities, based on any newly identified or updated risks.

Prior consultation

Article 36 GDPR requires data controllers to consult with the supervisory authority whenever a DPIA reveals that the processing of personal data would result in a high risk to the individuals whose data is being processed.⁹²⁰

Measures

The regulator is required to provide advice on whether the intended processing complies with the GDPR within 8 weeks upon receiving the enquiry (however, an additional 6 weeks may be provided for complex processing).⁹²¹ The requirement in question is well-intentioned, yet it lacks the necessary clarity, highlighting the importance of addressing it via the DPPA approach. The DPPA approach recommends that an evaluation of what the organisation regards as "high" privacy risks with respect to their processing activities be conducted to enhance clarity and provide direction. This measure leads to a business risk decision that must be made by the management and is therefore to be seen as part of the duties of the DPO (to advise the business of when "high-risk" should be interpreted as triggering the guidance of the supervisory authority). It is important to note that explicit inputs from the supervisory authorities may be helpful in terms of an official position on the suitability and adequacy of proposed TOMs.

One feasible approach to fulfilling the requirements of Article 36 of the GDPR involves determining that in instances where the processing of personal data results in a high risk after a thorough assessment via the DPIA, and if there are not appropriate measures to

⁹²⁰ Guidance from the regulator must be sought before the processing can be executed. The minimum information that needs to be provided to the Supervisory authority by the data controller is also outlined in Article 36 GDPR.

⁹²¹ See also, Recitals 94, 95 and 96 GDPR.

mitigate or eliminate the risk, guidance from the regulator is sought before commencing the processing activities.

Q: Are the findings and conclusions of the DPIA reported to the relevant external regulators and stakeholders?

An affirmative response to the aforementioned query indicates the existence of a well-defined procedure or system that facilitates the controller's determination of when and how to submit a DPIA to the supervisory authority, based on the specific circumstances. In order to demonstrate compliance with the GDPR, it is crucial to make informed decisions regarding the necessity of such reporting and maintain thorough documentation to demonstrate that consultations were undertaken.⁹²²

Designation of the data protection officer

Article 37 GDPR Identifies three situations in which the data controller or data processor must appoint a DPO in an independent oversight role⁹²³ – if they: (i) are a public sector body; (ii) are a body which processes large amounts of special category data;⁹²⁴ or (iii) undertake large scale, regular and systematic monitoring of individuals in the EU. The appointment may also be required by specific Union or MS law. The DPO must have expert knowledge of data protection law, may be an employee or third party under contract and

⁹²² Compliance evidence example: (a) A record of DPIAs that detect processing that poses a high risk. (b) Correspondence asking the Supervisory authority for guidance on how to proceed with the envisaged processing. (c) A response from the Supervisory authority that offers guidance regarding the processing of the data.

⁹²³ GDPR, Recital 97.

⁹²⁴ GDPR, Articles 9 and 10.

their contact details must be published and provided to the regulator. A DPO is crucial for any organization processing personal data, regardless of whether it is required by the GDPR. The DPO can be formal or informal, full-time or part-time, in-house or outsourced. With the multifaceted nature of data protection, having a designated focal point for data protection matters is essential, ideally in the form of a competent data protection specialist or expert.

Q: The organisation appointed an independent Data Protection Officer (DPO)?

An affirmative answer to the above query implies that a governance process is in place that includes the selection and designation of a DPO. Assigning responsibility for data protection and privacy issues, ensuring the office's independence, providing ongoing funding and resources, resolving conflicts of interest, and emphasising the DPO's oversight of all data processing activities are some of the aspects that must be considered in this process.⁹²⁵

Position of the data protection officer

Article 38 GDPR establishes the role of the DPO within the organisation, mandating participation in all matters pertaining to the processing of personal data, the provision of adequate resources, the maintenance of an independent stance, and the provision of direct

⁹²⁵ Compliance evidence example: (a) A privacy notice that includes the DPO's contact information; (b) Proof that the Supervisory authority has been made aware of the DPO's contact information. (c) Proof of a DPO's qualifications, including the following: Curriculum vitae, credentials, and professional affiliations. c) An organisational chart illustrating the management level to which the DPO reports. d) A job description for the DPO role, and e) evidence of the budget and resources allocated to the DPO role.

reporting to the highest level of management. DPOs are also required to be available to be contacted by data subjects.⁹²⁶ Because the DPO must be involved during the design and implementation of systems that process personal data, they play an important role in the implementation of PbDD.

Measures

As regular communication needs to be maintained between the DPO, senior management, developers, lawyers, engineers and all other stakeholders responsible or accountable for privacy and data protection, a “Privacy Steering Group” should be established to decide on organisational data protection matters. The assignment of responsibility for data protection must thus include the broader organisation while ensuring the funding, resourcing and independence of the DPO⁹²⁷ and emphasising the DPO's duty to oversee all processing activities.⁹²⁸

Tasks of the data protection officer

Article 39 GDPR lays out the tasks and responsibilities of the DPO, which include the following: advising the organisation and its employees of their data protection obligations; monitoring compliance (which includes assigning data protection responsibilities, staff training, and audits); advising on and monitoring DPIAs; cooperating with and contacting

⁹²⁶ GDPR, Recital 97.

⁹²⁷ In this process it is important to address the resolution of eventual conflicts of interest.

⁹²⁸ Otherwise, without the management support and the organisational engagement, the DPO role may be deemed powerless and ineffective.

the supervisory authority as required; and reviewing (and help mitigating through the implementation of TOMs) processing risk. The DPO is also responsible for monitoring ongoing data protection compliance requirements, which includes regularly conducting research to maintain expert knowledge regarding data protection law and practises in order to determine what, if any, changes need to be made to the data protection and PbDD plans, as a result of any developments in legal or regulatory frameworks.

In this context, the following Q&As will assist the controller in identifying the appropriate TOMs:

Q: Does the organisation assign roles and responsibilities to those accountable for data protection and privacy? Are ongoing privacy compliance requirements being recognised by the DPO, such as EU and MS law, case law, codes, and guidelines from the supervisory authority and EDPB?

An affirmative answer to the above query implies that a governance process is in place that includes defining data protection and privacy-related roles within an organisation via job descriptions, contracts, or other means. Moreover, a governance mechanism is in place addressing how the DPO maintains up to date on privacy and data protection law and practises, as well as deciding what modifications to the data protection program may be necessary due to changes in legal or regulatory requirements.⁹²⁹

⁹²⁹ Compliance evidence example: For the position of DPO, there ought to be a job description that addresses the responsibilities detailed in Article 39 of the GDPR. a) A subscription to a privacy law research and news reporting service. Evidence of participation in privacy and data protection conferences. (b) Evidence that legal counsel was sought when required.

Q: Does the organisation provide staff training on data protection and privacy?

An affirmative answer to the above question implies that a governance procedure or mechanism are in place that enables the DPO to enhance the awareness of personnel involved in processing activities and give the necessary training. Additionally, a system or process to record any documentation required to demonstrate compliance are in place.⁹³⁰

This DPPA section corresponds to Chapter IV of the GDPR and provided the DPPA approach to implementing measures related to the responsibilities and obligations of data controllers and processors.

9.3. Implementing PbDD measures allowing for transfers of data to third countries or international organisations

This section considers the PbDD measures related to the transfer of data to third countries or international organisations.

General principles for transfers

Article 44 GDPR establishes that a personal data transfer may take place only if the GDPR data transfer provisions are adhered to. As a result, any organisation that transfers personal data to a third country or international organisation must keep documentation demonstrating compliance with the following provisions: Article 45 GDPR – adequacy;

⁹³⁰ Compliance evidence example: Evidence of the content and delivery of a training and awareness programme (for example, records of professional training provided).

Article 46 GDPR – appropriate safeguards; Article 47 GDPR – BCRs; Article 48 GDPR – not authorised by Union law; and Article 49 GDPR – derogations.⁹³¹

Article 45 GDPR enables the transfer of personal data to a third country or international organisation if the EC determines that the country or organisation provides an adequate level of protection (for example, offers equivalent laws, Regulations, and official compliance mechanisms).⁹³² This is one of the legal bases on which organisations can rely on when exporting personal data outside of the EEA. In general, when transferring personal data to third countries, data controllers and processors will be required to identify and document the legal basis for doing so, therefore, maintaining a record of this decision and ensure that it remains valid for the duration of the transfer.⁹³³

Measures

Article 45 GDPR requires the implementation of appropriate measures to identify the recipient country's inclusion on the EC list of countries with an adequacy decision (for example, monitoring the official list for changes), ensuring that appropriate agreements are in place with third-parties recipients of such data transfers,⁹³⁴ and ensuring compliance with the accountability principle, by updating the organisation's ROPA.

⁹³¹ Article 44 GDPR only implies PBDD actions to ensure compliance with the accountability principle.

⁹³² See also, Recitals 103-107 GDPR.

⁹³³ This record should be included in the organisation's ROPA.

⁹³⁴ See, Article 28 GDPR.

Q: Are documents concerning the transfer mechanism utilised for cross-border data flows kept up to date by the organisation (for example, SCCs, BCRs, and supervisory authority's approval)?

An affirmative answer to the above question implies that a system or process are in place that assists the privacy office in managing international data flows and tracking the utilisation of cross-border transfer mechanisms. (Articles 45, 46 and 49 GDPR should be considered).⁹³⁵

Transfers subject to appropriate safeguards

Article 46 GDPR allows data controllers or processors to transfer personal data to a third country if appropriate safeguards, enforceable data subject rights, and legal remedies are in place. Appropriate safeguards may include: (a) legally binding and enforceable instruments between public bodies; (b) legally binding corporate rules (BCRs); (c) standard contractual clauses (SCCs); (d) an approved Code of Conduct; and (e) an approved certification mechanism. Relying on any of these safeguards would not require express regulatory approvals for the transfer. Alternatively, appropriate safeguards could be introduced through additional contractual provisions; however, these require the express approval of the supervisory authority.⁹³⁶

⁹³⁵ Compliance evidence example: Before a transfer occurs, an inventory of all international data transfers must be created, identifying the reason for each transfer, or documentary evidence that 'inadequate third country' recipients of personal data have been assessed.

⁹³⁶ See also, Recitals 108 and 109 GDPR.

Measures

To comply with Article 46 of the GDPR, it is crucial to establish and implement measures that address cross-border data flows. These measures must include the establishment of robust systems and processes to maintain comprehensive records of the transfer mechanism employed for such data flows (for example, SCCs, BCRs, approvals from the regulator).

Q: When transferring data outside the EEA, does the organisation make use of any contractual agreements (for example, Standard Contractual Clauses)?

An affirmative answer to the above question implies that a governance measure is in place to assist with the use of Standard Contractual Clauses for transfers to third countries.⁹³⁷

Q: Are approvals from the supervisory authority required prior to any data transfer?

An affirmative answer to the above question implies that a mechanism is in place to engage the supervisory authority in the process of approving a data transfer to a third country.⁹³⁸

Q: Does the organisation rely on adequacy or one of the derogations (for example, consent, performance of a contract or public interest) as a basis for data transfer?

An affirmative answer to the above question implies that a process is in place to address the use of exemptions to the requirement to send

⁹³⁷ Compliance evidence example: Including the EU Standard Contractual Clauses in contracts with data importers or exporters.

⁹³⁸ Compliance evidence example: Decisions made by the Supervisory authority authorising the transfer (approval of contractual safeguards in data protection agreements with data importers or exporters, for instance).

personal data to third countries that provide an "adequate" level of privacy protection. (Applies to Articles 45, 48 and 49 GDPR).⁹³⁹

Binding corporate rules (BCR)

Article 47 GDPR explains the criteria for BCR approval. If using BCRs as a data transfer mechanism, approval applications must ensure that the BCRs meet the specified content requirements.⁹⁴⁰ Formalities may affect, for example, contractual terms, compliance arrangements and liabilities, therefore, the Data Protection Officer must be consulted to confirm that they meet the requirements described in this Article and are appropriate for the specific transfer of personal data.

Q: Does the organisation transfer data outside the EEA using Binding Corporate Rules (BCRs)?

An affirmative answer to the above query implies that a governance procedure is in place for implementing, authorising, and monitoring a set of corporate rules that can be utilised as a legal framework for moving data between corporate members, hence managing data transfers between corporate groupings.⁹⁴¹

⁹³⁹ Compliance evidence example: (a) A data transfer inventory that identifies international data transfers and provides the reason for each transfer. (b) Data subject consent forms, including an explanation of the potential risks caused by a lack of suitable measures. (c) A determination that weighs the data controller's legitimate interests against the individual's rights and freedoms.

⁹⁴⁰ See also, Recital 110 GDPR.

⁹⁴¹ Compliance evidence example: (a) Adoption of binding corporate rules (b) Monitoring outcomes of the BCR (such as audits), or (c) A current overview of the extent and coverage of the BCR.

Transfers or disclosures not authorised by Union law

Article 48 GDPR addresses the circumstances under which data controllers or processors may rely on the decision of a court or tribunal in order to transfer personal data to a third country.⁹⁴²

Measures

The controller must consider what TOMs are required to be in place in order to identify the use of a data transfer mechanism that is based on either an adequacy decision or one of the derogations, such as consent, the performance of a contract, or public interest. Specifically, this action implies relying on derogations to the requirement to send personal data to third countries that provide an "adequate" level of protection for personal data. In general, the implementation and maintenance of procedures for responding to requests from law enforcement are two of the accountability mechanisms that should be considered in relation to Article 48 GDPR. Other accountability measures include the registering of legal advice relating to the disclosure of personal data and the Court order decision requiring the transfer of personal data.

Derogations for specific situations

Article 49 GDPR identifies the conditions under which personal data may be transferred to a third country in the absence of an adequacy decision or other appropriate safeguards, namely; (a) with the data subject's explicit consent; (b) for contract performance or pre-contractual measures; (c) for important reasons of public interest; (d) for the

⁹⁴² See also, Recital 115 GDPR.

establishment, exercise, or defence of legal claims; (e) to protect a person's vital interests; (f) for transfers made from public registers in certain cases; and (g) in the data controller's compelling legitimate interests.⁹⁴³ Where none of the above conditions apply, and transfers cannot be based on an adequacy decision or appropriate safeguards, a transfer may take place only if it is not repetitive,⁹⁴⁴ concerns a small number of data subjects and is required for the purposes of the data controller's compelling legitimate interests, provided that the data subject rights do not prevail.

Measures

In this scenario, the TOMs must include the implementation of mechanisms and systems to document the use of derogations.

This DPPA section corresponds to Chapter V of the GDPR and provided the DPPA approach to implementing measures related to the transfers of personal data to third countries or international organisations.

⁹⁴³ See also, Recitals 111-114 GDPR.

⁹⁴⁴ See, Article 29 Working Party (2005), Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995, WP 114, Brussels, 25 November. The WP29 advises that relying on derogations for specific situations must be exceptional, based on individual cases, and cannot be used for mass or repetitive transfers.

9.4. Implementing PbDD measures in the context of the provisions relating to specific processing situations

This section delves into the measures that pertain to the provisions related to specific processing situations.

Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

Article 89 GDPR ensures that processing carried out for public interest archiving, scientific or historical research, or statistical purposes is subject to appropriate safeguards, including data minimisation. Therefore, processing should make extensive use of pseudonymised or anonymised data. In addition, Union or MS law may exempt processing for these purposes from the GDPR provisions governing data subject rights.

Measures

In compliance with Article 89 of the GDPR, it is essential for the controller to establish and implement systems or processes that facilitate the adoption of appropriate TOMs. These measures should include the formulation of policies and procedures for the de-identification of personal data and the integration of data protection into research practices. This includes mechanisms to obtain personal data for research purposes, ensuring the acquisition of valid consents, a process for de-identifying data whenever possible, and taking measures to ensure that research data maintained for scientific, historical, or statistical research is protected from improper use, by application of privacy enhancing tools such as encryption and access restriction. In addition, organisations must implement specific TOMs to ensure compliance with the data minimisation principle. The

controller must also include a procedure to maintain a registry of research ethics approvals that address data protection and privacy challenges.⁹⁴⁵

Q: Does the organisation have policies and procedures in place to de-identify personal information?

An affirmative answer to the above question implies that a system or process are in place to ensure that data minimisation procedures are implemented in the organisation's data processing operations.⁹⁴⁶

Existing data protection rules of churches and religious associations

Article 91 GDPR determines that churches, religious associations, and communities that process personal data in accordance with comprehensive rules are permitted to continue doing so as long as those rules are brought into compliance with the GDPR.⁹⁴⁷

Measures

The TOMs that are deemed appropriate for compliance with Article 9 of the GDPR are those that relate to the specific data processing obligations that apply to organisations handling special category data, which includes information pertaining to religious or philosophical beliefs (Article 9 GDPR). This may include the implementation of measures such as

⁹⁴⁵ See also, Recitals 156-162 GDPR.

⁹⁴⁶ Compliance evidence example: (a) Policies and procedures for data minimization, pseudonymization, or anonymization. (b) Approval by an ethics committee that addresses data minimization and privacy protection. c) The use of technology that leads to the pseudonymization or anonymization of personally identifiable information.

⁹⁴⁷ See also, Recital 165 GDPR.

encryption and pseudonymisation. Additionally, the controller must address the need to implement specific organisational policies related to data protection and privacy.⁹⁴⁸

Scope of GDPR

It is important to note that the controller must consider the application of the DPPA in terms of: a) material scope,⁹⁴⁹ the GDPR is applicable to the processing of personal data by automated means (e.g., computers and other digital devices) as well as the processing of personal data by means other than automated means (e.g., paper records) that form part of a filing system or are intended to become a filing system;⁹⁵⁰ b) territorial scope,⁹⁵¹ it applies to data controllers who are established in the EU and who process personal information about data subjects within the context of those establishments.⁹⁵² Additionally, GDPR applies to controllers outside of the EU who process personal data in order to provide goods and services or monitor the behaviour of data subjects residing in the EU.

⁹⁴⁸ See, 7.1.1. and 7.1.2.

⁹⁴⁹ GDPR, Article 2.

⁹⁵⁰ Includes any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

⁹⁵¹ GDPR, Article 3.

⁹⁵² A controller's main establishment in the European Union will be the place from which it makes most of its decisions regarding the purpose and means of its data processing activities. The administrative centre will be the main location for a processor in the EU. The controller who is located outside the EU must appoint a representative for the purposes of dealing with supervisory authorities in the jurisdiction in which the controller operates.

Supervisory authorities

Data controllers are liable for, and must be able to demonstrate, compliance with the data protection principles. Consequently, in most EU countries, national data protection authorities have been set up to act as “the guardians of privacy”. supervisory authorities are given the power to investigate and take action against violations of data protection laws, as well as the responsibility to raise awareness of data protection rights and obligations generally.⁹⁵³ In addition, effective cooperation between data protection authorities ensures greater consistency of data protection across the EU.⁹⁵⁴ The effectiveness of supervisory authorities is reinforced in the EU by the requirement that they must be independent of any political, governmental, or other influence.⁹⁵⁵ Article 16(2) TFEU and Article 8(3) CFR both require supervisory authorities to be independent. The CJEU has repeatedly emphasised that control by an independent body is an essential component of the right to data protection and has established the criteria for such independence: the supervisory authority must act with complete independence - implying decision-making power independent of any direct or indirect external influence. The CJEU also emphasised the critical role of EU independent supervisory authorities in protect individuals whilst facilitating the free flow of data,⁹⁵⁶ as well as controlling international transfers to non-EU countries.

⁹⁵³ See, Recital 117 GDPR for the establishment of supervisory authorities; Recital 118 GDPR for monitoring of the supervisory authorities; Recital 119 GDPR for organisation of several supervisory authorities of a Member State; Recital 120 GDPR for features of supervisory authorities; and Recital 122 GDPR for responsibility of the supervisory authorities.

⁹⁵⁴ GDPR, Article 61.

⁹⁵⁵ See, Recital 121, GDPR for independence of the supervisory authorities.

⁹⁵⁶ The CJEU determined, e.g., that supervisory authorities must establish ‘a fair balance between the protection of the right to private life and the free movement of personal data.’ *Case C-518/07 European Commission v Federal Republic of Germany (GC) EU:C:2010:125, [2010] ECR I-01885.* (para 30).

Chapter 10 – Overarching conclusions

This thesis focused on discussing how organisations must implement Data Protection by Design and Default (PbDD) to safeguard personal data and ensure effective compliance with the GDPR. By synthesising the core arguments, research methodology, insights gained, limitations, and future research directions, this concluding chapter provides a comprehensive overview of the study's outcomes and sets the stage for further exploration in this increasingly important area of law. The primary objective of my study was to propose a methodology for implementing PbDD in accordance with the legal framework of the GDPR. To achieve this goal, this research addressed the challenges faced by businesses during the implementation of PbDD and presented an operational framework to alleviate the compliance burden. This framework, named Data Protection Principles Approach (DPPA), aims to identify, analyse, and emphasise the essential requirements of PbDD within the context of the GDPR. In pursuit of this objective, my research explored a range of pertinent questions that guided the development of the DPPA. Some of these key questions include:

- Which data protection principles should be implemented when processing personal data?
- What do we mean when we talk about personal data?
- What are the rights of the data subject, and how may they be accommodated into data operations?
- How are organisations affected by GDPR?
- What are the main obligations of a data controller (and processor)?
- Which GDPR Articles are relevant for its implementation?

- What and which 'appropriate TOMs' are available within the meaning of the GDPR?

Unlike the accountability approach, which places emphasis on demonstrating compliance with the Regulation through internal controls, the DPPA focuses on the application of the data protection principles and ensuring data controllers' adherence to the rights of data subjects. The DPPA provides a practical guide for organisations to simplify the GDPR implementation process and identify appropriate measures for each relevant GDPR Article and processing activity. By highlighting the potential benefits of integrating PbDD into operational practices, the DPPA underscores the importance of aligning data protection with organisational objectives and values.

In terms of the applied methodology, the investigation that led to the development of the DPPA involved a systematic examination of fines issued by EU supervisory authorities. The insights gained from these cases enabled a deeper understanding of the issues surrounding the implementation of PbDD and the GDPR. Through the analysis of fines, exploration of relevant literature, and examination of case law, this study has identified key factors that influence the effective implementation of PbDD. These findings have played a crucial role in informing the development of the DPPA, ensuring its applicability and robustness, even in the presence of emerging technologies.

Throughout this study, several key issues pertaining to the implementation of PbDD have been identified and explored. These issues encompass a lack of awareness and understanding of the PbDD concept, which poses challenges in effectively incorporating it into organisational practices. This highlights the critical need for comprehensive education

and widespread dissemination of knowledge regarding the role of PbDD in upholding GDPR principles and protecting the rights of data subjects among the relevant stakeholders.

Moreover, this thesis presents conclusive evidence that the incorporation of PbDD into existing organisational processes and systems poses a notable challenge. Specifically, the discussion highlights the impracticality of implementing PbDD into emerging technologies such as AI, Blockchain, and IoT. This reveals that achieving an optimal balance between protecting privacy and fostering innovation presents an additional significant challenge that requires urgent attention. In this regard, it was concluded that navigating the delicate equilibrium between adhering to data protection Regulations and promoting the advancement of emerging technologies is not always feasible. Striking the right balance between stringent data protection measures and fostering innovation can be challenging. However, it may be necessary to prioritise robust data protection measures to avoid compromising individuals' privacy rights, considering the current state of the art.

Furthermore, the realm of technology introduces its own set of challenges. Issues such as legacy data retention and destruction, robust data security measures, and the practical implementation of the principle of data minimisation were thoroughly addressed and critically examined in this work. The conclusions drawn from these examinations played a pivotal role in the development of the DPPA. These conclusions highlight the importance for organisations to establish proper protocols and processes for handling legacy data to ensure compliance with the GDPR and mitigate potential risks associated with data breaches. They also emphasise the significance of implementing mechanisms for efficient encryption, access controls, regular security audits, and ongoing monitoring of data security practices. Additionally, they underscore the importance of collecting and storing only necessary personal data, regularly reviewing data collection practices, and ensuring

that data retention periods are appropriate and justified. Together, these findings informed the development of the DPPA and its comprehensive approach to addressing data protection challenges and aligning with the requirements of the GDPR.

While the DPPA framework offers practical guidance for achieving GDPR compliance, it is important to acknowledge its limitations. This study is not without constraints, such as the reliance on publicly available data for the analysis of GDPR fines and its limited scope. However, these limitations provide opportunities for future research to explore and delve deeper into these areas. Moving forward, further research is warranted to address the questions that have emerged from this study. Areas of future investigation may include refining the DPPA framework based on additional case studies, evaluating its effectiveness in diverse organisational contexts, and exploring its adaptability to future regulatory developments. These investigations will help address the challenges posed by emerging technologies and ensure the framework remains relevant and effective in safeguarding data protection in evolving regulatory landscapes.

The following sections delve into the fundamental aspects of the research and provide a synopsis of the findings.

10.1. Enhancing data security

Every individual in the EU has the right to the protection of his or her personal data, as well as the right to know and determine how his or her personal data is used, kept, protected, transferred, and deleted. It is widely recognised that the fundamental principle of "integrity and confidentiality" is indispensable in safeguarding personal data, preventing infringements upon the rights and freedoms of data subjects that may arise from

accidental, unauthorised, or unlawful access, use, modification, disclosure, loss, or destruction of that data. PbDD plays a critical role here, as the GDPR mandates organisations to implement appropriate measures in the scope of data security, which may include anonymisation and pseudonymisation, depending on the circumstances of processing. As we have seen, there is currently no best practice or even a “magical” tool that can provide a mechanism to ensure complete data security; the obstacles and challenges are numerous and diverse, both internal – such as human error, and lack of requisite skill sets, and external – such as systems hacking. The inclusion in the DPPA of a functional list of TOMs, specifically addressing the security of systems and processing activities, represents a significant step in addressing an existing gap in the GDPR.

The limits of PbD legacy approaches to data protection and security are becoming increasingly apparent, primarily due to the rapid evolution of technology and the increasing sophistication of cyber threats. These factors make it difficult to implement and maintain a PbDD-based security framework. Additionally, some argue that PbDD alone may not be sufficient to protect privacy and that a more comprehensive approach, such as the data principles-based approach, may be required to ensure effective data security and protection. Therefore, future interdisciplinary research must explore new pathways for incorporating PbDD into modern data processing activities and systems, with a focus on individuals' rights and data protection principles, rather than risk management. This approach requires less emphasis on developing risk mitigation measures and more on measures that eliminate risk from the outset of data processing. Although stricter, this strategy, grounded on the ‘hard core’ data protection principles⁹⁵⁷ is outlined in the DPPA,

⁹⁵⁷ Tzanou (n 6).

'by recognizing a 'core' or 'essence' of the right to data protection that cannot be subjected to restrictions.'⁹⁵⁸ I posit that, particularly when applied to special categories of personal data, this approach is likely to aid organisations in achieving GDPR compliance more effectively and augment the safeguarding of individuals' privacy.

To assist organisations in attaining a high level of compliance maturity, this work provides the necessary tools for integrating PbDD into modern enterprise systems and activities, including those that leverage novel, emerging technologies. My research led to the identification of appropriate TOMs in relation to each of the GDPR requirements (on an Article-by-Article basis), resulting in a strategy to PbDD implementation that considers, (in addition to the measures indicated by the GDPR, such as pseudonymisation and anonymisation): a) the implementation of mechanisms and systems to integrate data protection into an information security policy; b) the implementation of mechanisms and systems to integrate and maintain technical security measures from the outset of processing activities; c) the implementation of mechanisms and systems to integrate and maintain measures to encrypt personal data; and d) the implementation of mechanisms and systems to limit the processing of personal data, whenever it is possible to do so.

Furthermore, the DPPA complements the security requirements articulated in the GDPR by offering incentives for data controllers to include procedures for periodic data security and cybersecurity reviews in their PbDD plan (e.g., penetration testing), procedures for incorporating privacy risks in data security risk assessments, and procedures for establishing and maintaining privacy requirements for third parties (e.g., customers, suppliers, and data processors). These measures encourage data controllers to adopt

⁹⁵⁸ *ibid.*

robust security practices and prioritise data protection throughout their data processing activities, aligning with the stringent requirements set forth by the GDPR.

Given that GDPR compliance and accountability can also be demonstrated through industry certifications such as ISO certification, SOC 2/3 certification, or ITIL certification, this research aligns the proposed TOMs with external high-level information security controls. This alignment effectively creates an intersection between law and technology, bridging the gap between legal requirements and industry-recognised best practices in information security. Other crucial elements of data security are identified to ensure the confidentiality and integrity of personal data in line with GDPR requirements. Organisations must implement both technological measures, such as firewalls and anti-virus software, and organisational measures, such as security guidelines and policies. These measures work in tandem to establish a comprehensive data security framework within the PbDD plan, safeguarding personal data from unauthorised access or compromise. The implementation of an information security policy is also emphasised in this work as a crucial measure to provide comprehensive guidance on maintaining the security and confidentiality of all processed personal data. Considering that the principles of integrity and confidentiality have practical implications for how organisations operate, this work addressed these implications, focusing on the mechanisms necessary to ensure proper data storage, secure access to personal data, secure data transfer, and the secure disposal of data.

10.2. Safeguarding data Protection Principles

One of the key insights derived from the analysis of GDPR fines issued by the EU supervisory authorities is the need for organisations to adapt their service delivery approach in accordance with the GDPR. This requires a comprehensive understanding of data subjects' privacy concerns, highlighting the importance of a deeper comprehension of data protection issues in the provision of services. To meet the requirements of the GDPR, organisations must consider the principles of data protection outlined in Article 5 GDPR and conduct periodical reviews of their measures, policies, and organisational procedures for the collection, further processing, and protection of personal data. It should be noted that many of the GDPR's requirements are not explicitly defined in the Regulation, leaving room for interpretation. This is particularly evident in the case of PbDD, where the adoption of suitable "TOMs" is a major concern that this study successfully addressed and resolved.

The data protection principles act as a fundamental framework for the just and lawful processing of personal data. By issuing fines for non-compliance with these principles, supervisory authorities aim to motivate organisations to adopt strong data protection practices, abide by the law, and uphold individuals' rights. The data protection principles are central to the GDPR, and the Regulation mandates their integration into an organisation's processing activities through PbDD. Organisations are required to process personal information fairly, lawfully, and transparently when collecting, storing, using, sharing, and disposing of it. They must explain to the data subject why they are collecting the information and use it solely for that stated purpose. Only the personal data needed for the stated purpose should be collected – no more, no less. Furthermore, organisations must keep personal data accurate and up to date for only as long as necessary before

securely destroying it (or anonymise it). To ensure that personal data is handled properly, they must keep it safe, follow data protection principles and demonstrate that they have done so. It is worth noting that, as evidenced by the analysis of fines data, non-compliance with the general data protection principles attracts the highest number of fines under the enforcement of the GDPR.

This work provides a framework that makes it easier for organisations to understand and implement appropriate measures to ensure the lawful processing of personal data. Furthermore, this research highlights the imperative that personal data must not be processed in a manner that causes harm to data subjects or involves unexpected or misleading processing. It provides controllers with guidance on how to effectively achieve this objective. Moreover, it assists organisations in upholding complete transparency, openness, and honesty regarding the purposes of personal data processing.

Data controllers must be prepared to incorporate appropriate measures into the systems and processes that process personal data in order to comply with the GDPR principles. They must also be ready to demonstrate compliance in light of the accountability principle. In pursuit of this objective, this work offers valuable recommendations for systematically integrating data protection principles and accountability mechanisms into the systems and processing activities of organisations. These recommendations provide an innovative and effective strategy for achieving GDPR compliance, resulting in a significant advancement in the operationalisation of the Regulation. Although the study does not provide an exhaustive list of TOMs available to organisations – since each case is unique – it undoubtedly paves the way for a more efficient methodology to integrate the legal concepts into the operational activities in accordance with the state of the art, the implementation costs, and the risks of the processing activity.

By analysing the penalties levied by EU supervisory authorities, it was possible to determine that the primary personal data processing risks stem from inadequate PbDD implementation, namely failing to prepare for a data breach, failing to obtain data subject consent, and mishandling personal data in online environments. It is worth noting that organisations that place less reliance on risk mitigation are more likely to successfully implement the data protection principles, thereby achieving compliance with the Regulation more easily. Arguably, this approach will test organisations' intentions and capacity to protect the fundamental rights and interests of data subjects, as well as their resilience to withstand potential data breach attempts. While prevention is essential, threats are rarely eliminated by risk mitigation.

Therefore, this work highlights that while eliminating risk may restrict an organisation's commercial flexibility and, to some extent, impede innovation, it will undoubtedly enhance business continuity in the event of a data breach and provide better protection for the rights and freedoms of data subjects. Successful businesses will surely reap the benefits of effectively addressing data security and protection concerns by employing procedures that make risk elimination the most effective data protection tool. Win-win approaches, which are frequently based on business economic reasoning, do not always provide the best long-term outcome, especially if the result of a data breach is a hefty fine; up to 10 million euros, or, in the case of an undertaking, up to 2% of its entire global turnover for the preceding fiscal year, whichever is greater, as well as irreparable reputational damage. An organisation that chooses not to utilise technologies such as social listening, social monitoring, and profiling when the principles of data protection cannot be implemented, is a good illustration of risk elimination in practise (for example, do not carry out the processing activity if the data subject cannot be provided with data

protection information in accordance with Article 13 GDPR). Another example would be that an organisation refrains from entering into a service contract with a third party (data processor) that cannot ensure the security of personal data or that involves the international transfer of personal data to third countries that do not provide data protection standards equivalent to those of EU member states (as previously mentioned, the United States is an example of a country lacking comparable legislation, yet it is the single country that imports the most personal data from the EU).

In this work, I also investigated the compatibility of new and emerging technologies with the GDPR's PbDD. The aim was to identify areas of compliance that are currently challenging for organisations to achieve, potentially representing a "command that cannot be obeyed" in terms of PbDD implementation. These areas necessitate special attention from the legislator due to their increasing importance and the evolving nature of technology, which poses risks to privacy and presents inherent challenges in ensuring effective data protection. I consider this research important since the majority of GDPR requirements stem from the data protection principles that PbDD is responsible for incorporating into processing activities - it is impossible to discuss GDPR compliance without basic adherence to these core principles. The findings of this study indicate that the incorporation of PbDD into these technologies is inherently impractical from an operational point of view. Consequently, a relationship between the principles of data protection and emerging technologies (IoT, Blockchain, Big Data) is extremely difficult to achieve due to the challenges (mostly technological limitations) associated with PbDD implementation. Additionally, it has been difficult to design corrective mechanisms that could help address these challenges, namely through the use of PETs. Large-scale studies will be necessary to evaluate the suitability of PbDD for emerging technologies and,

consequently, the feasibility of integrating data protection principles and individual rights into them. It is evident that for emerging technologies to gain trust and acceptance, appropriate measures, including specific PETs, need to be developed to mitigate their privacy risks.

To assist organisations in addressing this challenge, this work presents an approach to personal data processing in new technologies that focuses on risk eradication rather than mitigation. However, while risk eradication is a noble goal, its practical implementation can be challenging due to feasibility, resource intensity, and technological complexities. A pragmatic approach involves thus a combination of risk eradication for critical elements and robust risk mitigation strategies where complete eradication is not practical. This approach entails conducting a DPIA to assess the potential risks to the rights and freedoms of data subjects. If the DPIA identifies a high risk, the data controller should explore alternative methods of processing. If no suitable alternatives are available and the processing activity must proceed, the controller should then adhere to the principle of data minimisation. This involves identifying the specific purpose of the processing activity and ensuring that only the necessary personal data are collected and processed for that purpose. From the outset, to comply with the principle of data minimisation, the data controller must take two steps: first, the purpose of processing personal data must be determined, and second, each proposed processing activity must be deemed as necessary in respect of that purpose. It is important to note that, as suggested by the DPPA, the cyclical deletion of excess or unnecessary personal data, along with the implementation of measures to ensure data minimisation throughout the processing lifecycle, plays a critical role in all data protection operations.

10.3. Data subject rights: Ensuring compliance and operational efficiency

The rights to privacy and data protection are established in the EU Treaties and in the EU Charter of Fundamental Rights. Article 8 CFR states that personal data must be protected. On the very top of the EU legal hierarchy, these rights aim to protect individuals' autonomy and dignity and they are a precondition for the exercise of other fundamental rights and freedoms, such as the freedom of expression and religion. When putting the individual's rights into practise, freedom of expression, economic interests and professional secrecy must also be taken into account.

The GDPR determines the implementation of TOMs to ensure observance of the following data subject's rights: right to be informed; right to access to personal data; right to rectification; right to erasure; right to restrict processing; right to data portability; right to object processing; and the right to not to be subject to a decision based solely on automated decision making, including profiling. In addition, it requires data controllers to provide information to data subjects in a concise, transparent, intelligible, and easily accessible form, using clear and plain language, whether through privacy notices, communications regarding access, rectification, correction, and objection rights, or as part of breach notifications, for which, the controller must establish and maintain appropriate safeguards.

This work has significantly focused on the implementation of TOMs to facilitate the processing operations required for the fulfilment of data subject rights. This encompasses the development of systems, policies, and procedures aimed at effectively responding to requests for personal data access. The study particularly delved into the examination of mechanisms and systems for locating and retrieving personal information from an

organisation's data repositories. Furthermore, it placed emphasis on the significance of implementing and maintaining internal procedures and systems to effectively manage any associated processing activities. This encompasses the establishment of appropriate communication systems to keep individuals informed about the status of their personal data.

The analysis of fines by EU supervisory authorities revealed that non-compliance with data subject rights encompasses various violations. These violations include failure to respond to data subject requests within the designated time frame, providing insufficient or inaccurate information in response to such requests, or failing to provide any information at all. Furthermore, organisations may face fines for obtaining inadequate consent for processing personal data or for exceeding the scope of consent granted by the data subject. My research on GDPR fines indicates that regulators take non-compliance with data subject rights very seriously as these violations can have a significant impact on individuals. It is important to note that the fines imposed by EU supervisory authorities also act as a deterrent for organisations that may not be adequately prioritising the requirements of the GDPR. Furthermore, these fines serve to convey to the public that the GDPR is being actively enforced, and that individuals' rights and freedoms are being safeguarded.

This thesis addresses this aspect of compliance by providing practical examples of TOMs that can be applied to implement the obligations related to the rights of data subjects set out in Chapter 3 of the GDPR. Alongside the data protection principles, the observation and compliance with these criteria constitute the foundation of the presented DPPA framework, which implementation can also be used by organisations to provide evidence of compliance and accountability.

As emphasised throughout this work, there are instances where risk mitigation measures may inadvertently infringe upon the rights of data subjects. In other words, sometimes risk mitigation might result in taking away data subject's rights. Some authors have suggested that organisations maintain parallel systems with the explicit purpose of safeguarding these rights. However, this approach may not be practical in terms of data minimisation and storage limitation. Systems created to retain data for the purpose of facilitating access, erasure, and objection, as well as systems designed to process additional data, potentially supplied by the data subject, for re-identification purposes, would result in duplicating existing personal data into new datasets or subsets of data. This duplication is likely to amplify the risks associated with processing personal data.

Privacy-enhancing technologies (PETs) must be incorporated into the systems responsible for processing personal data to effectively handle tasks such as data erasure or data location without the need for data duplication. It is equally crucial to include data at rest, including archives and backups, in this process. PETs should enable real-time execution of these tasks while ensuring data privacy and security. Although this thesis presents a range of TOMs, including spiders, data crawlers, and SQL scripts, that can assist data controllers in integrating PbDD into their business operations, it is important to acknowledge that the software industry has not fully embraced the integration of these tools "by design." In other words, there is still a significant gap to be bridged before these measures become commonplace in software development. Until then, achieving effective GDPR compliance will continue to pose challenges for organisations.

The storage limitation principle represents a particular challenge in meeting data subject rights obligations when legacy data is present in an organisation's data ecosystem. This work specifically addressed this issue, with a particular focus on it during the

development of the DPPA operational framework. The analysis of the data related to GDPR fines further supports the notion that adopting a more stringent approach to data storage management is the optimal choice for ensuring compliance with data protection requirements and safeguarding the rights and freedoms of data subjects. However, it should be acknowledged that in certain cases, implementing a stringent approach may not be feasible due to the specific nature of the personal data processing involved. For example, there may be situations where an organisation is obligated to retain data for extended periods to meet other legal obligations, or where processing health data is necessary for monitoring a patient's medical history. In such scenarios, the approach advocated by the DPPA is to implement the principle of data minimisation alongside robust data cataloguing methods, preferably operating on encrypted data containers.

In conclusion, ensuring compliance with data subject rights is a significant concern in the field of data protection, and regulatory bodies are taking steps to enforce GDPR requirements. As a result, this work has placed a particular emphasis on the complex task of designing and maintaining systems and procedures to address data subject requests, including the right to be forgotten. This entails fulfilling several functional requirements, such as identifying stored data, authenticating access, and carrying out data erasure, including data at rest (e.g., backups and archives). When it comes to data erasure in response to a request to be forgotten, the DPPA suggests implementing PbDD measures that encompass data erasure, anonymisation, or, in certain circumstances, rendering the data beyond use.

10.4. The GDPR Articles relevant to the implementation of PbDD

An important aspect of this work is its ability to assist businesses in identifying and prioritising their compliance efforts beyond the legal language of the GDPR. It goes beyond merely explaining the legal text in a way that laypersons can understand. Instead, it provides valuable operational guidance by highlighting specific actions that need to be taken to ensure GDPR compliance. This fills a gap in the Regulation that has been identified by many scholars and practitioners, as it helps bridge the divide between theory and practice. The thesis explicitly focuses on the GDPR Articles that require operational action from data controllers and provides practical recommendations for implementing suitable TOMs. By doing so, it helps organisations meet their compliance obligations effectively.⁹⁵⁹ Moreover, this work offers organisations unequivocal and precise guidance on the measures necessary to meet their GDPR obligations. It also provides valuable insights to ensure the effective implementation of these measures. As a result, organisations can have increased confidence in their compliance efforts, as they are guided by specific requirements supported by the DPPA.

Additionally, the presented approach outlines the essential steps for establishing a data protection program, which is built upon the successful implementation of data protection principles and mechanisms to uphold data subject rights through PbDD. Furthermore, it provides an extensive list of additional TOMs to assist data controllers in demonstrating compliance and accountability.

⁹⁵⁹ See Annex 5 for a list of GDPR articles requiring PbDD implementation.

When adopting this approach to GDPR compliance, the first step for the data controller is to conduct a "gap analysis" to assess the organisation's *status quo* in meeting the general GDPR requirements. This involves investigating the scope of the business's activities related to data subjects, any involvement of third parties in processing operations, the information assets used, the existing security controls, and the organisational aspects of the business, including contracts, policies, and notices.

The thesis also argues for the establishment of a robust governance structure that includes key stakeholders such as the Data Protection Officer (DPO), Chief Information Security Officer (CISO), Legal Counsel, and departmental roles responsible for data protection, such as privacy champions. It is crucial to determine and allocate operational tasks and roles across the organisation's data protection network, involving all employees with responsibilities for processing personal data. An essential aspect for the operationalisation of the GDPR is the formation of a data protection steering group, comprising key internal stakeholders and, if feasible, an external consultant representing the interests of data subjects. The outcomes of the group's meetings should be communicated to all employees, who should also receive up-to-date training relevant to any new or changed processing operations. This can be included as part of the training and awareness programme, serving as regular refresher training.

It is my belief that the proposed methodology serves as a practical tool to facilitate data protection governance and operationalise the GDPR in a manner that can be customised to meet the specific needs of each organisation. Although the presented operational framework emerges from the trends identified in the analysis of GDPR fines issued by the EU supervisory authorities, which primarily relate to the electronic processing of personal data and encompass issues such as large-scale processing and non-compliance

with digital data security and protection requirements, the DPPA is intentionally designed to be industry-neutral and, to the greatest extent possible, technologically neutral. Its objective is to identify legal and operational gaps and provide practical recommendations to address these gaps.

10.5. Contributions and future work

This thesis introduces a new approach to operationalising GDPR through PbDD, drawing on previous research in the literature, advancements in the state of the art, and the findings of a comprehensive analysis of GDPR fines issued by EU supervisory authorities from May 2018 to December 2022. Furthermore, this study makes a significant contribution to the existing literature on PbDD and data protection through a comprehensive analysis of current legislation and practices regarding GDPR implementation. The research identifies key issues and proposes an approach to compliance that goes beyond traditional commercial economics and risk management strategies. This user-centric approach prioritises data protection principles and the respect for data subjects' rights, leading to a more comprehensive and equitable approach to the processing of personal data.

This thesis presents compelling evidence that the current approach of PbDD to GDPR implementation, particularly in the realm of emerging technologies, results in a "command that cannot be obeyed." However, it acknowledges that by adopting a more stringent approach to data protection principles and data subjects' rights, PbDD has the potential to become a highly effective tool for ensuring compliance with the legislator's objectives. Regrettably, without additional research into novel approaches to address the

intricate processing areas discussed in this thesis, such as blockchain, IoT, and AI, the goals established by the EU legislator in enacting the GDPR may not be fully achieved.

Furthermore, this thesis emphasises the significance of establishing a GDPR implementation framework that is firmly based on the PbDD requirements outlined in Article 25 of the GDPR. The adoption of the DPPA can significantly aid organisations in enhancing the effective implementation of the core data protection principles, integrating essential safeguards into their data processing operations to meet GDPR standards, and safeguarding the rights of data subjects. This approach is in contrast to a risk mitigation strategy that prioritises the organisation's interests over the protection of data subjects.

The conducted study outlines the appropriate TOMs that align with the provisions of the Regulation, in addition to those already identified in the GDPR. It also identifies instances where there is a misalignment between data protection requirements and data security practices within organisations engaged in the processing of personal data. Additionally, the research brings attention to operational conflicts that may arise between legal norms and emerging technological advancements. This analysis, specifically focusing on PbDD and presented in a well-structured manner, makes a significant contribution to the existing data protection literature.

The proposed DPPA framework is not specific to any particular economic sector. It is designed to contribute to various business areas, systems processing personal data, and processing activities. The framework encompasses neutral security measures and allows for the integration of a wide range of Privacy Enhancing Technologies (PETs) that address specific requirements.

This thesis streamlines the process for the Privacy Office to identify and resolve issues related to specific processing activities in relation to GDPR Articles, requirements,

and obligations. It provides a clear scope of application for PbDD in terms of data security and data protection requirements. The DPPA guides the expedited identification of operational concerns by mapping the relevant GDPR Articles and implementing suitable measures to address any conflicts that may arise between the processing activity, legislation, and technology. This methodology also benefits Data Protection Officers (DPOs) by providing a mechanism to select the appropriate TOMs for implementing data protection requirements.

Furthermore, the DPPA has been developed with a specific emphasis on the requirements outlined in the GDPR, ensuring full compliance with the Regulation. This means that the framework is not merely theoretical but is firmly grounded in a practical context. This practicality can assist EU regulators in making well-informed decisions regarding personal data protection and compliance in the future.

Subsequent research has the potential to build upon the findings of this study by exploring the efficacy of the DPPA framework from various perspectives. This could involve assessing its effectiveness in managing restricted data transfers, ensuring data portability, addressing liability issues, and examining its validity and resilience in diverse business scenarios. Furthermore, there is a need for additional research to delve into the theoretical foundations of data protection by design and by default, particularly in relation to its future implications for emerging technologies. This research could explore how the concept of TOMs evolve to address novel and emerging technologies.

The work presented in this thesis provides an original perspective to the existing body of knowledge by systematically mapping out operational actions for PbDD to ensure compliance with the GDPR. In addition to identifying data security models and specifying suitable TOMs for each relevant GDPR Article, this thesis takes a practitioner's viewpoint,

addressing the practical challenges encountered in real-life scenarios. It offers practical insights and solutions that can be applied by organisations to overcome common hurdles in achieving GDPR compliance.

Furthermore, the thesis highlights the significant operational challenges that arise within the current landscape of data protection law and technology. It brings attention to the complexities and intricacies involved in aligning operational practices with the requirements of the GDPR. The extensive work involved in exploring new technologies has resulted in significant advances in understanding the challenges posed to privacy and data protection, enabling the integration of the findings into the solutions provided by the DPPA. Considering the extensive scope, rapid pace of development, and continually evolving nature of emerging technologies, it may not have been feasible to fully encompass their entire processing scope. Therefore, additional exploration is recommended to thoroughly examine the comprehensive applicability of the framework in the context of emerging technologies, such as IoT, Blockchain, and AI. Further validation of the framework in these domains and in different technological scenarios would undoubtedly provide valuable insights into its effectiveness and potential adjustments required to address the specific emergent challenges. Moving forward, it is crucial to engage non-academic experts from the technology industry in PbDD research to enhance its effectiveness and applicability. These industry professionals can provide valuable insights and practical understanding of implementing TOMs, as well as privacy-enhancing technologies, in real-world business contexts. Their involvement facilitates the intersection of law and technology, enabling a comprehensive approach to data protection. Specifically, PbDD research can benefit from their deep knowledge and expertise in implementing measures that align with industry practices. Their insights can help bridge the gap between theoretical concepts and practical

implementation, ensuring that PbDD frameworks are realistic and effective in addressing both data protection challenges and the objectives of legislators.

They can contribute insights into the feasibility, scalability, and effectiveness of TOMs and offer valuable guidance on addressing emerging challenges in the ever-evolving technological landscape. With rapid advancements in technologies such as IoT, Blockchain, and AI, it is crucial to stay updated and adapt PbDD frameworks to effectively address the privacy implications of these innovations.

Collaboration between academic researchers and non-academic experts fosters a multidisciplinary approach that combines theoretical knowledge with practical insights. In my view, this collaboration is a requirement when dealing with a law that predominantly pertains to technological aspects. Such collaborative efforts ensure that PbDD research remains relevant, impactful, and aligned with the evolving needs of organisations while upholding a high level of compliance with the fundamental rights of data subjects.

Bibliography

'11 Drafting Flaws for the European Commission to Address in Its Upcoming GDPR Review' <<https://iapp.org/news/a/11-drafting-flaws-for-the-ec-to-address-in-its-upcoming-gdpr-review/>>

A. B. Haque and others, 'GDPR Compliant Blockchains—A Systematic Literature Review' (2021) 9 IEEE Access 50593

A. Brooker B, Raman S and M. Sullivan J, 'The Need for Clarity After Schrems II' (*Lawfare*, 29 September 2020) <<https://www.lawfareblog.com/need-clarity-after-schrems-ii>>

Acquisti A, 'The Economics and Behavioral Economics of Privacy' in Helen Nissenbaum and others (eds), *Privacy, Big Data, and the Public Good: Frameworks for Engagement* (Cambridge University Press 2014) <<https://www.cambridge.org/core/books/privacy-big-data-and-the-public-good/economics-and-behavioral-economics-of-privacy/A8FFC368B41B90B49479970A05E71B77>>

Allen R and Masters D, 'Artificial Intelligence: The Right to Protection from Discrimination Caused by Algorithms, Machine Learning and Automated Decision-Making' (2019) 20 ERA-Forum 585

Altman M and others, 'Practical Approaches to Big Data Privacy over Time' (2018) 8 International Data Privacy Law 29

'An Update On Our Use of Face Recognition' (*Meta*, 2 November 2021) <<https://about.fb.com/news/2021/11/update-on-use-of-face-recognition/>>

Anonymous, 'GDPR Implementation Costs Enterprises More than Expected' (2018) 55 Security 14

Argyrou A, 'Making the Case for Case Studies in Empirical Legal Research' (2017) 13 Utrecht law review 95

Article 29 Data Protection Working Party, 'Opinion 05/2014 on Anonymisation Techniques' (WP29 2014) 0829/14/EN WP216 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf>

—, 'Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks' (2014) 14/EN WP 218 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf>

—, 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation' (2017) 2016/679

—, 'Guidelines on Transparency under Regulation 2016/679' 17/EN WP260

—, ‘Opinion 04/2007 on the Concept of Personal Data, (WP136, 20 June 2007).’

Article 29 Data Protection Working Party and Working Party on Police and Justice, ‘The Future of Privacy - Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data’ (Article 29 Data Protection Working Party, Working Party on Police and Justice 2009) 02356/09/EN, WP 168

Article 29 Working Party, ‘Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC’ (2014) <<https://ec.europa.eu/newsroom/article29/news-overview.cfm>>

—, ‘Opinion 8/2014 on the on Recent Developments on the Internet of Things’ 14/EN WP 223 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm>

‘Artificial Intelligence and the GDPR: Incompatible Realities?’ (*White Label Consultancy*, 31 March 2021) <<https://whitelabelconsultancy.com/2021/03/artificial-intelligence-and-the-gdpr/>>

Batt J, ‘Reputational Risk and the GDPR: What’s at Stake and How To Handle It’ (*Economy*, 23 May 2018) <<https://www.brinknews.com/reputational-risk-and-the-gdpr-whats-at-stake-and-how-to-handle-it/>>

Baybutt P, ‘Cyber Security Vulnerability Analysis: An Asset-Based Approach’ (2003) 22 *Process Safety Progress* 220

Becker M, ‘Privacy in the Digital Age: Comparing and Contrasting Individual versus Social Approaches towards Privacy’ (2019) 21 *Ethics and Information Technology* 307

Becker R and others, ‘DAISY: A Data Information System for Accountability under the General Data Protection Regulation’ (2019) 8 *Gigascience* <<https://go.exlibris.link/1NfSHBDc>>

Beckett P, ‘GDPR Compliance: Your Tech Department’s next Big Opportunity’ (2017) 2017 *Computer Fraud & Security* 9

Bednar K, Spiekermann S and Langheinrich M, ‘Engineering Privacy by Design: Are Engineers Ready to Live up to the Challenge?’ (2019) 35 *The Information society* 122

Bendiek A and Römer M, ‘Externalizing Europe: The Global Effects of European Data Protection’ (2019) 21 *Digital Policy, Regulation and Governance* 32

Benyahya M and others, ‘The Interface of Privacy and Data Security in Automated City Shuttles: The GDPR Analysis’ (2022) 12 *Applied Sciences*

Berberich M and Steiner M, ‘Blockchain Technology and the GDPR - How to Reconcile Privacy and Distributed Ledgers Reports: Practitioner’s Corner’ (2016) 2 *European Data Protection Law Review (EDPL)* 422

Bert-Jaap Koops, 'The Trouble with European Data Protection Law' (2014) 4 *International Data Privacy Law* 250

Bier C and others, 'How Is Positive-Sum Privacy Feasible?' in Nils Aschenbruck and others (eds), *Future Security* (Springer Berlin Heidelberg 2012)

Black J, 'Principles Based Regulation: Risks, Challenges and Opportunities' (Sydney, Australia, 28 March 2007) <<http://eprints.lse.ac.uk/62814/>>

—, 'Forms and Paradoxes of Principles-Based Regulation' (2008) 3 *Capital markets law journal* 425

Blancco Technology Group, 'Locating Customer Data Will Be Half the Battle to Fulfill EU GDPR's "Right to Be Forgotten"' (2017) 47 *Database and Network Journal* 5+

Boban M, 'GDPR AND DATA PROTECTION IMPACT ASSESSMENT (DPIA)', *Economic and Social Development: Book of Proceedings* (Varazdin Development and Entrepreneurship Agency (VADEA) 2020) <<https://go.exlibris.link/9ZqTv5Yh>>

Bollen GMH and Schoordjik MCE, 'HLA Tissue Typing of Family Donors: Respect for Privacy and Wellness' (2009) 43 *Bone marrow transplantation* (Basingstoke) S310

Braun E and Wield D, 'Regulation as a Means for the Social Control of Technology' (1994) 6 *Technology Analysis & Strategic Management* 259

Braun V and Clarke V, 'Using Thematic Analysis in Psychology' (2006) 3 *Qualitative Research in Psychology* 77

Brimsted K, 'GDPR Series: Accountability - a Blueprint for GDPR Compliance' (*Thomson Reuters Practical Law, Privacy and Data Protection*) <<https://uk.westlaw.com/Document/I58CF05C0F57511E6A70DB1D5CDC31199/View/FullText.html>>

BRKAN M and BONNET G, 'Legal and Technical Feasibility of the GDPR's Quest for Explanation of Algorithmic Decisions: Of Black Boxes, White Boxes and Fata Morganas' (2020) 11 *European Journal of Risk Regulation : EJRR* 18

Brown L, 'Beware the Spy in Your Baby Monitor and Smart Camera' (*Mail Online*, 3 March 2020) <<https://www.dailymail.co.uk/news/article-8067561/Beware-spy-baby-monitor-smart-camera-security-chiefs-warn-cyber-crooks-hack-them.html>>

Bu F and others, "'Privacy by Design" Implementation: Information System Engineers' Perspective' (2020) 53 *International Journal of Information Management* 102124

Buckley G, Caulfield T and Becker I, "'It May Be a Pain in the Backside but." Insights into the Impact of GDPR on Business after Three Years' <<https://go.exlibris.link/ry3tTcKk>>

Buckley JA, Thompson PB and Whyte KP, 'Collingridge's Dilemma and the Early Ethical Assessment of Emerging Technology: The Case of Nanotechnology Enabled Biosensors' (2017) 48 *Technology in Society* 54

Bu-Pasha S, 'Cross-Border Issues under EU Data Protection Law with Regards to Personal Data Protection' (2017) 26 *Information & communications technology law* 213

Bygrave LA, 'Data Protection by Design and by Default : Deciphering the EU's Legislative Requirements' (2017) 1 *Oslo Law Review* 105

Calvi A and Kotzinos D, 'Enhancing AI Fairness through Impact Assessment in the European Union: A Legal and Computer Science Perspective', *ACM International Conference Proceeding Series* (2023) <<https://go.exlibris.link/NYcLPcYz>>

Campbell J, Goldfarb A and Tucker C, 'Privacy Regulation and Market Structure' (2015) 24 *Journal of Economics & Management Strategy* 47

CARMEL E, ESPINOSA JA and DUBINSKY Y, "'Follow the Sun" Workflow in Global Software Development' (2010) 27 *Journal of Management Information Systems* 17

Cavoukian A, 'Privacy by Design: The 7 Foundational Principles' (Information and Privacy Commissioner of Ontario 2010) 1

—, 'Privacy by Design: The Definitive Workshop. A Foreword by Ann Cavoukian, Ph.D' (2010) 3 *Identity in the Information Society* 247

—, 'Privacy by Design [Leading Edge]' (2012) 31 *IEEE technology & society magazine* 18

—, 'Global Privacy and Security, by Design: Turning the "Privacy vs. Security" Paradigm on Its Head' (2017) 7 *Health and technology* 329

—, 'Understanding How to Implement Privacy by Design, One Step at a Time' (2020) 9 *IEEE consumer electronics magazine* 78

Cavoukian A, Taylor S and Abrams ME, 'Privacy by Design: Essential for Organizational Accountability and Strong Business Practices' (2010) 3 *Identity in the Information Society* 405

Cerna L, 'The Nature of Policy Change and Implementation: A Review of Different Theoretical Approaches' (OECD 2013) <<https://www.oecd.org/education/cei/The%20Nature%20of%20Policy%20Change%20and%20Implementation.pdf>>

Channel 4 News Investigations Team, 'Exposed: Undercover Secrets of Trump's Data Firm' (20 May 2018) <<https://www.channel4.com/news/exposed-undercover-secrets-of-donald-trump-data-firm-cambridge-analytica>>

Chaudhuri A and Cavoukian A, 'The Proactive and Preventive Privacy (3P) Framework for IoT Privacy by Design' (2018) 57 *EDPACS* 1

Chavez N, 'Arkansas Judge Drops Murder Charge in Amazon Echo Case' (*Crime + Justice*, 2 December 2017) <<https://edition.cnn.com/2017/11/30/us/amazon-echo-arkansas-murder-case-dismissed/index.html>>

Chivot E and Castro D, 'The EU Needs to Reform the GDPR To Remain Competitive in the Algorithmic Economy' (*Artificial Intelligence*, 13 May 2019) <<https://datainnovation.org/2019/05/the-eu-needs-to-reform-the-gdpr-to-remain-competitive-in-the-algorithmic-economy/>>

Churilov AY and National Research Tomsk State University, 'Principles of the EU General Regulations for the Protection of Personal Data (GDPR): Problems and Perspectives for Implementation' (2019) 16 *Vestnik of the Omsk Law Academy* 29

Commission Nationale de l'Informatique et des Libertés (CNIL), 'Blockchain and the GDPR: Solutions for a Responsible Use of the Blockchain in the Context of Personal Data' (*Blockchain*, 6 November 2018) <<https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data>> accessed 21 July 2021

Consultancy.uk, 'GDPR Compliance to Cost FTSE100 Firms £15 Million, Banks Face Largest Bill' (*News*, 21 December 2017) <<https://www.consultancy.uk/news/15101/gdpr-compliance-to-cost-ftse100-firms-15-million-banks-face-largest-bill>>

Dancyger L, 'Fitbits Are Snitching on Criminals -- Here's How' (*Rolling Stone*, 4 October 2018) <<https://www.rollingstone.com/culture/culture-news/fitbit-apple-watch-crime-help-solve-733050/>>

Daško N, 'General Data Protection Regulation (GDPR) – Revolution Coming to European Data Protection Laws in 2018. What's New for Ordinary Citizens?' (2018) 23 *Comparative Law Review* 123

'Data Protection by Design and by Default | Data Protection Commission' (*Data protection by Design and by Default | Data Protection Commission*) <<https://www.dataprotection.ie/organisations/know-your-obligations/data-protection-design-and-default>>

'Data-Hungry Algorithms and the Thirst for AI' *ICT Monitor Worldwide* (30 March 2017) <<https://link.gale.com/apps/doc/A488389720/ITOF?u=rdg&sid=summon&id=b19557a3>>

Davies G, 'The Relationship between Empirical Legal Studies and Doctrinal Legal Research' (2020) 2020 *Erasmus law review* 1

de Hert P and Lazcoz G, 'When GDPR-Principles Blind Each Other: Accountability, Not Transparency, at the Heart of Algorithmic Governance' (2022) 8 *European data protection law review* (Internet) 31

de Hert PJA and Gutwirth S, 'Privacy, Data Protection and Law Enforcement' in E Claes, A Duff and S Gutwirth (eds), *Opacity of the individual and transparency of power* (Intersentia 2006)

'Délibération SAN-2019-005 Du 28 Mai 2019' (Commission Nationale de l'Informatique et des Libertés 2018) 2019-005 <<https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000038552658/>>

DivvyCloud, '2020 Cloud Misconfigurations Report' (2020)
<<https://divvycloud.com/misconfigurations-report-2020/>>

Drev M and Delak B, 'Conceptual Model of Privacy by Design' (2022) 62 *The Journal of computer information systems* 888

EDPB, 'Guidelines 5/2019 on the Criteria of the Right to Be Forgotten in the Search Engines Cases under the GDPR (Part 1)' (7 July 2020) <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-52019-criteria-right-be-forgotten-search-engines_en>

'EDPS Opinion 5/2018 - Preliminary Opinion On Privacy By Design' (2018)
<<https://link.gale.com/apps/doc/A549172127/ITOF?u=rdg&sid=ITOF&xid=e41d0c3c>>

Elena C, 'Evolution of the Quality of Regulation Concept in the Context of Ensuring Legal Certainty' (2019) 7 *Academic Journal of Law and Governance (AJLG)* 107

El-Gazzar R and Stendal K, 'Examining How GDPR Challenges Emerging Technologies' (2020) 10 *Journal of information policy (University Park, Pa.)* 237

Emanuel Lobato Cervantes V, 'The Schrems II Judgment of the Court of Justice Invalidates the EU – U.S. Privacy Shield and Requires “Case by Case” Assessment on the Application of Standard Contractual Clauses (SCCs)' (2020) 6 *European Data Protection Law Review*
<<https://doi.org/10.21552/edpl/2020/4/18>>

EPIC, 'The Value of Cross-Border Data Flows to Europe: Risks and Opportunities' (*DIGITALEUROPE*) <<https://www.digitaleurope.org/resources/the-value-of-cross-border-data-flows-to-europe-risks-and-opportunities/>>

Espinoza J, 'EU Must Overhaul Flagship Data Protection Laws, Says a “Father” of Policy' (*Data Protection*, 3 March 2021) <<https://www.ft.com/content/b0b44dbe-1e40-4624-bdb1-e87bc8016106>>

'EU AI Act: First Regulation on Artificial Intelligence | News | European Parliament' (8 June 2023)
<<https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence>>

'EU TOP COURT STRIKES DOWN PRIVACY SHIELD, CCIA CALLS FOR URGENT LEGAL CERTAINTY AND SOLUTIONS' *States News Service* (16 July 2020) NA

Eugene R, 'A Delphi Study: A Model to Help IT Management within Financial Firms Reduce Regulatory Compliance Costs for Data Privacy and Cybersecurity' (DIT, Capella University 2020)

European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 25.01.2012, COM(2012) 11 Final'

—, 'Questions and Answers - Data Protection Reform Package' (*Press corner*, 24 May 2017) <https://ec.europa.eu/commission/presscorner/detail/en/MEMO_17_1441>

—, 'Two Years of the GDPR: Questions and Answers' (2020) QANDA/20/1166 <https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_1166>

European Data Protection Board (EDPB), 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0' (EDPB 2020) <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en>

European Data Protection Supervisor, 'Accountability' (*Our work by topics*) <<https://edps.europa.eu/data-protection/our-work/subjects/accountability>>

European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data Protection Law (2018 Edn, Publications Office of the European Union)*

'Experian Data Breach Resolution and Ponemon Institute Find Organizations Are Not Ready for Global Security Risks and Regulations: Only 9 Percent of Companies Are Prepared for the Global Data Protection Regulation (GDPR) Half Don't Know Where to Begin' *PR Newswire* (New York, 27 June 2017) <<https://www.proquest.com/wire-feeds/experian-data-breach-resolution-ponemon-institute/docview/1913638074/se-2?accountid=13460>>

'Facebook Policy Change Rekindles Privacy Fears and It Turns to Voice' [2013] *Biometric technology today* 2

Faifr A and Januška M, 'Factors Determining the Extent of GDPR Implementation within Organizations: Empirical Evidence from Czech Republic' (2021) 22 *Journal of Business Economics and Management* 1124

Fenwick M and Wrška S, 'The Shifting Meaning of Legal Certainty' in Mark Fenwick and Stefan Wrška (eds), *Legal Certainty in a Contemporary Context: Private and Criminal Law Perspectives* (Springer Singapore 2016) <https://doi.org/10.1007/978-981-10-0114-7_1>

Fielder A and others, 'Risk Assessment Uncertainties in Cybersecurity Investments' (2018) 9 *Games*

Finck M, 'Blockchain and the General Data Protection Regulation - Can Distributed Ledgers Be Squared with European Data Protection Law?' (2019) <<https://eptanetwork.org/database/policy-briefs-reports/1796-blockchain-and-the-general-data-protection-regulation-can-distributed-ledgers-be-squared-with-european-data-protection-law-stoa>>

Franklin J, 'In-House Counsel: 100% Compliance with GDPR Almost Impossible' [2020] *International Financial Law Review* <<https://www.proquest.com/trade-journals/house-counsel-100-compliance-with-gdpr-almost/docview/2373953912/se-2?accountid=13460>>

Frischhut M, 'Status Quo of Ethics and Morality in EU Law' in Markus Frischhut (ed), *The Ethical Spirit of EU Law* (Springer International Publishing 2019) <https://doi.org/10.1007/978-3-030-10582-2_3>

Galai D and Sade O, 'The "Ostrich Effect" and the Relationship between the Liquidity and the Yields of Financial Assets' (2006) 79 *The Journal of Business* 2741

Ganglmair B, Krämer J and Gambato J, 'Regulatory Compliance with Limited Enforceability: Evidence from Privacy Policies' <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4600876>

Gately E, '80 Percent of Companies Still Not GDPR-Compliant' (13 June 2018) <<https://www.channelpartneronline.com/2018/07/13/80-percent-of-companies-still-not-gdpr-compliant/>>

'GDPR & AI: Privacy by Design in Artificial Intelligence' (*Silo AI*, 28 February 2018) <<https://silo.ai/gdpr-ai-privacy-by-design-in-artificial-intelligence/>>

'GDPR One Year Anniversary: A Risk-Based Approach to GDPR Is Key for Achieving Compliance' *ENP Newswire* (15 July 2019) <<https://link.gale.com/apps/doc/A593354902/ITOF?u=rdg&sid=summon&xid=877ee309>>

Gellert R, *The Risk-Based Approach to Data Protection* (Oxford University Press 2020) <<https://doi.org/10.1093/oso/9780198837718.001.0001>>

Genus A and Stirling A, 'Collingridge and the Dilemma of Control: Towards Responsible and Accountable Innovation' (2018) 47 *Research Policy* 61

GPEN, '2016 GPEN Sweep Internet of Things [with a Focus on Accountability]' (2016) <<https://ico.org.uk/media/about-the-ico/disclosure-log/1625142/irq0648379-attachment.pdf>>

Greze B, 'The Extra-Territorial Enforcement of the GDPR: A Genuine Issue and the Quest for Alternatives' (2019) 9 *International Data Privacy Law* 109

Guardum, 'UK Businesses Expend £1.59 Million and 14 Person Years Annually Processing DSARs Finds New Survey amongst DPOs' (May 2020) <<https://www.globalsecuritymag.com/UK-businesses-expend-L1-59-Million,20200518,98707.html>>

Hall HK, 'Arkansas v. Bates: Reconsidering the Limits of a Reasonable Expectation of Privacy' (2017) 6 *University of Baltimore Journal of Media Law & Ethics* 22

Hauser C, 'In Connecticut Murder Case, a Fitbit Is a Silent Witness' (*New York*, 27 April 2017) <<https://www.nytimes.com/2017/04/27/nyregion/in-connecticut-murder-case-a-fitbit-is-a-silent-witness.html>>

Hérault S and Belvaux B, 'Privacy paradox et adoption de technologies intrusives Le cas de la géolocalisation mobile/Privacy paradox and the adoption of intrusive technologies. The case of mobile location-based services' [2014] *Décisions Marketing* 67

Herian R, 'Blockchain, GDPR, and Fantasies of Data Sovereignty' (2020) 12 *Law, Innovation and Technology* 156

Hern A, 'Cambridge Analytica Did Work for Leave. EU, Emails Confirm' *The Guardian* (30 July 2019)

Hildebrandt M, 'Defining Profiling: A New Type of Knowledge?' in Mireille Hildebrandt and Serge Gutwirth (eds), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer Netherlands 2008) <https://doi.org/10.1007/978-1-4020-6914-7_2>

Hildebrandt M and Tielemans L, 'Data Protection by Design and Technology Neutral Law' (2013) 29 *Computer Law & Security Review* 509

Hjerpe K, Ruohonen J and Leppanen V, 'The General Data Protection Regulation: Requirements, Architectures, and Constraints', *2019 IEEE 27th International Requirements Engineering Conference (RE)* (IEEE 2019)

Hoepman J-H, 'Privacy Design Strategies (The Little Blue Book)' (University of Groningen 2020) <<https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf>>

Höne K and Eloff JHP, 'Information Security Policy — What Do International Information Security Standards Say?' (2002) 21 *Computers & security* 402

Hoofnagle CJ, Sloat B and Zuiderveen Borgesius FJ, 'The European Union General Data Protection Regulation: What It Is and What It Means' (2019) 28 *Information & communications technology law* 65

Horák M, Stupka V and Husák M, 'GDPR Compliance in Cybersecurity Software: A Case Study of DPIA in Information Sharing Platform', *Proceedings of the 14th International Conference on availability, reliability and security* (ACM 2019)

'ICANN: Clarity Required on GDPR Compliance' [2018] *Enterprise Innovation* <<https://www.proquest.com/trade-journals/icann-clarity-required-on-gdpr-compliance/docview/2021099454/se-2?accountid=13460>>

ICO, 'Principle (d): Accuracy' (17 October 2022) <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/accuracy/>>

—, 'Accountability and Governance' (*Guide to the General Data Protection Regulation (GDPR)*) <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/#top>>

—, 'Big Data, Artificial Intelligence, Machine Learning, and Data Protection' <<https://ico.org.uk/media/for-organisation/documents/2013559/big-data-ai-ml-and-data-protection.pdf>>

—, ‘Data Protection by Design and Default’ (*Accountability and Governance*, n.d.) <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/>>

—, ‘Principle (c): Data Minimisation’ (*Guide to the General Data Protection Regulation (GDPR)*) <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation/>>

—, ‘Principle (e): Storage Limitation’ (*Guide to the General Data Protection Regulation (GDPR)*) <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/>>

Information Commissioner’s Office, ‘The Principles’ (*Guide to the General Data Protection Regulation (GDPR)*) <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/>>

Ingram D, ‘Factbox: Who Is Cambridge Analytica and What Did It Do?’ (*Technology News*, 20 March 2018) <<https://www.reuters.com/article/facebook-cambridge-analytica-idINKBN1GW0A4>>

Internet Society, ‘A Short Guide to IP Addressing - How Are IP Addresses Managed and Distributed?’ (11 September 2015) <<https://www.internetsociety.org/resources/deploy360/2015/short-guide-ip-addressing/>>

Irwin L, ‘How Much Does GDPR Compliance Cost in 2021?’ (*IT Governance* 2021) <<https://www.itgovernance.eu/blog/en/how-much-does-gdpr-compliance-cost-in-2020>>

—, ‘How Much Does GDPR Compliance Cost in 2022?’ (*IT Governance Blog En*, 26 April 2022) <<https://www.itgovernance.eu/blog/en/how-much-does-gdpr-compliance-cost-in-2020>>

Jackson O, ‘GDPR: Companies at Risk over Unstructured Data’ [2018] *International financial law review*

Jakobi T and others, ‘The Role of IS in the Conflicting Interests Regarding GDPR’ (2020) 62 *Business & Information Systems Engineering* 261

Jelinek A, ‘EDPB Response to the MEP Sophie in’t Veld’s Letter on Unfair Algorithms’ (October 2020) <https://edpb.europa.eu/sites/default/files/files/file1/edpb_letter_out2020_0004_intvel_dalgorithms_en.pdf>

—, ‘EDPB Letter to the European Institutions on the Privacy and Data Protection Aspects of a Possible Digital Euro’ (18 June 2021) <https://edpb.europa.eu/system/files/2021-07/edpb_letter_out_2021_0113-digitaleuro-toconsiliumsi_en.pdf>

Kalloniatis C and others, 'Applying Soft Computing Technologies for Implementing Privacy-Aware Systems' in Marko Bajec and Johann Eder (eds), *Advanced Information Systems Engineering Workshops* (Springer Berlin Heidelberg 2012)

Kaminski ME and Malgieri G, 'Multi-Layered Explanations from Algorithmic Impact Assessments in the GDPR', *FAT 2020 - Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency* (2020) <<https://go.exlibris.link/t94NBbLD>>

Kaneen CK and Petrakis EGM, 'Towards Evaluating GDPR Compliance in IoT Applications' (2020) 176 *Knowledge-Based and Intelligent Information & Engineering Systems: Proceedings of the 24th International Conference KES2020* 2989

Kaplan A and Haenlein M, 'Siri, Siri, in My Hand: Who's the Fairest in the Land? On the Interpretations, Illustrations, and Implications of Artificial Intelligence' (2019) 62 *Business horizons* 15

Kindylidi I and Antas de Barros I, 'AI Training Datasets & Article 14 GDPR: A Risk Assessment for the Proportionality Exemption of the Obligation to Provide Information' (2021) 13 *Revista de direito, estado e telecomunicações* 1

Klitou D, 'Privacy by Design and Privacy-Invasive Technologies: Safeguarding Privacy, Liberty and Security in the 21st Century' (2011) 5 *Legisprudence* 297

Knight AM, 'Towards a New Approach to the Legal Definition of Personal Data and a Jurisdictional Model of Data Protection Law: Surpassing the Requirement for an Assessment of Identifiability from Data with an Effects-Based Approach' (PhD, University of Southampton (United Kingdom) 2017) <<https://search.proquest.com/dissertations-theses/towards-new-approach-legal-definition-personal/docview/2430827794/se-2?accountid=13460>>

Kostadinov D, 'Key Elements of an Information Security Policy' (*Management, compliance & auditing*, 20 July 2020) <<https://resources.infosecinstitute.com/topic/key-elements-information-security-policy/>>

Krause MS, 'Associational versus Correlational Research Study Design and Data Analysis' (2018) 52 *Quality and Quantity* 2691

Krówczyński W and Faculty of Management and Social Communication at Jagiellonian University in Krakow, 'The Influence Of The Regulation Of European Parliament And Council Of The European Union (GDPR) On The Level Of Transactional Costs Of Managing Medical Data In Medical Entities' (2018) 91 *Optimum studia ekonomiczne* 80

Kuneva M, 'European Consumer Commissioner, Keynote Speech; Roundtable on Online Data Collection, Targeting and Profiling' (Roundtable on Online Data Collection, Targeting and Profiling, Brussels, 31 March 2009) <https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_09_156>

Lachaud E, 'Should the DPO Be Certified?' (2014) 4 *International Data Privacy Law* 189

Langbroek PM and others, 'Methodology of Legal Research : Challenges and Opportunities' (2017) 13 Utrecht law review 1

Layton R, 'The 10 Problems of the GDPR, The US Can Learn from the EU's Mistakes and Leapfrog Its Policy' (2019) <<https://www.judiciary.senate.gov/imo/media/doc/Layton%20Testimony1.pdf>>

Leenes R and others, *Data Protection and Privacy: The Age of Intelligent Machines*, vol 10 (Hart Publishing Ltd 2017) <<https://go.exlibris.link/23sBBF6K>>

Lenhart A and others, "'You Shouldn't Need to Share Your Data": Perceived Privacy Risks and Mitigation Strategies Among Privacy-Conscious Smart Home Power Users' (2023) 7 Proc. ACM Hum.-Comput. Interact. <<https://doi.org/10.1145/3610038>>

Li ZS and others, 'GDPR Compliance in the Context of Continuous Integration'

Lifante-Vidal I, 'Is Legal Certainty a Formal Value?' (2020) 11 Jurisprudence 456

Liu L, Cao M and Sun Y, 'A Fusion Data Security Protection Scheme for Sensitive E-Documents in the Open Network Environment' (2021) 16 PloS one e0258464

Lomas N, 'GDPR's Two-Year Review Flags Lack of "vigorous" Enforcement' (*TechCrunch+*, 24 June 2020) <<https://techcrunch.com/2020/06/24/gdprs-two-year-review-flags-lack-of-vigorous-enforcement/>>

Lopes IM, Guarda T and Oliveira P, 'Implementation of ISO 27001 Standards as GDPR Compliance Facilitator' (2019) 4 Journal of information systems engineering & management <<https://go.exlibris.link/g0s9scjZ>>

Lynn T and others, *Data Privacy and Trust in Cloud Computing: Building Trust in the Cloud Through Assurance and Accountability* (Springer International Publishing AG 2020) <<https://go.exlibris.link/HQxtCksX>>

Lynskey O, *The Foundations of EU Data Protection Law* (Oxford University Press 2015)

—, 'Grappling with "Data Power": Normative Nudges from Data Protection and Privacy' (2019) 20 Theoretical inquiries in law 189

Lyons T, Courcelas L and Timsit K, 'Blockchain and the GDPR' (European Union Blockchain Observatory and Forum 2018) <https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf>

M. Colesky, J. Hoepman, and C. Hillen, 'A Critical Analysis of Privacy Design Strategies', 2016 *IEEE Security and Privacy Workshops (SPW)* (2016)

M Gawas V, 'Doctrinal Legal Research Method a Guiding Principle in Reforming the Law and Legal System towards the Research Development' (2017) Volume 3 International Journal of Law 128

M. Payton T and Claypoole T, *Privacy in the Age of Big Data* (Rowman & Littlefield 2014)

MACENAITE M, 'The "Riskification" of European Data Protection Law through a Two-Fold Shift' (2017) 8 *European journal of risk regulation* 506

Machuletz D and Böhme R, 'Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR' (2019) 2020 *Proceedings on Privacy Enhancing Technologies* 481

Malgieri G, 'The Concept of Fairness in the GDPR: A Linguistic and Contextual Interpretation', *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency* (Association for Computing Machinery 2020) <<https://doi.org/10.1145/3351095.3372868>>

—, 'The Limitations and the Alternatives of a Vulnerability-Based Interpretation of the GDPR' in Gianclaudio Malgieri (ed), *Vulnerability and Data Protection Law* (Oxford University Press 2023) <<https://doi.org/10.1093/oso/9780192870339.003.0008>>

Managing Privacy through Accountability (Daniel Guagnin, Leon Hempel, Carla Ilten, Inga Kroener, Daniel Neyland, Hector Postigo, Palgrave Macmillan London) <<https://doi.org/10.1057/9781137032225>>

Mansfield-Devine S, 'Meeting the Needs of GDPR with Encryption' (2017) 2017 *Computer Fraud & Security* 16

Marr B, 'What Is Unstructured Data And Why Is It So Important To Businesses? An Easy Explanation For Anyone' (*Forbes*) <<https://www.forbes.com/sites/bernardmarr/2019/10/16/what-is-unstructured-data-and-why-is-it-so-important-to-businesses-an-easy-explanation-for-anyone/>>

Martín Rodríguez P, "'A Missing Piece of European Emergency Law: Legal Certainty and Individuals" Expectations in the EU Response to the Crisis"' (2016) 12 *European Constitutional Law Review* 265

May 2020 PR, 'What Is the True Cost of Handling DSARs?' (*GRC World Forums*) <<https://www.grcworldforums.com/data-protection-and-privacy/what-is-the-true-cost-of-handling-dsars/58.article>>

McCarthy-Jones S, 'The Autonomous Mind: The Right to Freedom of Thought in the Twenty-First Century' (2019) 2 *Frontiers in Artificial Intelligence* 19

McKean R, Kurowska-Tober E and Waem H, 'DLA Piper GDPR Fines and Data Breach Survey: January 2022' (2022) <<https://www.dlapiper.com/en/uk/insights/publications/2022/1/dla-piper-gdpr-fines-and-data-breach-survey-2022/>>

McLaughlin EC, 'Suspect OKs Amazon to Hand over Echo Recordings in Murder Case | CNN Business' (*CNN*, 7 March 2017) <<https://www.cnn.com/2017/03/07/tech/amazon-echo-alexa-bentonville-arkansas-murder-case/index.html>>

McLeod S, 'What's the Difference between Qualitative and Quantitative Research?' (*Simply Psychology*, 2019) <<https://www.simplypsychology.org/qualitative-quantitative.html>>

Microsoft, 'Data Retention and Access through Privacy Settings' (2022) <<https://docs.microsoft.com/en-us/dynamics365/sales/data-retention-deletion-policy>>

—, 'Privacy and Personal Data for Microsoft Dynamics 365' (2022) <<https://docs.microsoft.com/en-us/dynamics365/get-started/gdpr/>>

'MinerEye to Demonstrate Interpretive AI Technology for Data Classification on GPUs at Nvidia's GTC Israel 2018: MinerEye Automatic Data Classification Is Critical to Unstructured Data Intensive Environments Accelerated by GPU, Including Hybrid Cloud and Data Center Storage' *PR Newswire* (New York, 15 October 2018) <<https://www.proquest.com/wire-feeds/minereye-demonstrate-interpretive-ai-technology/docview/2119923322/se-2?accountid=13460>>

Moerel L, 'GDPR Conundrums: The GDPR Applicability Regime — Part 1: Controllers' (*IAPP Privacy tracker*, 29 January 2018) <<https://iapp.org/news/a/gdpr-conundrums-the-gdpr-applicability-regime-part-1-controllers/>>

Mone V and Sivakumar C, 'An Analysis of the GDPR Compliance Issues Posed by New Emerging Technologies' (2022) 22 *Legal Information Management* 166

Monti A and Wacks R, *Protecting Personal Information: The Right to Privacy Reconsidered* (Bloomsbury Publishing Plc 2019)

'Netsparker GDPR Survey: 10 Percent of C-Level Security Execs Say GDPR Will Cost Them \$1M+' *Journal of Engineering* (23 April 2018) 839

O'Brien R, 'Privacy and Security: The New European Data Protection Regulation and It's Data Breach Notification Requirements' (2016) 33 *Business Information Review* 81

O'Callaghan P and Shiner B, 'The Right to Freedom of Thought in the European Convention on Human Rights' (2021) 8 *European Journal of Comparative Law and Governance* 112

OECD, 'OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data' <<https://www.oecd-ilibrary.org/content/publication/9789264196391-en>>

—, 'Data in the Digital Age' (OECD 2019) OECD Going Policy Note <<https://www.oecd.org/going-digital/data-in-the-digital-age.pdf>>

Office for National Statistics, 'Overview of Fraud and Computer Misuse Statistics for England and Wales' (2018) *Crime and Justice* <<https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/Articles/overviewoffraudandcomputermisusestatisticsforenglandandwales/2018-01-25>>

Opher A, Chou A and Onda A, 'The Rise of the Data Economy: Driving Value through Internet of Things Data Monetization' <https://hosteddocs.ittoolbox.com/rise_data_econ.pdf>

Organisation for Economic and Co-operation and Development, 'OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data - OECD' (1980) OECD Council Recommendation

<<https://www.oecd.org/sti/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm>>

P. Cheng and others, 'Smart Speaker Privacy Control - Acoustic Tagging for Personal Voice Assistants', *2019 IEEE Security and Privacy Workshops (SPW)* (2019)

Patel M, "'Privacy by Design" or Blockchain Transparency: Who Wins?' (*The Fintech Times*, 28 August 2018) <<https://thefintechtimes.com/privacy-by-design-or-blockchain-transparency-who-wins/>>

Paunio E, 'Beyond Predictability - Reflections on Legal Certainty and the Discourse Theory of Law in the EU Legal Order' (2009) 10 *German Law Journal* 1469

Pečarič M and others, 'Digitalisation and Law: The More Things Change – The More They Stay the Same' (2022) 20 *Lex Localis* 411

Peng L and others, 'Privacy Preservation in Permissionless Blockchain: A Survey' (2021) 7 *Digital Communications and Networks* 295

Perry R, 'GDPR – Project or Permanent Reality?' (2019) 2019 *Computer Fraud & Security* 9

Pinsent Masons, 'GDPR Lacks Clarity and Threatens Transatlantic Trade, Says Ross' (*Out-Law News*, May 31 2018) <<https://www.pinsentmasons.com/out-law/news/gdpr-lacks-clarity-threatens-transatlantic-trade>>

Ponemon Institute, 'How Much Does a Data Breach Cost?' (2021) <<https://www.ibm.com/security/data-breach>>

Poniszewska-Maranda A, 'Security Constraints in Modeling of Access Control Rules for Dynamic Information Systems' in Viliam Geffert and others (eds), *SOFSEM 2014: Theory and Practice of Computer Science* (Springer International Publishing 2014)

Portuese A, Gough O and Tanega J, 'The Principle of Legal Certainty as a Principle of Economic Efficiency' (2017) 44 *European Journal of Law and Economics* 131

'Pulse Survey: US Companies Ramping up General Data Protection Regulation (GDPR) Budgets' 3

Purtova N, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10 *Law, Innovation and Technology* 40

R. Singh, 'Cloud Computing and Covid-19', *2021 3rd International Conference on Signal Processing and Communication (ICPSC)* (2021)

'Recommendations for a Methodology of the Assessment of Severity of Personal Data Breaches' (ENISA) <<https://www.enisa.europa.eu/publications/dbn-severity>>

Redmon G, 'Incident Response Under GDPR: What to Do Before, During and After a Data Breach' (*Incident Response*, 27 July 2018) <<https://securityintelligence.com/incident-response-under-gdpr-what-to-do-before-during-and-after-a-data-breach/>>

Rees K, 'No, You Cannot Remove Data From the Blockchain. Here's Why.' (*MUO*, 4 August 2022) <<https://www.makeuseof.com/no-you-cannot-remove-data-from-the-blockchain-heres-why/>>

Regan PM and Johnson DG, 'Privacy and Trust in Socio-Technical Systems of Accountability' in Daniel Guagnin and others (eds), *Managing Privacy through Accountability* (Palgrave Macmillan UK 2012) <https://doi.org/10.1057/9781137032225_7>

Renieris E, 'Forget Erasure: Why Blockchain Is Really Incompatible with the GDPR' (*Governance of technology & the internet, The Berkman Klein Center for Internet & Society at Harvard University*, 23 September 2019) <<https://cyber.harvard.edu/story/2019-09/forget-erasure-why-blockchain-really-incompatible-gdpr>>

Ritzer C and Filkina N, 'First Multi-Million GDPR Fine in Germany: €14.5 Million for Not Having a Proper Data Retention Schedule in Place' (Norton Rose Fulbright LLP, Data Protection Report 2019) <<https://www.dataprotectionreport.com/2019/11/first-multi-million-gdpr-fine-in-germany-e14-5-million-for-not-having-a-proper-data-retention-schedule-in-place/>>

Room S, *Butterworths Data Security - Law and Practice* (LexisNexis 2009)

Rossi B, 'Why Businesses Should Be More Concerned with GDPR and AI than Brexit' (*Information Age*, 21 March 2017) <<https://www.information-age.com/businesses-concerned-gdpr-ai-brexite-4910/>>

Rowley J and Slack F, 'Conducting a Literature Review' (2004) 27 *Management research news* 31

Rubinstein IS and Good N, 'The Trouble with Article 25 (and How to Fix It): The Future of Data Protection by Design and Default' (2020) 10 *International Data Privacy Law* 37

Ruohonen J and Hjerpe K, 'The GDPR Enforcement Fines at Glance' (2022) 106 *Information Systems* 101876

S. Cimato and others, 'Privacy-Aware Biometrics: Design and Implementation of a Multimodal Verification System', *2008 Annual Computer Security Applications Conference (ACSAC)* (2008)

'Safyr Accelerates Personal Data Discovery in ERP & CRM Systems for GDPR Compliance' *Journal of Engineering* (23 October 2017) 148

Saifuddin F, 'Is There Any Central Authority in Blockchain Technology?' (*Blockchain Magazine*, 19 May 2022) <<https://blockchainmagazine.net/is-there-any-central-authority-in-blockchain-technology/>>

Salter M and Mason J, *Writing Law Dissertations : An Introduction and Guide to the Conduct of Legal Research : An Introduction and Guide to the Conduct of Legal Research* (Pearson Education UK 2007)
<<http://ebookcentral.proquest.com/lib/reading/detail.action?docID=5136574>>

Schneider G, 'Disentangling Health Data Networks: A Critical Analysis of Articles 9(2) and 89 GDPR' (2019) 9 *International Data Privacy Law* 253

Schwartz RL, 'Internal and External Method in the Study of Law' (1992) 11 *Law and Philosophy* 179

Selzer A, 'The Appropriateness of Technical and Organisational Measures under Article 32 GDPR Reports: Practitioners' Corner' (2021) 7 *European Data Protection Law Review (EDPL)* 120

Selzer A, Woods D and Bohme R, 'An Economic Analysis of Appropriateness under Article 32 GDPR Reports: Practitioners' Corner' (2021) 7 *European Data Protection Law Review (EDPL)* 456

Seo J and others, 'An Analysis of Economic Impact on IoT Industry under GDPR' (2018) 2018 *Mobile Information Systems* 6792028

Sharma TK, 'Public Vs. Private Blockchain : A Comprehensive Comparison' (7 August 2019)
<<https://www.blockchain-council.org/blockchain/public-vs-private-blockchain-a-comprehensive-comparison/>>

Sirur S, Nurse J and Webb H, 'Are We There Yet?: Understanding the Challenges Faced in Complying with the General Data Protection Regulation (GDPR)', *Proceedings of the 2nd International Workshop on multimedia privacy and security* (ACM 2018)

Siyal AA and others, 'Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives' (2019) 3 *Cryptography*

'Smart Camera and Baby Monitor Warning given by UK's Cyber-Defender' *BBC News* (3 March 2020) <<https://www.bbc.com/news/technology-51706631>>

Solove DJ, 'A Taxonomy of Privacy' (2006) 154 *University of Pennsylvania law review* 477

Sousa WG de and others, 'How and Where Is Artificial Intelligence in the Public Sector Going? A Literature Review and Research Agenda' (2019) 36 *Government information quarterly* 101392

Spiekermann S, 'The Challenges of Privacy by Design' (2012) 55 *Communications of The ACM - CACM* 38

Sreenivasan S and Weinberger L, 'The Importance of Privacy—Both Psychological and Legal | Psychology Today' <<https://www.psychologytoday.com/us/blog/emotional-nourishment/202007/the-importance-privacy-both-psychological-and-legal>>

Stanislav M and Beardsley T, 'HACKING IoT: A Case Study on Baby Monitor Exposures and Vulnerabilities' (2015) <<https://www.rapid7.com/globalassets/external/docs/Hacking-IoT-A-Case-Study-on-Baby-Monitor-Exposures-and-Vulnerabilities.pdf>>

Štarchoň P and Pikulík T, 'GDPR Principles in Data Protection Encourage Pseudonymization through Most Popular and Full-Personalized Devices - Mobile Phones' (2019) 151 *The 10th International Conference on Ambient Systems, Networks and Technologies (ANT 2019) / The 2nd International Conference on Emerging Data and Industry 4.0 (EDI40 2019) / Affiliated Workshops* 303

Stoica LA and Ghizlane C, 'Mathematical Approach on the GDPR Complexity' (2020) 16 *Journal of modern accounting and auditing*

Sumroy R, Mykura D and Ranson I, 'Blockchain and Data Protection (UK)' (*Practical Law*) <<https://uk.practicallaw.thomsonreuters.com/w-020-5436>>

Superintendence of Industry and Commerce, 'Sandbox on Privacy by Design and by Default in Artificial Intelligence Projects' (2021) <<https://globalprivacyassembly.org/wp-content/uploads/2021/07/B6.-SIC-Colombia-Sandbox-on-privacy-by-design-and-by-default-in-AI-projects.pdf>>

Synodinou TE, 'Lawfulness for Users in European Copyright Law: Acquis and Perspectives' (2019) 10 *JIPITEC* 20

Tamburri DA, 'Design Principles for the General Data Protection Regulation (GDPR): A Formal Concept Analysis and Its Evaluation' (2020) 91 *Information systems (Oxford)* 101469

Tapscott D, 'False Dichotomy: Privacy Isn't Always at Odds with Security' (2003) 6 *Intelligent enterprise (San Mateo, Calif.)* 12

Tarran B, 'What Can We Learn from the Facebook—Cambridge Analytica Scandal?' (2018) 15 *Significance* 4

Taylor C, 'What's the Big Deal With Unstructured Data?' (*Partner content: Tibco*) <<https://www.wired.com/insights/2013/09/whats-the-big-deal-with-unstructured-data/>>

Tene O, 'Privacy in the Age of Big Data: A Time for Big Decisions' <https://www.researchgate.net/publication/259892061_Privacy_in_the_Age_of_Big_Data_A_Time_for_Big_Decisions/>

'The GDPR as a Risk for the Annual Financial Statements | Friedrich Graf von Westphalen' <<https://www.fgvw.de/en/news/archive-2018/the-gdpr-as-a-risk-for-the-annual-financial-statements>>

The International Association of Privacy Professionals and Ernst & Young, 'IAPP-EY Annual Privacy Governance Report 2018' (2018) <https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/financial-services/ey-iapp-ey-annual-privacy-gov-report-2018.pdf>

The National Archives, 'Advice on Retention' (*Information Management*) <<https://www.nationalarchives.gov.uk/information-management/manage-information/policy-process/disposal/advice-on-retention/>>

'The "Tidal Wave" of Data Protection-Related Class Actions: Why We're Not Drowning Just Yet...'
<<https://www.twobirds.com/en/insights/2018/global/tidal-wave-of-data-protection-related-cases>> accessed 20 December 2022

'Third Biennial Ernst & Young 2018 Global Forensic Data Analytics Survey' (*GDPR compliance — from planning to action*, 2018) <https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/assurance/assurance-pdfs/ey-forensics-gdpr-compliance-from-planning-to-action.pdf>

Tierney A, 'Hacking Swann & FLIR/Lorex Home Security Camera Video' (*Internet of Things*, 26 July 2018) <<https://www.pentestpartners.com/security-blog/hacking-swann-home-security-camera-video/>>

Tyler TR, 'Methodology in Legal Research' (2017) 13 *Utrecht law review* 130

Tzanou M, 'Data Protection as a Fundamental Right next to Privacy? "Reconstructing" a Not so New Right' (2013) 3 *International Data Privacy Law* 88

—, *Health Data Privacy under the GDPR: Big Data Challenges and Regulatory Responses* (Taylor and Francis 2020) <<https://go.exlibris.link/8JD6V6Kj>>

Tzanou M and Vogiatzoglou P, 'In Search of Legal Certainty Regarding "Effective Redress" in International Data Transfers: Unpacking the Conceptual Complexities and Clarifying the Substantive Requirements' [2023] *Review of European Administrative Law*, Forthcoming <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4325287>

'Understanding Structured Data: A Comprehensive Guide 101' (28 June 2021) <<https://hevodata.com/learn/understanding-structured-data/>>

Ustraran E, *European Data Protection, Law and Practice* (Second Edition, IAPP 2019)

Uzunov AV, Fernandez EB and Falkner K, 'Security Solution Frames and Security Patterns for Authorization in Distributed, Collaborative Systems' (2015) 55 *Computers & security* 193

van der Aalst WMP, 'Responsible Data Science in a Dynamic World: The Four Essential Elements of Data Science', *IFIP Advances in Information and Communication Technology* (2019) <<https://go.exlibris.link/t3HD9bDW>>

van Rest J and others, 'Designing Privacy-by-Design' in Bart Preneel and Demosthenes Ikonomidou (eds), *Privacy Technologies and Policy* (Springer Berlin Heidelberg 2014)

Veale M, Binns R and Ausloos J, 'When Data Protection by Design and Data Subject Rights Clash' (2018) 8 *International data privacy law* 105

Vedula M, 'GDPR Compliance: The IT Role' (2019) 61 *ITNOW* 44

Véliz C, *Privacy Is Power* (Bantam Press 2020)

Voss WG, 'Cross-Border Data Flows, The GDPR, And Data Governance' (2020) 29 *Pacific Rim law & policy journal* 485

Wachter S and Mittelstadt B, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI Survey: Privacy, Data, and Business' (2019) 2019 *Columbia Business Law Review* 494

Watts S, 'Intelligent Combination – the Benefits of Tokenless Two-Factor Authentication' (2014) 2014 *Network Security* 17

'What Are the Accountability and Governance Implications of AI?' (19 May 2023) <<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/what-are-the-accountability-and-governance-implications-of-ai/>>

'White Paper – IAPP-OneTrust Research: Bridging ISO 27001 to GDPR' <<https://iapp.org/resources/article/iapp-onetrust-research-bridging-iso-27001-to-gdpr/>>

Wiese Schartum D, 'Making Privacy by Design Operative' (2016) 24 *International Journal of Law and Information Technology* 151

Zemler F and Westner M, *Blockchain and GDPR: Application Scenarios and Compliance Requirements* (2019)

Zerlang J, 'GDPR: A Milestone in Convergence for Cyber-Security and Compliance' (2017) 2017 *Network Security* 8

Zunin I, 'Intrusive Technology Means Privacy Rights Are Necessary' *Honolulu Star - Advertiser* (Honolulu, Hawaii, 25 February 2012) <<https://www.proquest.com/newspapers/intrusive-technology-means-privacy-rights-are/docview/923427687/se-2?accountid=13460>>

[This Page Intentionally Left Blank]

Annex 1 – Analysis of GDPR fines 2018 – 2023

i. Highest GDPR individual fines amount by Country

Country	Amount			
		CYPRUS	€	925,000.00
LUXEMBOURG	€ 746,000,000.00	HUNGARY	€	634,000.00
IRELAND	€ 405,000,000.00	FINLAND	€	608,000.00
FRANCE	€ 90,000,000.00	BELGIUM	€	600,000.00
GERMANY	€ 35,258,708.00	CROATIA	€	285,000.00
ITALY	€ 27,800,000.00	ISLE OF MAN	€	202,000.00
UNITED KINGDOM	€ 22,046,000.00	LATVIA	€	150,000.00
GREECE	€ 20,000,000.00	ROMANIA	€	150,000.00
SPAIN	€ 10,000,000.00	CZECH REPUBLIC	€	118,500.00
AUSTRIA	€ 9,500,000.00	LITHUANIA	€	110,000.00
NORWAY	€ 6,300,000.00	ESTONIA	€	100,000.00
SWEDEN	€ 5,000,000.00	MALTA	€	65,000.00
PORTUGAL	€ 4,300,000.00	ICELAND	€	51,000.00
THE NETHERLANDS	€ 3,700,000.00	SLOVAKIA	€	50,000.00
BULGARIA	€ 2,600,000.00	LIECHTENSTEIN	€	4,100.00
DENMARK	€ 1,300,000.00			
POLAND	€ 1,000,000.00			

ii. **Statistics: GDPR fines by Country (amount)**

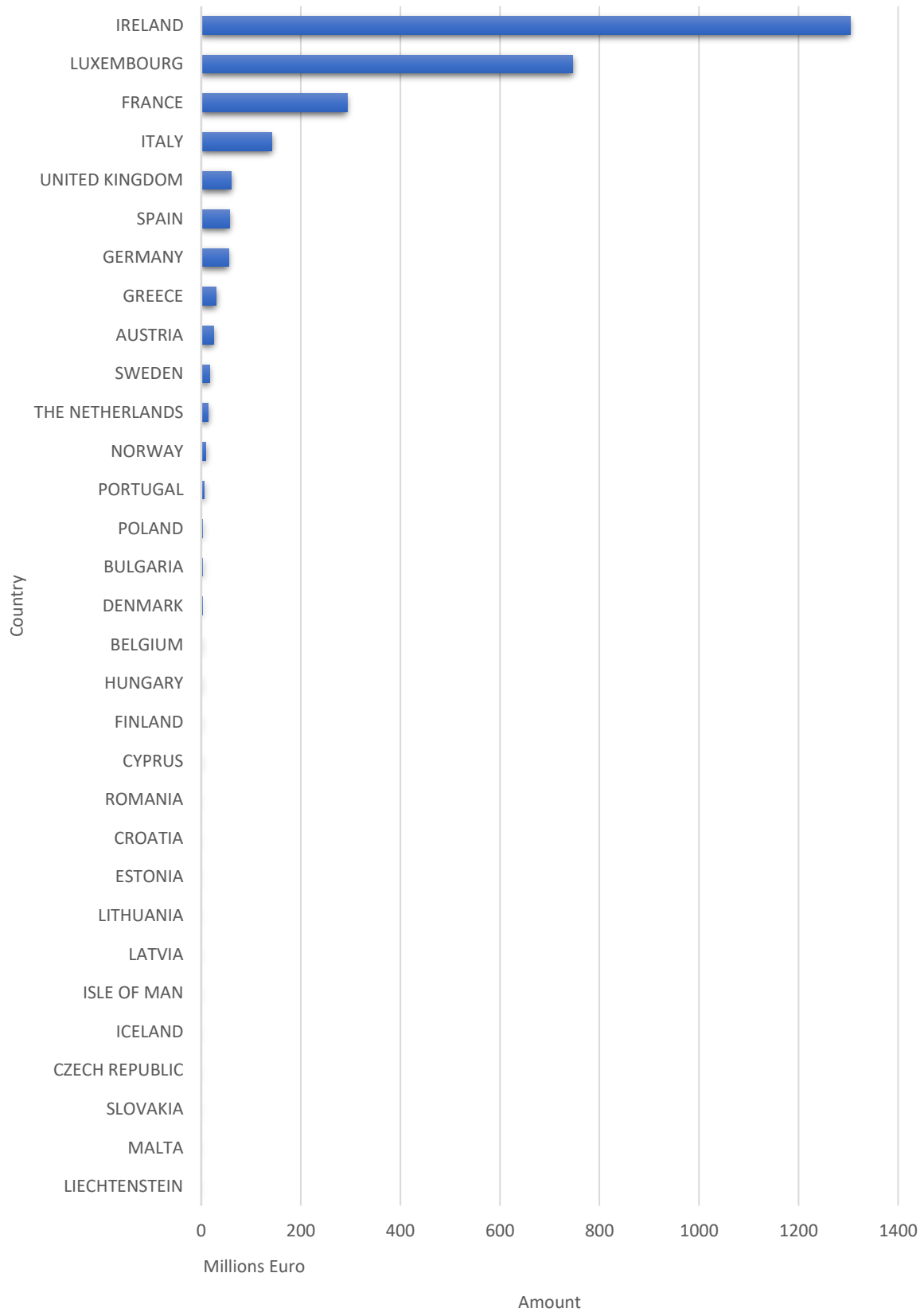
Country	Amount
Estonia	€ 300,604.00
Lithuania	€ 244,500.00
Latvia	€ 243,250.00
Isle Of Man	€ 218,750.00
Ireland	€ 1,303,515,900.00
Iceland	€ 218,500.00
Luxembourg	€ 746,273,600.00
Czech Republic	€ 165,903.00
France	€ 293,419,300.00
Slovakia	€ 130,600.00
Italy	€ 142,166,096.00
Malta	€ 70,000.00
United Kingdom	€ 60,632,800.00
Liechtenstein	€ 4,100.00
Spain	€ 57,537,390.00
Grand Total	€ 2,777,979,400.00
Germany	€ 54,741,853.00
Greece	€ 30,464,000.00
Austria	€ 24,750,150.00
Sweden	€ 16,232,230.00
The Netherlands	€ 14,594,500.00
Norway	€ 9,297,950.00
Portugal	€ 6,154,000.00
Poland	€ 3,396,348.00
Bulgaria	€ 3,211,070.00
Denmark	€ 2,411,400.00
Belgium	€ 1,819,500.00
Hungary	€ 1,750,761.00
Finland	€ 1,310,800.00
Cyprus	€ 1,291,500.00
Romania	€ 909,550.00
Croatia	€ 502,495.00

iii. Statistics: Total amount by type of violation

Violation Type	Sum of Amount
Non-compliance with general data processing principles	€ 1,651,341,499.00
Insufficient legal basis for data processing	€ 450,742,317.00
Insufficient TOMs to ensure information security	€ 375,780,219.00
Insufficient fulfilment of information obligations	€ 237,002,595.00
Insufficient fulfilment of data subjects' rights	€ 50,054,070.00
Unknown	€ 9,229,500.00
Insufficient fulfilment of data breach notification obligations	€ 1,497,161.00
Insufficient data processing agreement	€ 1,053,610.00
Insufficient involvement of data protection officer	€ 875,600.00
Insufficient cooperation with supervisory authority	€ 313,829.00
Insufficient fulfilment of data subject rights	€ 89,000.00
Grand Total	€ 2,777,979,400.00

While all themes (type of violation) considered in the study are relevant, greater emphasis has been placed on the top five areas of non-compliance. This approach enables the study to focus on the most significant challenges that organisations face in adhering to GDPR, and to concentrate efforts on identifying potential solutions to these challenges. By limiting the scope of the subsequent qualitative analysis to these key areas, a more comprehensive study of the pertinent issues affecting organisations can be conducted. Furthermore, this approach can facilitate the identification of appropriate TOMs that can be taken to address the implementation of PbDD. Ultimately, the study aims to provide valuable insights into the most pressing challenges faced by organisations, and to offer practical solutions to help mitigate these challenges.

Fines issued by Country (sum of amount)



iv. **Statistics: Percentage of GDPR fines by Country**

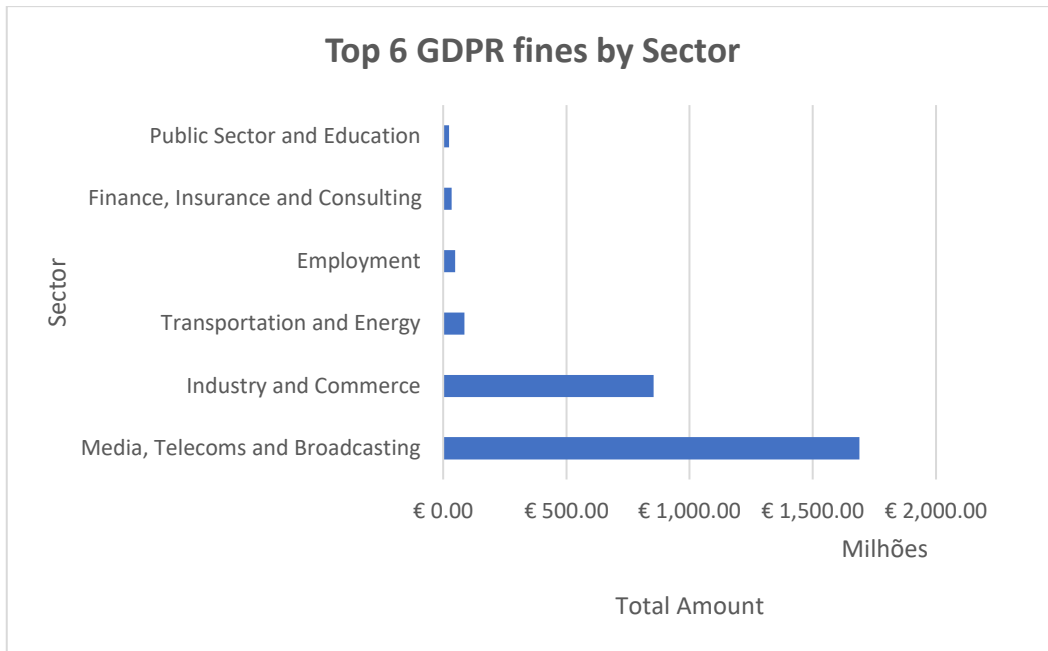
Country	%
IRELAND	46.92%
LUXEMBOURG	26.86%
FRANCE	10.56%
ITALY	5.12%
UNITED KINGDOM	2.18%
SPAIN	2.07%
GERMANY	1.97%
GREECE	1.10%
AUSTRIA	0.89%
SWEDEN	0.58%
THE NETHERLANDS	0.53%
NORWAY	0.33%
PORTUGAL	0.22%
POLAND	0.12%
BULGARIA	0.12%
DENMARK	0.09%
BELGIUM	0.07%
HUNGARY	0.06%
FINLAND	0.05%
CYPRUS	0.05%
ROMANIA	0.03%
CROATIA	0.02%
ESTONIA	0.01%
LITHUANIA	0.01%
LATVIA	0.01%
ISLE OF MAN	0.01%
ICELAND	0.01%
CZECH REPUBLIC	0.01%
SLOVAKIA	0.00%
MALTA	0.00%
LIECHTENSTEIN	0.00%
Grand Total	100.00%

Slovakia issued a total of 9 fines, out of which 4 fines amounted to €50,000, while no information was provided regarding the amount of the remaining 5 fines. Malta issued 2 fines in the sum of €70,000, whereas Liechtenstein imposed a single fine in the sum of €4,100. These values are relatively low and fall outside the percentile scale utilised in the study.



v. Statistics: GDPR fines by Sector EEA + UK

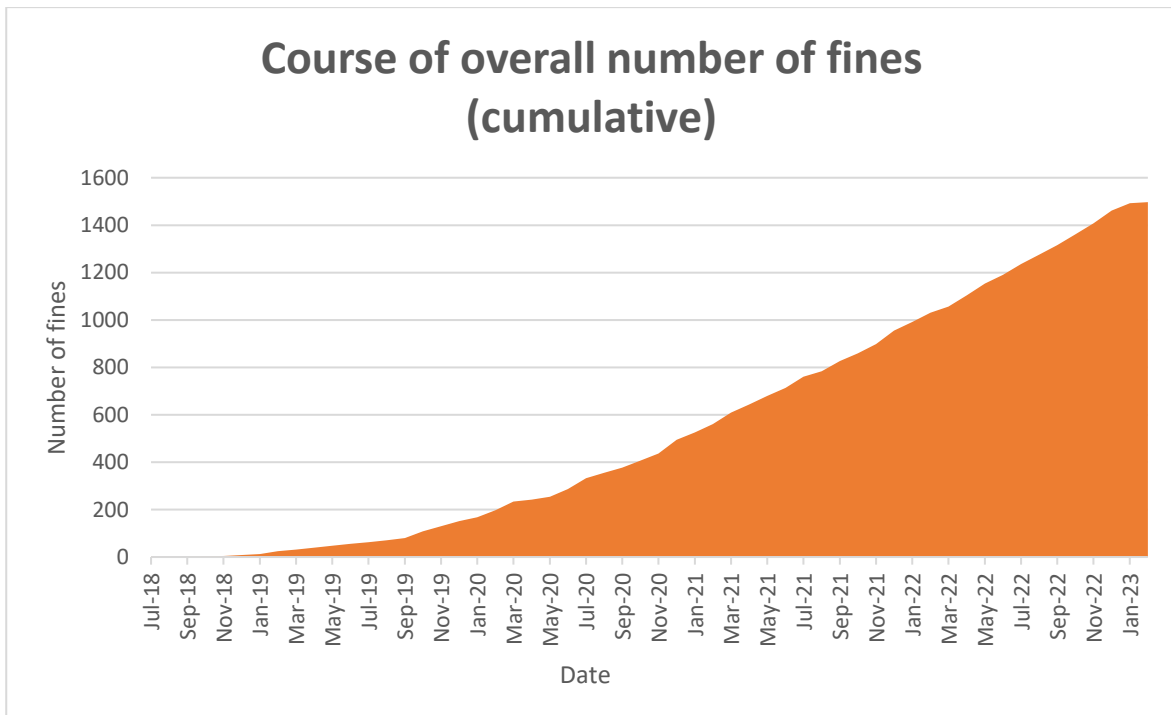
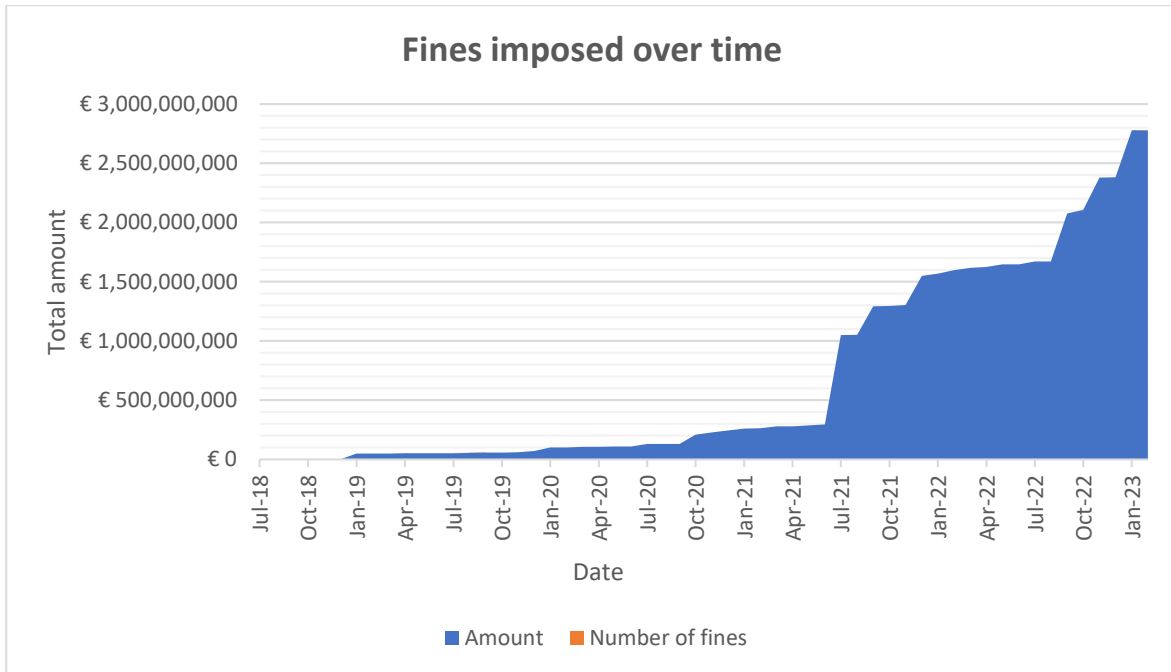
Sector	Sum of Amount
Media, Telecoms and Broadcasting	€ 1,688,555,541.00
Industry and Commerce	€ 854,307,297.00
Transportation and Energy	€ 86,459,214.00
Employment	€ 48,069,677.00
Finance, Insurance and Consulting	€ 34,426,108.00
Public Sector and Education	€ 23,829,763.00
Accommodation and Hospitality	€ 22,339,657.00
Health Care	€ 15,015,009.00
Real Estate	€ 2,578,190.00
Individuals and Private Associations	€ 1,595,596.00
Not assigned	€ 750,308.00
Unknown	€ 51,040.00
Property Owners Association	€ 2,000.00
Grand Total	€ 2,777,979,400.00



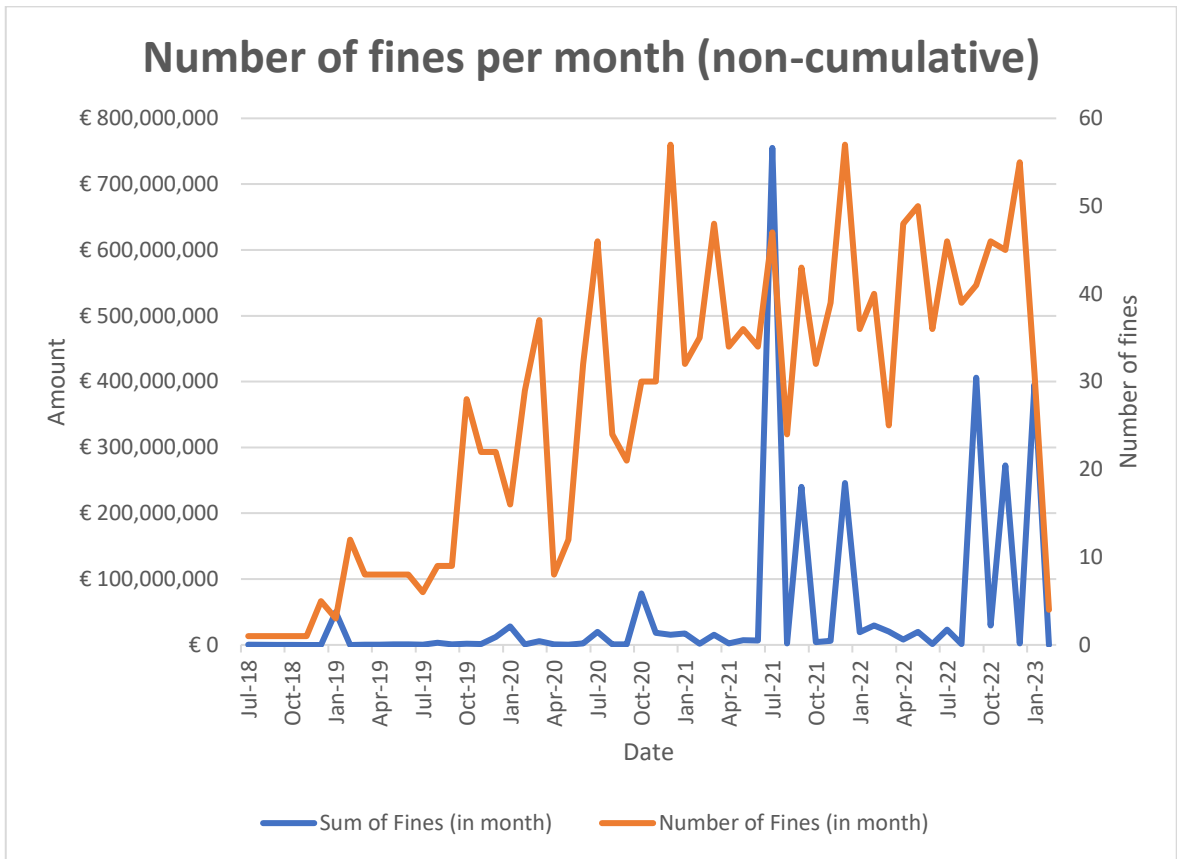
Percentage of fines by sector

Sector	% fines
Media, Telecoms and Broadcasting	60.78%
Industry and Commerce	30.75%
Transportation and Energy	3.11%
Employment	1.73%
Finance, Insurance and Consulting	1.24%
Public Sector and Education	0.86%
Accommodation and Hospitality	0.80%
Health Care	0.54%
Real Estate	0.09%
Individuals and Private Associations	0.06%
Not assigned	0.03%
Unknown	0.00%
Property Owners Association	0.00%
Grand Total	100.00%

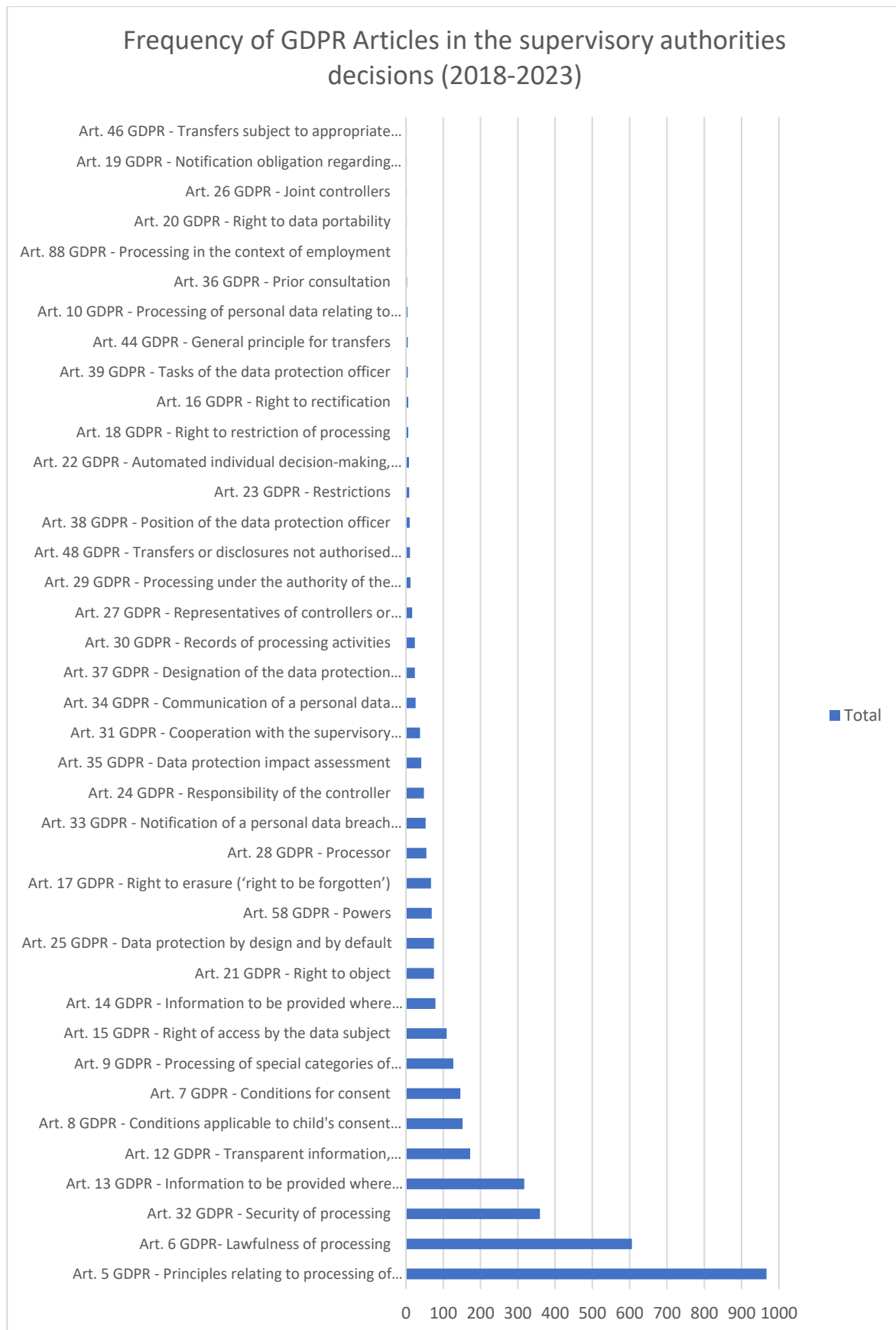
vi. **Statistics:** GDPR fines imposed over time EEA + UK



Number of fines per month EEA + UK (non-cumulative)



Annex 1.A - Frequency of fines



Number of fines by Article

Article GDPR	Occurrences
Art. 5 GDPR - Principles relating to processing of personal data	967
Art. 6 GDPR- Lawfulness of processing	606
Art. 32 GDPR - Security of processing	359
Art. 13 GDPR - Information to be provided where personal data are collected from the data subject	317
Art. 12 GDPR - Transparent information, communication, and modalities for the exercise of the rights of the data subject	172
Art. 8 GDPR - Conditions applicable to child's consent in relation to information society services	152
Art. 7 GDPR - Conditions for consent	146
Art. 9 GDPR - Processing of special categories of personal data	127
Art. 15 GDPR - Right of access by the data subject	109
Art. 14 GDPR - Information to be provided where personal data have not been obtained from the data subject	79
Art. 21 GDPR - Right to object	75
Art. 25 GDPR - Data protection by design and by default	75
Art. 58 GDPR - Powers	69
Art. 17 GDPR - Right to erasure ('right to be forgotten')	67
Art. 28 GDPR - Processor	55
Art. 33 GDPR - Notification of a personal data breach to the supervisory authority	53
Art. 24 GDPR - Responsibility of the controller	48
Art. 35 GDPR - Data protection impact assessment	41
Art. 31 GDPR - Cooperation with the supervisory authority	38
Art. 34 GDPR - Communication of a personal data breach to the data subject	26
Art. 37 GDPR - Designation of the data protection officer	24
Art. 30 GDPR - Records of processing activities	24
Art. 27 GDPR - Representatives of controllers or processors not established in the Union	17
Art. 29 GDPR - Processing under the authority of the controller or processor	12

Art. 48 GDPR - Transfers or disclosures not authorised by Union law	11
Art. 38 GDPR - Position of the data protection officer	10
Art. 23 GDPR - Restrictions	9
Art. 22 GDPR - Automated individual decision-making, including profiling	8
Art. 18 GDPR - Right to restriction of processing	6
Art. 16 GDPR - Right to rectification	6
Art. 39 GDPR - Tasks of the data protection officer	5
Art. 44 GDPR - General principle for transfers	5
Art. 10 GDPR - Processing of personal data relating to criminal convictions and offences	4
Art. 36 GDPR - Prior consultation	3
Art. 88 GDPR - Processing in the context of employment	2
Art. 20 GDPR - Right to data portability	2
Art. 26 GDPR - Joint controllers	2
Art. 19 GDPR - Notification obligation regarding rectification or erasure of personal data or restriction of processing	2
Art. 46 GDPR - Transfers subject to appropriate safeguards	2

Annex 2 - Correlation table analysis (example)

A fine can correspond to several GDPR violations, for example:

Date	Theme	Quoted Articles	SA decision (Qualitative analysis)
11/02/2021	<p>T1 Insufficient TOMs to ensure information security.</p> <p>T3 Non-compliance with general data processing principles.</p>	<p>Art. 5 (1) f) Art. 25 (1) Art. 28 (3) Art. 32 (1), (2)</p>	<p>[...] has violated the provisions of Article 5(1)(f), Article 25(1) and Article 28(1)(b) of Regulation (EC) No 1782/2003; 3, Article 32(1) and (2) of Regulation (EC) No 2016/679 [...], hereinafter referred to as "Regulation 2016/679", consisting in the non-fulfilment of the administrator's obligations under Regulation 2016/679, by:</p> <p>(a) failure to take appropriate TOMs to ensure the ability to ensure the continuity of confidentiality of processing services, failure to test and assess the effectiveness of TOMs to ensure the security of personal data contained in a copy of the database of the training platform of the National School of Judiciary and Public Prosecution, thereby taking due account of the risks associated with changes in the processing process,</p> <p>(b) entrusting the processing of personal data e. Sp. z o.o. with its registered office in W., in violation of Article 28(3) of Regulation 2016/679, i.e. without the contractual obligation of the processor to process personal data solely on the documented instructions of the controller, and without specifying in the contract the entrustment of the processing of personal data to categories of persons and without specifying the type of personal data by indicating their categories.⁹⁶⁰</p>

Art. 5 GDPR - Principles relating to processing of personal data; **Art. 25 GDPR** - Data protection by design and by default; **Art. 28 GDPR** – Processor; **Art. 32 GDPR** - Security of processing.

⁹⁶⁰ Source: President of the Office for Personal Data Protection, Krajowa Szkoła Sądownictwa i Prokuratury, Office for Personal Data Protection, Poland < <https://www.uodo.gov.pl/decyzje/DKN.5130.2024.2020>>.

ANNEX 3 – Table of variables {Cnt.X}, {Art.X}, {Violation_X}

Country	Violated Article (Per decision)	Violation Type (PbDD classification)
AUSTRIA	Art. 12 (2) GDPR	Insufficient fulfilment of data subjects' rights
	Art. 13 GDPR	Insufficient fulfilment of information obligations
	Art. 13 GDPR, Art. 35 GDPR, Art. 37 GDPR	Insufficient fulfilment of information obligations
	Art. 31 GDPR	Insufficient cooperation with supervisory authority
	Art. 5 (1) a) GDPR, Art. 5 (1) c) GDPR, Art. 6 (1) GDPR, Art. 13 GDPR	Insufficient legal basis for data processing
	Art. 5 (1) a) GDPR, Art. 6 GDPR	Insufficient legal basis for data processing
	Art. 5 (1) a) GDPR, Art. 9 (1), (2) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) a) GDPR, Art. 9 GDPR	Insufficient legal basis for data processing
	Art. 5 (1) a), c) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) f) GDPR, Art. 32 GDPR	Insufficient TOMs to ensure information security
	Art. 5 GDPR, Art. 13 GDPR, Art. 14 GDPR	Insufficient legal basis for data processing
	Art. 5 GDPR, Art. 6 GDPR	Insufficient legal basis for data processing
	Art. 6 GDPR	Insufficient legal basis for data processing
	Art. 6 GDPR, Art. 7 GDPR, Art. 12 GDPR	Insufficient legal basis for data processing
	Art. 9 GDPR	Insufficient legal basis for data processing
	Unknown	Unknown
AUSTRIA (ENDS)		
BELGIUM	Art. 12 (3) GDPR, Art. 14 (1), (2), (3) GDPR, Art. 15 GDPR, Art. 17 (1) c) GDPR, Art. 21 (2) GDPR	Insufficient fulfilment of data subjects' rights
	Art. 12 GDPR, Art. 15 GDPR, Art. 17 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 14 (1), (2) GDPR, Art. 12 (1), (2), (3) GDPR, Art. 15 (1) GDPR, Art. 5 (1) c), (2) GDPR, Art. 24 (1), (2) GDPR	Insufficient fulfilment of data subjects' rights
	Art. 14 (1), (2) GDPR, Art. 12 (3) GDPR, Art. 6 GDPR, Art. 5 (1) c), (2) GDPR, Art. 24 (1), (2) GDPR	Insufficient fulfilment of data subjects' rights
	Art. 17 GDPR, Art. 21 GDPR, Art. 31 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 31 GDPR, Art. 58 GDPR, Art. 37 GDPR	Insufficient involvement of data protection officer
	Art. 38 (6) GDPR	Insufficient involvement of data protection officer
	Art. 5 (1) a) GDPR, Art. 5 (2) GDPR, Art. 6 (1) GDPR, Art. 9 (1), (2) GDPR, Art. 12 (1) GDPR, Art. 13 GDPR, Art. 14 GDPR, Art. 24 (1) GDPR, Art. 30 GDPR, Art. 31 GDPR, Art. 32 (1), (2) GDPR, Art. 37 GDPR	Insufficient legal basis for data processing
	Art. 5 (1) a) GDPR, Art. 6 (1) f) GDPR, Art. 15 GDPR, Art. 17 GDPR, Art. 18 GDPR, Art. 21 GDPR, Art. 28 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 5 (1) a), b) GDPR, Art. 6 (1) c) GDPR, Art. 6 (3) GDPR, Art. 9 (2) i) GDPR, Art. 12 (1) GDPR, Art. 13 (1) c) GDPR, Art. 13 (2) e) GDPR, Art. 35 (1), (7) GDPR	Insufficient legal basis for data processing

	Art. 5 (1) a), c) GDPR, Art. 6 (1) GDPR, Art. 12 (2) GDPR, Art. 21 (2), (3), (4) GDPR	Insufficient legal basis for data processing
	Art. 5 (1) a), c), f) GDPR, Art. 6 (1) GDPR, Art. 9 GDPR, Art. 12 GDPR, Art. 14 GDPR, Art. 30 GDPR, Art. 32 GDPR, Art. 35 GDPR	Non-compliance with general data processing principles
	Art. 5 (1) a), c), f) GDPR, Art. 6 (1) GDPR, Art. 9 GDPR, Art. 12 GDPR, Art. 14 GDPR, Art. 32 GDPR	Non-compliance with general data processing principles
	Art. 5 (1) b) GDPR, Art. 6 GDPR	Insufficient legal basis for data processing
	Art. 5 (1) c) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) c) GDPR, Art. 6 (1) e) GDPR, Art. 9 (2) g) GDPR, Art. 12 GDPR, Art. 13 (1) c) GDPR, Art. 13 (2) e) GDPR, Art. 35 (1), (3), (7) b) GDPR	Insufficient legal basis for data processing
	Art. 5 (1) c) GDPR, Art. 6 (1) GDPR, Art. 8 GDPR	Insufficient legal basis for data processing
	Art. 5 (1) e) GDPR, Art. 5 (2) GDPR, Art. 6 (1) a) GDPR, Art. 7 (1), (3) GDPR, Art. 12 GDPR, Art. 13 GDPR, Art. 14 GDPR, Art. 24 GDPR	Insufficient legal basis for data processing
	Art. 5 (1) f) GDPR, Art. 12 GDPR, Art. 13 GDPR, Art. 14 GDPR, Art. 32 GDPR, Art. 35 (1), (3) GDPR	Insufficient TOMs to ensure information security
	Art. 5 (1) f) GDPR, Art. 32 GDPR	Insufficient TOMs to ensure information security
	Art. 5 (1) f), (2) GDPR, Art. 24 GDPR, Art. 32 GDPR, Art. 33 (1), (5) GDPR, Art. 34 (1) GDPR	Insufficient TOMs to ensure information security
	Art. 5 GDPR, Art. 6 GDPR	Insufficient legal basis for data processing
	Art. 5 GDPR, Art. 6 GDPR, Art. 12 GDPR, Art. 13 GDPR, Art. 30 GDPR, Art. 37 (5) GDPR, Art. 37 (7) GDPR	Non-compliance with general data processing principles
	Art. 5 GDPR, Art. 6 GDPR, Art. 14 GDPR	Insufficient legal basis for data processing
	Art. 5 GDPR, Art. 6 GDPR, Art. 15 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 5 GDPR, Art. 6 GDPR, Art. 17 (1) a) GDPR, Art. 12 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 5 GDPR, Art. 6 GDPR, Art. 7 GDPR, Art. 13 GDPR, Art. 24 GDPR, Art. 25 GDPR, Art. 28 GDPR	Insufficient legal basis for data processing
	Art. 5 GDPR, Art. 6 GDPR, Art. 9 GDPR	Insufficient legal basis for data processing
	Art. 6 (1) a) GDPR, Art. 7 (1) GDPR, Art. 12 (1) GDPR, Art. 13 GDPR, Art. 14 GDPR	Insufficient legal basis for data processing
	Art. 6 (1) GDPR, Art. 12 (3) GDPR, Art. 21 (1) GDPR	Insufficient legal basis for data processing
	Art. 6 GDPR	Insufficient legal basis for data processing
	Art. 6 GDPR, Art. 21 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 6 GDPR, Art. 25 GDPR	Insufficient legal basis for data processing
	Art. 6 GDPR, Art. 7 GDPR	Insufficient legal basis for data processing
	Art. 6 GDPR, Art. 12 GDPR, Art. 13 GDPR	Insufficient fulfilment of information obligations
BELGIUM (ENDS)		
BULGARIA	Art. 12 (3) GDPR, Art. 15 (1) GDPR	Insufficient fulfilment of data subjects' rights
	Art. 12 (4) GDPR, Art. 15 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 15 GDPR	Insufficient fulfilment of data subjects' rights

	Art. 25 (1) GDPR, Art. 32 GDPR	Insufficient TOMs to ensure information security
	Art. 25 (1) GDPR, Art. 32 GDPR, Art. 6 GDPR	Insufficient TOMs to ensure information security
	Art. 31 GDPR	Insufficient cooperation with supervisory authority
	Art. 32 GDPR	Insufficient TOMs to ensure information security
	Art. 5 (1) a) GDPR, Art. 6 GDPR	Insufficient legal basis for data processing
	Art. 5 (1) a) GDPR, Art. 9 (1) GDPR, Art. 9 (2) GDPR, Art. 6 (1) GDPR	Insufficient legal basis for data processing
	Art. 5 (1) b) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) b) GDPR, Art. 6 GDPR	Insufficient legal basis for data processing
	Art. 5 (1) GDPR, Art. 6 (1) GDPR	Insufficient legal basis for data processing
	Art. 6 (1) GDPR	Insufficient legal basis for data processing
	Art. 6 (1) GDPR, Art. 25 (1) GDPR	Insufficient legal basis for data processing
	Art. 6 (1) GDPR, Art. 58 (2) e) GDPR	Insufficient legal basis for data processing
	Art. 6 GDPR	Insufficient legal basis for data processing
	Art. 6 GDPR, Art. 5 (1) a) GDPR	Insufficient legal basis for data processing
BULGARIA (ENDS)		
CROATIA	Art. 13 GDPR, Art. 14 GDPR, Art 27 (1) of the National Implementation Law	Insufficient fulfilment of information obligations
	Art. 15 (1), (3) GDPR	Insufficient fulfilment of data subjects' rights
	Art. 15 (3) GDPR	Insufficient fulfilment of data subjects' rights
	Art. 25 (1) GDPR, Art. 32 (1) b) GDPR, Art. 32 (2) GDPR	Insufficient TOMs to ensure information security
	Art. 27 (1) Zakona o provedbi Opće uredbe o zaštiti podataka	Insufficient fulfilment of information obligations
	Art. 32 (1) b), (2) GDPR	Insufficient TOMs to ensure information security
	Art. 32 (1) b), d) GDPR, Art. 32 (2) GDPR, Art. 32 (4) GDPR	Insufficient TOMs to ensure information security
	Art. 32 (1) b), d) GDPR, Art. 32 (2), (4) GDPR	Insufficient TOMs to ensure information security
CROATIA (ENDS)		
CYPRUS	Art. 12 GDPR, Art. 15 GDPR, Art. 31 GDPR, Art. 58 (1) e) GDPR	Insufficient fulfilment of information obligations
	Art. 15 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 31 GDPR	Insufficient cooperation with supervisory authority
	Art. 31 GDPR, Art. 58 (1) a) GDPR	Insufficient cooperation with supervisory authority
	Art. 32 (4)	Insufficient TOMs to ensure information security
	Art. 32 GDPR	Insufficient TOMs to ensure information security
	Art. 5 (1) a) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) e), f) GDPR, Art. 32 (1) b), c) GDPR, Art. 33 (1) GDPR	Insufficient TOMs to ensure information security
	Art. 5 (1) f) GDPR, Art. 5 (2) GDPR, Art. 15 GDPR, Art. 32 GDPR, Art. 33 GDPR	Insufficient TOMs to ensure information security
	Art. 5 GDPR, Art. 6 GDPR	Insufficient legal basis for data processing
	Art. 5 GDPR, Art. 6 GDPR	Insufficient legal basis for data processing

	Art. 6 (1) GDPR, Art. 9 (2) GDPR	Insufficient legal basis for data processing
	Art. 6 GDPR	Insufficient legal basis for data processing
	Art. 6 GDPR, Art. 9 GDPR	Insufficient legal basis for data processing
CZECH REPUBLIC	Art. 12 (1) GDPR	Insufficient fulfilment of information obligations
	Art. 12 (2) GDPR, Art. 15 (1) GDPR	Insufficient fulfilment of data subjects' rights
	Art. 15 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 24 GDPR, Art. 32 (1) GDPR	Insufficient TOMs to ensure information security
	Art. 32 GDPR	Insufficient TOMs to ensure information security
	Art. 48 (1) b) LGT, Art. 21 GDPR, Art. 23 (4) LOPDGDD	Non-compliance with general data processing principles
	Art. 5 (1) a) GDPR	Insufficient fulfilment of information obligations
		Insufficient legal basis for data processing
	Art. 5 (1) a) GDPR, Art. 12 (1) GDPR, Art. 28 (2), (3) GDPR	Insufficient fulfilment of information obligations
	Art. 5 (1) a) GDPR, Art. 6 (1) GDPR, Art. 12 (2), (3) GDPR, Art. 15 GDPR, Art. 16 GDPR, Art. 17 GDPR, Art. 18 GDPR, Art. 19 GDPR, Art. 20 GDPR, Art. 21 GDPR, Art. 22 GDPR	Non-compliance with general data processing principles
	Art. 5 (1) a) GDPR, Art. 6 (1) GDPR, Art. 13 GDPR, Art. 14 (3) GDPR	Insufficient legal basis for data processing
	Art. 5 (1) a) GDPR, Art. 6 GDPR	Insufficient legal basis for data processing
	Art. 5 (1) c) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) c) GDPR, Art. 6 (1) GDPR, Art. 7 (1) GDPR, Art. 12 GDPR, Art. 13 GDPR, Art. 15 GDPR, Art. 16 GDPR, Art. 17 GDPR, Art. 18 GDPR, Art. 19 GDPR, Art. 20 GDPR, Art. 21 GDPR	Non-compliance with general data processing principles
	Art. 5 (1) GDPR	Non-compliance with general data processing principles
	Art. 5 GDPR, Art. 6 GDPR	Insufficient legal basis for data processing
	Art. 6 (1) GDPR, Art. 13 GDPR	Insufficient legal basis for data processing
	Art. 6 (1) GDPR, Art. 14 GDPR	Insufficient legal basis for data processing
	Art. 6 GDPR	Insufficient legal basis for data processing
	Art. 6 GDPR, Art. 7 GDPR	Insufficient legal basis for data processing
DENMARK	Art. 15 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 32 GDPR	Insufficient TOMs to ensure information security
	Art. 32 GDPR, Art. 33 GDPR	Insufficient TOMs to ensure information security
	Art. 36 GDPR	Insufficient TOMs to ensure information security
	Art. 5 (1) e) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) e) GDPR, Art. 5 (2) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) f) GDPR, Art. 32 GDPR	Insufficient TOMs to ensure information security
	Art. 5 (2) GDPR	Non-compliance with general data processing principles

	Art. 5 GDPR, Art. 32 GDPR	Insufficient TOMs to ensure information security
	Art. 5 GDPR, Art. 6 GDPR	Insufficient legal basis for data processing
	Art. 5 GDPR, Art. 6 GDPR, Art. 33 GDPR, Art. 34 GDPR	Non-compliance with general data processing principles
	Unknown	Non-compliance with general data processing principles
DENMARK (ENDS)		
ESTONIA	Art. 5 GDPR, Art. 6 GDPR	Insufficient legal basis for data processing
	Art. 6 GDPR	Insufficient legal basis for data processing
ESTONIA (ENDS)		
FINLAND	Art. 12 GDPR, Art. 13 GDPR, Art. 14 GDPR, Art. 15 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 35 GDPR	Non-compliance with general data processing principles
	Art. 5 (1) a) GDPR, Art. 12 (1), (2), (3), (4) GDPR, Art. 13 (1), (2) GDPR, Art. 15 (1), (3) GDPR, Art. 25 GDPR	Insufficient fulfilment of information obligations
	Art. 5 (1) a) GDPR, Art. 7 (2), (4) GDPR, Art. 12 (2) GDPR, Art. 21 (2) GDPR, Art. 24 (1) GDPR, Art. 28 (1), (3) GDPR	Insufficient legal basis for data processing
	Art. 5 (1) a), c) GDPR, Art. 25 (2) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) a), d) GDPR, Art. 12 (3) GDPR, Art. 13 GDPR, Art. 15 (1) GDPR, Art. 25 (1) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) c) GDPR, Art. 12 (1), (2), (3), (4), (6) GDPR, Art. 15 GDPR, Art. 17 GDPR, Art. 25 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 5 (1) c) GDPR, Art. 12 (3), (4), (6) GDPR, Art. 14 (2) a) GDPR, Art. 14 (3) GDPR, Art. 15 GDPR, Art. 17 (1) a) GDPR, Art. 25 (2) GDPR	Insufficient fulfilment of data subjects' rights
	Art. 5 (1) c) GDPR, Art. 6 GDPR, § 3 Law 759/2004	Non-compliance with general data processing principles
	Art. 5 (1) f) GDPR, Art. 17 GDPR, Art. 25 GDPR, Art. 32 GDPR	Insufficient TOMs to ensure information security
	Art. 5 (1) f) GDPR, Art. 33 (1) GDPR, Art. 34 (1) GDPR	Non-compliance with general data processing principles
	Art. 5 GDPR, Art. 6 GDPR	Insufficient legal basis for data processing
	Art. 5 GDPR, Art. 6 GDPR, Art. 35 GDPR	Non-compliance with general data processing principles
	Art. 58 (2) GDPR	Insufficient cooperation with supervisory authority
FINLAND (ENDS)		
FRANCE	Art. 12 GDPR, Art. 13 GDPR	Insufficient fulfilment of information obligations
	Art. 12 GDPR, Art. 13 GDPR, Art. 15 GDPR, Art. 21 GDPR, Art. 32 GDPR, L. 34-5 CPCE	Insufficient fulfilment of data subjects' rights
	Art. 12 GDPR, Art. 15 GDPR, Art. 17 GDPR, Art. 32 GDPR, Art. 33 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 12 GDPR, Art. 15 GDPR, Art. 21 GDPR, Art. 25 GDPR, Art. 32 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 13 GDPR, Art. 14 GDPR, Art. 6 GDPR, Art. 5 GDPR	Insufficient legal basis for data processing
	Art. 14 GDPR, Art. 15 GDPR, Art. 21 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 14 GDPR, Art. 28 GDPR	Insufficient fulfilment of information obligations
	Art. 16 GDPR, Art. 17 GDPR, Art. 30 GDPR, Art. 31 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 28 GDPR, Art. 29 GDPR, Art. 32 GDPR	Insufficient TOMs to ensure information security

	Art. 28 GDPR, Art. 32 GDPR, Art. 34 GDPR	Insufficient TOMs to ensure information security
	Art. 32 GDPR	Insufficient TOMs to ensure information security
	Art. 32 GDPR, Art. 33 GDPR	Insufficient TOMs to ensure information security
	Art. 5 (1) c) GDPR, Art. 12 GDPR, Art. 13 GDPR, Art. 32 GDPR	Insufficient legal basis for data processing
	Art. 5 (1) c) GDPR, Art. 5 (1) e) GDPR, Art. 5 (2) GDPR, Art. 32 GDPR	Non-compliance with general data processing principles
	Art. 5 (1) c), e) GDPR, Art. 12 GDPR	Non-compliance with general data processing principles
	Art. 5 (1) c), e) GDPR, Art. 14 GDPR, Art. 21 GDPR, Art. 28 GDPR	Insufficient legal basis for data processing
	Art. 5 (1) e) GDPR	Insufficient TOMs to ensure information security
	Art. 5 (1) e) GDPR, Art. 13 GDPR, Art. 14 GDPR	Non-compliance with general data processing principles
	Art. 5 (1) e) GDPR, Art. 13 GDPR, Art. 17 GDPR, Art. 32 GDPR, Art. 82 Loi informatique et libertés, Art. L. 34-5 CPCE	Non-compliance with general data processing principles
	Art. 5 (1) e) GDPR, Art. 13 GDPR, Art. 25 (2) GDPR, Art. 32 GDPR, Art. 35 GDPR	Non-compliance with general data processing principles
	Art. 5 (1) e) GDPR, Art. 32 GDPR	Insufficient TOMs to ensure information security
	Art. 5 (1) GDPR, Art. 13 GDPR, Art. 14 GDPR	Non-compliance with general data processing principles
	Art. 5 GDPR	Non-compliance with general data processing principles
	Art. 5 GDPR, Art. 12 GDPR, Art. 13 GDPR, Art. 15 GDPR, Art. 17 GDPR, Art. 21 GDPR, Art. 32 GDPR, Art. 33 GDPR	Non-compliance with general data processing principles
	Art. 5 GDPR, Art. 6 GDPR, Art. 13 GDPR, Art. 14 GDPR, Art. 21 GDPR, Art. 31 GDPR, Art. 44 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 6 GDPR, Art. 12 GDPR, Art. 15 GDPR, Art. 17 GDPR, Art. 31 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 7 GDPR, Art. 12 GDPR, Art. 13 GDPR, Art. 14 GDPR, Art. 15 GDPR, Art. 21 GDPR, Art. L. 34-5 CPCE	Insufficient fulfilment of data subjects' rights
	Art. 82 loi Informatique et Libertés	Insufficient legal basis for data processing
FRANCE (ENDS)		
GERMANY	Art. 12 (3) GDPR, Art. 15 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 12 GDPR, Art. 13 GDPR	Insufficient data processing agreement
	Art. 13 GDPR, Art. 28 GDPR, Art. 30 GDPR, Art. 35 GDPR	Insufficient fulfilment of information obligations
	Art. 15 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 15 GDPR, Art. 17 GDPR, Art. 21 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 15 GDPR, Art. 28 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 21 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 24 GDPR, Art. 32 GDPR	Insufficient TOMs to ensure information security
	Art. 25 GDPR, Art. 32 GDPR	Insufficient TOMs to ensure information security
	Art. 26 (2) GDPR	Insufficient data processing agreement
	Art. 28 (3) GDPR	Insufficient data processing agreement
	Art. 32 (1) GDPR	Insufficient TOMs to ensure information security
	Art. 32 GDPR	Insufficient TOMs to ensure information security
	Art. 33 (1) GDPR, Art. 34 (1) GDPR	Insufficient fulfilment of data breach notification obligations

	Art. 33 GDPR, Art. 34 GDPR	Insufficient fulfilment of data breach notification obligations
	Art. 37 GDPR	Insufficient involvement of data protection officer
	Art. 38 (6) GDPR	Insufficient involvement of data protection officer
	Art. 5 (1) a) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) a) GDPR, Art. 6 (1) GDPR	Insufficient legal basis for data processing
	Art. 5 (1) b) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) c) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) c) GDPR, Art. 17 GDPR, Art. 35 (3) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) GDPR, Art. 6 (1) GDPR, Art. 9 GDPR	Insufficient legal basis for data processing
	Art. 5 (1), (2) GDPR, Art. 6 (1) GDPR, Art. 7 (1) GDPR	Insufficient legal basis for data processing
	Art. 5 (2) GDPR	Non-compliance with general data processing principles
	Art. 5 GDPR	Non-compliance with general data processing principles
	Art. 5 GDPR, Art. 25 GDPR	Non-compliance with general data processing principles
	Art. 5 GDPR, Art. 32 GDPR	Insufficient TOMs to ensure information security
		Non-compliance with general data processing principles
	Art. 5 GDPR, Art. 6 GDPR	Insufficient legal basis for data processing
	Art. 5 GDPR, Art. 6 GDPR, Art. 32 GDPR	Insufficient TOMs to ensure information security
	Art. 58 (1) f) GDPR	Insufficient cooperation with supervisory authority
	Art. 58 (1) GDPR	Insufficient cooperation with supervisory authority
	Art. 6 (1) GDPR	Insufficient legal basis for data processing
	Art. 6 (1) GDPR, Art. 14 GDPR	Insufficient legal basis for data processing
	Art. 6 GDPR	Insufficient legal basis for data processing
	Art. 6 GDPR, Art. 12 GDPR	Insufficient legal basis for data processing
	Art. 6 GDPR, Art. 32 GDPR	Insufficient TOMs to ensure information security
	Art. 6 GDPR, Art. 5 GDPR	Insufficient legal basis for data processing
	Art. 6 GDPR, Art. 9 GDPR	Insufficient legal basis for data processing
	Unknown	Insufficient involvement of data protection officer
	Unknown	Insufficient legal basis for data processing
GERMANY (ENDS)		
GREECE	Art. 12 (1) GDPR, Art. 15 (1) GDPR	Insufficient fulfilment of data subjects' rights
	Art. 12 (1), (2) GDPR, Art. 15 (1) GDPR	Insufficient fulfilment of data subjects' rights
	Art. 12 (1), (2), (3) GDPR, Art. 15 (1) GDPR	Insufficient fulfilment of data subjects' rights
	Art. 12 (3) GDPR	Insufficient fulfilment of data subjects' rights
	Art. 12 (3), (4) GDPR	Insufficient fulfilment of information obligations
	Art. 12 GDPR, Art. 11 Law 3471/2006	Insufficient fulfilment of data subjects' rights

	Art. 12 GDPR, Art. 14 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 13 GDPR	Insufficient fulfilment of information obligations
	Art. 13 GDPR, Art. 14 GDPR, Art. 11 Law 3471/2006	Insufficient fulfilment of information obligations
	Art. 13 GDPR, Art. 32 GDPR, Art. 33 GDPR, Art. 37 GDPR	Insufficient TOMs to ensure information security
	Art. 15 GDPR	Insufficient fulfilment of data subject rights
		Insufficient fulfilment of data subjects' rights
	Art. 15 GDPR, Art. 11 Law 3471/2006	Insufficient fulfilment of data subjects' rights
	Art. 15 GDPR, Art. 58 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 17 GDPR, Art. 21 GDPR, Art. 25 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 21 (3) GDPR, Art. 25 GDPR	Insufficient fulfilment of data subjects' rights
		Non-compliance with general data processing principles
	Art. 21 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 28 (3) c) GDPR, Art. 32 (2), (4) GDPR, Art. 11 (1) Νόμος 3471/2006	Insufficient TOMs to ensure information security
	Art. 29 GDPR	Insufficient legal basis for data processing
	Art. 31 GDPR	Insufficient cooperation with supervisory authority
	Art. 32 GDPR	Insufficient TOMs to ensure information security
	Art. 5 (1) a) GDPR	Insufficient legal basis for data processing
	Art. 5 (1) a) GDPR, Art. 5 (2) GDPR, Art. 13 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 5 (1) a) GDPR, Art. 5 (2) GDPR, Art. 13 GDPR, Art. 14 GDPR, Art. 25 (1) GDPR, Art. 26 GDPR, Art. 28 GDPR, Art. 35 (7) GDPR	Insufficient TOMs to ensure information security
	Art. 5 (1) a) GDPR, Art. 5 (2) GDPR, Art. 6 GDPR, Art. 12 (2) GDPR	Insufficient fulfilment of data subjects' rights
	Art. 5 (1) a) GDPR, Art. 6 GDPR, Art. 9 GDPR, Art. 12 GDPR, Art. 14 GDPR, Art. 15 GDPR, Art. 27 GDPR	Non-compliance with general data processing principles
	Art. 5 (1) a), (2) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) a), (2) GDPR Total	
	Art. 5 (1) a), b) GDPR, Art. 12 (3) GDPR, Art. 15 GDPR, Art. 17 GDPR	Non-compliance with general data processing principles
	Art. 5 (1) a), b) GDPR, Art. 5 (2) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) a), b) GDPR, Art. 5 (2) GDPR, Art. 6 GDPR, Art. 12 GDPR, Art. 13 GDPR, Art. 30 GDPR	Non-compliance with general data processing principles
	Art. 5 (1) a), e) GDPR, Art. 5 (2) GDPR, Art. 6 (1) GDPR, Art. 12 (2), (3) GDPR, Art. 17 GDPR	Non-compliance with general data processing principles
	Art. 5 (1) c) GDPR, Art. 12 (3) GDPR, Art. 15 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 5 (1) c) GDPR, Art. 25 GDPR	Non-compliance with general data processing principles
	Art. 5 (1) c) GDPR, Art. 6 (1) f) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) e) GDPR, Art. 25 GDPR	Non-compliance with general data processing principles
	Art. 5 (1) f) GDPR	Non-compliance with general data processing principles

	Art. 5 (1) f) GDPR, Art. 33 GDPR, Art. 34 GDPR	Non-compliance with general data processing principles
	Art. 5 (1) GDPR, Art. 5 (2) GDPR, Art. 6 (1) GDPR, Art. 13 (1) c) GDPR, Art. 14 (1) c) GDPR	Insufficient legal basis for data processing
	Art. 5 GDPR	Non-compliance with general data processing principles
	Art. 5 GDPR, Art. 6 GDPR, Art. 32 GDPR	Insufficient TOMs to ensure information security
	Art. 6 (1) c) GDPR, Art. 12 (3), (4) GDPR, Art. 17 (1) d) GDPR	Insufficient legal basis for data processing
	Art. 6 GDPR, Art. 12 (2) GDPR, Art. 21 GDPR	Insufficient legal basis for data processing
GREECE (ENDS)		
HUNGARY	Art. 12 (3), (4), (5) GDPR, Art. 15 GDPR, Art. 18 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 12 (4) GDPR, Art. 15 GDPR, Art. 18 (1) c) GDPR, Art. 13 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 12 GDPR, Art. 15 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 12 GDPR, Art. 15 GDPR, Art. 17 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 12 GDPR, Art. 15 GDPR, Art. 18 (1) c) GDPR, Art. 25 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 15 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 24 GDPR, Art. 32 GDPR	Insufficient TOMs to ensure information security
	Art. 25 (1), (2) GDPR, Art. 32 (1) b) GDPR, Art. 34 (1) GDPR	Insufficient TOMs to ensure information security
	Art. 32 (1) a), b) GDPR, Art. 32 (2) GDPR, Art. 33 (1) GDPR, Art. 34 (1) GDPR	Insufficient TOMs to ensure information security
	Art. 32 (1) GDPR	Insufficient TOMs to ensure information security
	Art. 32 GDPR, Art. 33 GDPR	Insufficient fulfilment of data breach notification obligations
	Art. 33 (1) GDPR, Art. 33 (5) GDPR, Art. 34 (1) GDPR	Insufficient fulfilment of data breach notification obligations
	Art. 33 GDPR	Insufficient fulfilment of data breach notification obligations
	Art. 5 (1) a) GDPR, Art. 5 (1) c) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) a) GDPR, Art. 5 (2) GDPR, Art. 12 (3), (4) GDPR, Art. 31 GDPR	Non-compliance with general data processing principles
	Art. 5 (1) a) GDPR, Art. 6 GDPR	Insufficient legal basis for data processing
	Art. 5 (1) a), (2) GDPR, Art. 6 GDPR, Art. 13 GDPR	Insufficient legal basis for data processing
	Art. 5 (1) a), b) GDPR, Art. 6 (1) GDPR, Art. 9 (1) GDPR	Insufficient legal basis for data processing
	Art. 5 (1) a), b) GDPR, Art. 6 (1), (4) GDPR, Art. 12 (1) GDPR, Art. 13 GDPR, Art. 14 GDPR, Art. 21 (1), (2) GDPR, Art. 24 (1) GDPR, Art. 25 (1), (2) GDPR	Insufficient legal basis for data processing
	Art. 5 (1) a), b), c) GDPR, Art. 6 (1) GDPR, Art. 9 (2) GDPR, Art. 12 GDPR, Art. 13 GDPR	Insufficient legal basis for data processing
	Art. 5 (1) a), b), c) GDPR, Art. 6 GDPR, Art. 13 (1), (2) GDPR	Insufficient legal basis for data processing
	Art. 5 (1) b) GDPR, Art. 5 (1) c) GDPR, Art. 13 (3) GDPR, Art. 17 (1) GDPR, Art. 6 (4) GDPR	Insufficient fulfilment of data subjects' rights
	Art. 5 (1) b) GDPR, Art. 6 (1) GDPR, Art. 12 (1) GDPR, Art. 14 GDPR	Non-compliance with general data processing principles
	Art. 5 (1) b), (e) GDPR, Art. 32 (1), (2) GDPR	Insufficient TOMs to ensure information security
	Art. 5 (1) b), c) GDPR, Art. 13 (1) GDPR	Insufficient fulfilment of information obligations

	Art. 5 (1) b), c) GDPR, Art. 5 (2) GDPR, Art. 6 (1) GDPR, Art. 13 (1), (2) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) b), c) GDPR, Art. 6 (1) f) GDPR, Art. 13 (1), (2) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) c) GDPR, Art. 6 (1) GDPR, Art. 9 (1) GDPR, Art. 12 GDPR	Insufficient legal basis for data processing
	Art. 5 (1) d) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) d) GDPR, Art. 6 (1) GDPR, Art. 12 (2), (3), (4) GDPR, Art. 17 (1) GDPR, Art. 25 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 5 (1) GDPR, Art. 12 (2) GDPR, Art. 13 (1) GDPR	Insufficient fulfilment of data subjects' rights
	Art. 5 (1), (2) GDPR, Art. 6 (1) GDPR, Art. 12 (1) GDPR, Art. 13 GDPR	Insufficient legal basis for data processing
	Art. 5 (1), (2) GDPR, Art. 6 GDPR, Art. 13 GDPR	Insufficient legal basis for data processing
	Art. 5 (2) GDPR, Art. 24 GDPR	Non-compliance with general data processing principles
	Art. 5 (2) GDPR, Art. 6 (1) GDPR, Art. 12 (1) GDPR	Insufficient legal basis for data processing
	Art. 5 (2) GDPR, Art. 6 (1) GDPR, Art. 12 (2) GDPR, Art. 17 (1) b) GDPR	Insufficient legal basis for data processing
	Art. 5 GDPR, Art. 14 GDPR	Non-compliance with general data processing principles
	Art. 5 GDPR, Art. 6 GDPR	Insufficient legal basis for data processing
	Art. 5 GDPR, Art. 6 GDPR, Art. 12 GDPR, Art. 15 GDPR, Art. 17 GDPR	Insufficient legal basis for data processing
	Art. 5 GDPR, Art. 6 GDPR, Art. 13 GDPR	Non-compliance with general data processing principles
	Art. 5 GDPR, Art. 6 GDPR, Art. 13 GDPR, Art. 24 GDPR, Art. 25 GDPR	Non-compliance with general data processing principles
	Art. 5 GDPR, Art. 6 GDPR, Art. 17 GDPR	Insufficient legal basis for data processing
	Art. 5 GDPR, Art. 6 GDPR, Art. 21 GDPR	Insufficient legal basis for data processing
	Art. 5 GDPR, Art. 6 GDPR, Art. 13 GDPR, Art. 24 GDPR, Art. 25 GDPR	Non-compliance with general data processing principles
	Art. 6 (1) GDPR	Insufficient legal basis for data processing
	Art. 6 GDPR, Art. 15 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 6 GDPR, Art. 5 (1) b) GDPR, Art. 13 GDPR	Insufficient legal basis for data processing
HUNGARY (ENDS)		
ICELAND	Art. 15 (1), (3) GDPR, Art. 9 (1) Act 90/2018, Art. 17 (2) Act 90/2018	Insufficient fulfilment of data subjects' rights
	Art. 32 (1) b), d) GDPR	Insufficient TOMs to ensure information security
	Art. 5 (1) a), c) GDPR, Art. 6 (1) GDPR, Art. 12 (1) GDPR, Art. 13 (1), (2) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) c) GDPR, Art. 6 GDPR	Non-compliance with general data processing principles
	Art. 5 (1) f) GDPR, Art. 32 GDPR	Insufficient TOMs to ensure information security
	Art. 5 GDPR, Art. 6 GDPR, Art. 28 GDPR, Art. 32 GDPR	Non-compliance with general data processing principles
	Art. 5 GDPR, Art. 6 GDPR, Art. 32 GDPR	Insufficient legal basis for data processing
	Art. 5 GDPR, Art. 6 GDPR, Art. 7 GDPR, Art. 13 GDPR, Art. 25 GDPR, Art. 28 GDPR, Art. 32 GDPR	Non-compliance with general data processing principles
ICELAND (ENDS)		
IRELAND	Art. 13 GDPR, Art. 12 GPDR, Art. 15 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 21 GDPR	Insufficient fulfilment of data subjects' rights

	Art. 25 (1), (2) GDPR	Insufficient TOMs to ensure information security
	Art. 32 (1) GDPR	Insufficient TOMs to ensure information security
	Art. 32 GDPR, Art. 33 GDPR, Art. 34 GDPR	Insufficient TOMs to ensure information security
	Art. 33 (1), (5) GDPR	Insufficient fulfilment of data breach notification obligations
	Art. 33 GDPR	Insufficient fulfilment of data breach notification obligations
	Art. 5 (1) a) GDPR, Art. 12 (1) GDPR, Art. 13 (1) c) GDPR	Insufficient fulfilment of information obligations
	Art. 5 (1) a) GDPR, Art. 12 GDPR, Art. 13 GDPR, Art. 14 GDPR	Insufficient fulfilment of information obligations
	Art. 5 (1) a) GDPR, Art. 6 (1) GDPR, Art. 12 GDPR, Art. 13 (1) c) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) a), c) GDPR, Art. 6 (1) GDPR, Art. 12 (1) GDPR, Art. 24 GDPR, Art. 25 (1), (2) GDPR, Art. 35 GDPR	Non-compliance with general data processing principles
	Art. 5 (1) e), f) GDPR, Art. 32 (1) GDPR, Art. 33 (1) GDPR	Insufficient TOMs to ensure information security
	Art. 5 (1) f) GDPR, Art. 24 GDPR, Art. 28 (1), (3) GDPR, Art. 30 (1) GDPR, Art. 32 (1) GDPR	Insufficient TOMs to ensure information security
	Art. 5 (1) f) GDPR, Art. 32 (1) GDPR	Insufficient TOMs to ensure information security
	Art. 5 (1) GDPR, Art. 32 (1) GDPR, Art. 33 GDPR	Insufficient TOMs to ensure information security
	Art. 5 (2) GDPR, Art. 24 (1) GDPR	Insufficient TOMs to ensure information security
	Art. 5 (2) GDPR, Art. 24 (1) GDPR, Art. 25 (1) GDPR	Insufficient TOMs to ensure information security
	Art. 5 GDPR, Art. 32 GDPR	Insufficient TOMs to ensure information security
	Art. 5 GDPR, Art. 6 GDPR	Insufficient legal basis for data processing
IRELAND (ENDS)		
ISLE OF MAN	Art. 12 GDPR, Art. 15 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 31 GDPR	Insufficient cooperation with supervisory authority
	Art. 5 (1) c), f) GDPR, Art. 5 (2) GDPR, Art. 24 GDPR, Art. 25 GDPR, Art. 32 GDPR, Art. 34 GDPR, Art. 58 GDPR	Non-compliance with general data processing principles
ISLE OF MAN (ENDS)		
ITALY	Art. 12 (1), (2), (3), (4) GDPR, Art. 15 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 12 (3) GDPR, Art. 14 GDPR, Art. 15 GDPR, Art. 17 GDPR, Art. 21 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 12 (3) GDPR, Art. 15 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 12 (3), (4) GDPR	Insufficient fulfilment of data subjects' rights
		Insufficient legal basis for data processing
	Art. 12 (3), (4) GDPR, Art. 15 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 12 (3), (4) GDPR, Art. 17 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 12 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 12 GDPR, Art. 13 GDPR, Art. 14 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 12 GDPR, Art. 15 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 12 GDPR, Art. 17 GDPR, Art. 157 Codice della privacy	Insufficient fulfilment of data subjects' rights
	Art. 13 GDPR	Insufficient fulfilment of information obligations

Art. 13 GDPR, Art. 15 GDPR, Art. 21 GDPR, Art. 157 Codice della privacy, Art. 166 (2) Codice della privacy	Insufficient fulfilment of data subjects' rights
Art. 15 GDPR	Insufficient fulfilment of data subjects' rights
Art. 28 (2) GDPR, Art. 32 GDPR	Insufficient TOMs to ensure information security
Art. 28 GDPR	Insufficient data processing agreement
Art. 28 GDPR, Art. 32 GDPR	Insufficient TOMs to ensure information security
Art. 32 GDPR	Insufficient TOMs to ensure information security
Art. 5 (1) a) GDPR	Insufficient legal basis for data processing
	Non-compliance with general data processing principles
Art. 5 (1) a) GDPR, Art. 12 GDPR, Art. 13 GDPR	Insufficient fulfilment of information obligations
	Insufficient legal basis for data processing
Art. 5 (1) a) GDPR, Art. 12 GDPR, Art. 15 GDPR	Insufficient fulfilment of data subjects' rights
Art. 5 (1) a) GDPR, Art. 13 GDPR	Insufficient fulfilment of information obligations
	Insufficient legal basis for data processing
Art. 5 (1) a) GDPR, Art. 13 GDPR, Art. 14 GDPR, Art. 28 (2), (3) GDPR, Art. 32 GDPR	Non-compliance with general data processing principles
Art. 5 (1) a) GDPR, Art. 13 GDPR, Art. 88 GDPR, Art. 114 Codice della privacy	Non-compliance with general data processing principles
Art. 5 (1) a) GDPR, Art. 6 (1) a) GDPR, Art. 12 GDPR, Art. 13 GDPR, Art. 14 GDPR, Art. 21 GDPR	Insufficient legal basis for data processing
Art. 5 (1) a) GDPR, Art. 6 (1) a) GDPR, Art. 12 GDPR, Art. 21 GDPR	Insufficient legal basis for data processing
Art. 5 (1) a) GDPR, Art. 6 (1) GDPR	Insufficient legal basis for data processing
Art. 5 (1) a) GDPR, Art. 6 (1) GDPR, Art. 21 (2), (3) GDPR, Art. 12 (3) GDPR, Art. 25 (1) GDPR	Insufficient legal basis for data processing
Art. 5 (1) a) GDPR, Art. 6 GDPR, Art. 113 Codice della privacy, Art. 114 Codice della privacy	Insufficient legal basis for data processing
Art. 5 (1) a) GDPR, Art. 6 GDPR, Art. 13 GDPR, Art. 28 GDPR, Art. 32 GDPR	Insufficient TOMs to ensure information security
Art. 5 (1) a) GDPR, Art. 6 GDPR, Art. 28 GDPR, Art. 2-ter Codice della privacy	Insufficient legal basis for data processing
Art. 5 (1) a) GDPR, Art. 6 GDPR, Art. 2-ter (1), (3) Codice della privacy	Insufficient legal basis for data processing
Art. 5 (1) a) GDPR, Art. 6 GDPR, Art. 30 (2) GDPR, Art. 2-ter Codice della privacy	Insufficient legal basis for data processing
Art. 5 (1) a) GDPR, Art. 6 GDPR, Art. 37 (1) a) GDPR, Art. 37 (7) GDPR, Art. 38 (6) GDPR	Non-compliance with general data processing principles
Art. 5 (1) a) GDPR, Art. 6 GDPR, Art. 7 GDPR, Art. 12 (1) GDPR, Art. 13 GDPR, Art. 130 (1), (2), (3) Codice della privacy	Non-compliance with general data processing principles
Art. 5 (1) a) GDPR, Art. 6 GDPR, Art. 7 GDPR, Art. 13 GDPR, Art. 14 GDPR	Insufficient legal basis for data processing
Art. 5 (1) a) GDPR, Art. 6 GDPR, Art. 88 GDPR, Art. 113 Codice della privacy	Insufficient legal basis for data processing
Art. 5 (1) a) GDPR, Art. 6 GDPR, Art. 9 GDPR	Insufficient legal basis for data processing
Art. 5 (1) a) GDPR, Art. 6 GDPR, Art. 9 GDPR, Art. 10 GDPR, Art. 2-ter Codice della privacy, Art. 2-sexies Codice della privacy, Art. 2-octies Codice della privacy	Insufficient legal basis for data processing

Art. 5 (1) a) GDPR, Art. 6 GDPR, Art. 9 GDPR, Art. 32 GDPR	Insufficient TOMs to ensure information security
Art. 5 (1) a) GDPR, Art. 9 GDPR	Insufficient legal basis for data processing
Art. 5 (1) a) GDPR, Art. 9 GDPR, Art. 13 GDPR, Art. 30 (1) c) GDPR	Non-compliance with general data processing principles
Art. 5 (1) a), b), c) GDPR, Art. 6 (1) c), e) GDPR, Art. 6 (2) GDPR, Art. 6 (3) b) GDPR, Art. 37 (1), (7) GDPR	Non-compliance with general data processing principles
Art. 5 (1) a), b), e) GDPR, Art. 6 GDPR, Art. 9 GDPR, Art. 12 GDPR, Art. 13 GDPR, Art. 14 GDPR, Art. 15 GDPR, Art. 27 GDPR	Non-compliance with general data processing principles
Art. 5 (1) a), b), f) GDPR, Art. 6 GDPR, Art. 7 GDPR, Art. 9 GDPR, Art. 12 GDPR, Art. 13 GDPR, Art. 27 GDPR	Non-compliance with general data processing principles
Art. 5 (1) a), c) GDPR	Insufficient legal basis for data processing
	Non-compliance with general data processing principles
Art. 5 (1) a), c) GDPR, Art. 114 Codice della privacy	Non-compliance with general data processing principles
Art. 5 (1) a), c) GDPR, Art. 12 (1) GDPR, Art. 13 GDPR, Art. 35 GDPR	Non-compliance with general data processing principles
Art. 5 (1) a), c) GDPR, Art. 12 (3), (4) GDPR, Art. 2-ter Codice della privacy	Non-compliance with general data processing principles
Art. 5 (1) a), c) GDPR, Art. 13 GDPR	Non-compliance with general data processing principles
Art. 5 (1) a), c) GDPR, Art. 6 (1) b), c) GDPR, Art. 9 (1) b) GDPR	Insufficient legal basis for data processing
Art. 5 (1) a), c) GDPR, Art. 6 (1) c), e) Art. 6 (2) GDPR, Art. 6 (3) b) GDPR GDPR, Art. 2-ter (1), (3) Codice della privacy	Insufficient legal basis for data processing
Art. 5 (1) a), c) GDPR, Art. 6 (1) c), e) GDPR, Art. 6 (2) GDPR, Art. 6 (3) b) GDPR	Insufficient legal basis for data processing
	Non-compliance with general data processing principles
Art. 5 (1) a), c) GDPR, Art. 6 (1) c), e) GDPR, Art. 6 (2) GDPR, Art. 6 (3) b) GDPR, Art. 37 (1) a) GDPR, Art. 37 (7) GDPR	Non-compliance with general data processing principles
Art. 5 (1) a), c) GDPR, Art. 6 (1) c), e) GDPR, Art. 6 (2) GDPR, Art. 6 (3) b) GDPR, Art. 9 (1), (2), (4) GDPR, Art. 2-ter (1), (3) Codice della privacy, Art. 2-septies (8) Codice della privacy	Non-compliance with general data processing principles
Art. 5 (1) a), c) GDPR, Art. 6 GDPR	Insufficient legal basis for data processing
Art. 5 (1) a), c) GDPR, Art. 6 GDPR, Art. 10 GDPR, Art. 2-ter Codice della privacy, Art. 2-octies Codice della privacy	Insufficient legal basis for data processing
Art. 5 (1) a), c) GDPR, Art. 6 GDPR, Art. 2-ter Codice della privacy	Insufficient legal basis for data processing
Art. 5 (1) a), c) GDPR, Art. 6 GDPR, Art. 2-ter Codice della privacy	Non-compliance with general data processing principles
Art. 5 (1) a), c) GDPR, Art. 6 GDPR, Art. 9 GDPR	Insufficient legal basis for data processing
Art. 5 (1) a), c) GDPR, Art. 6 GDPR, Art. 9 GDPR, Art. 13 GDPR, Art. 35 GDPR	Non-compliance with general data processing principles
Art. 5 (1) a), c) GDPR, Art. 9 GDPR, Art. 2-ter Codice della privacy	Non-compliance with general data processing principles
Art. 5 (1) a), c), d) GDPR, Art. 25 GDPR, Art. 35 GDPR	Non-compliance with general data processing principles
Art. 5 (1) a), c), e) GDPR, Art. 12 GDPR, Art. 13 GDPR	Non-compliance with general data processing principles
Art. 5 (1) a), c), e) GDPR, Art. 13 GDPR, Art. 157 Codice della privacy	Non-compliance with general data processing principles
Art. 5 (1) a), c), e) GDPR, Art. 13 GDPR, Art. 22 (3) GDPR, Art. 25 GDPR, Art. 30	Non-compliance with general data processing principles

	(1) a), b), c), f), g) GDPR, Art. 32 GDPR, Art. 35 GDPR, Art. 37 (7) GDPR	
	Art. 5 (1) a), c), e) GDPR, Art. 13 GDPR, Art. 22 (3) GDPR, Art. 25 GDPR, Art. 30 (1) c), f), g) GDPR, Art. 32 GDPR, Art. 35 GDPR, Art. 37 (7) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) a), c), e) GDPR, Art. 6 GDPR, Art. 9 GDPR, Art. 13 GDPR, Art. 25 GDPR, Art. 35 GDPR, Art. 44 GDPR, Art. 46 GDPR, Art. Art. 2-sexies Codice della Privacy	Non-compliance with general data processing principles
	Art. 5 (1) a), d) GDPR, Art. 5 (2) GDPR, Art. 6 (1) GDPR, Art. 12 GDPR, Art. 13 GDPR, Art. 21 GDPR, Art. 24 GDPR, Art. 25 (1) GDPR, Art. 30 GDPR, Art. 31 GDPR, Art. 130 (1), (2), (4) Codice della privacy	Insufficient legal basis for data processing
	Art. 5 (1) a), d) GDPR, Art. 5 (2) GDPR, Art. 6 GDPR, Art. 9 GDPR, Art. 12 GDPR, Art. 13 GDPR, Art. 14 GDPR, Art. 24 GDPR	Non-compliance with general data processing principles
	Art. 5 (1) a), d), f) GDPR, Art. 9 GDPR, Art. 32 (1) b) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) a), e) GDPR, Art. 13 GDPR, Art. 12 (3) GDPR, Art. 15 GDPR, Art. 157 Codice della privacy, Art. 166 (2) Codice della privacy	Insufficient legal basis for data processing
	Art. 5 (1) a), e) GDPR, Art. 5 (2) GDPR, Art. 12 GDPR, Art. 13 GDPR, Art. 24 GDPR, Art. 38 (6) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) a), e) GDPR, Art. 6 (1) b), c) GDPR	Insufficient legal basis for data processing
	Art. 5 (1) a), e) GDPR, Art. 6 GDPR, Art. 9 GDPR, Art. 28 GDPR	Insufficient legal basis for data processing
	Art. 5 (1) a), e), f) GDPR, Art. 6 GDPR, Art. 7 GDPR, Art. 12 (1) GDPR, Art. 13 GDPR, Art. 14 GDPR, Art. 27 (4) GDPR, Art. 28 GDPR, Art. 32 GDPR, Art. 35 GDPR	Non-compliance with general data processing principles
	Art. 5 (1) a), f) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) a), f) GDPR, Art. 13 GDPR, Art. 14 GDPR, Art. 25 GDPR, Art. 30 GDPR, Art. 32 GDPR, Art. 35 GDPR	Non-compliance with general data processing principles
	Art. 5 (1) a), f) GDPR, Art. 13 GDPR, Art. 25 GDPR, Art. 32 GDPR	Non-compliance with general data processing principles
	Art. 5 (1) a), f) GDPR, Art. 6 (1) e) GDPR, Art. 9 (2) g) GDPR, Art. 32 GDPR, Art. 2-ter Codice della privacy, Art. 2-sexies Codice della privacy	Insufficient TOMs to ensure information security
	Art. 5 (1) a), f) GDPR, Art. 6 (1) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) a), f) GDPR, Art. 6 GDPR	Insufficient legal basis for data processing
	Art. 5 (1) a), f) GDPR, Art. 9 GDPR	Insufficient legal basis for data processing
		Non-compliance with general data processing principles
	Art. 5 (1) a), f) GDPR, Art. 9 GDPR, Art. 25 GDPR, Art. 32 GDPR	Insufficient TOMs to ensure information security
	Art. 5 (1) a), f) GDPR, Art. 9 GDPR, Art. 32 GDPR	Insufficient TOMs to ensure information security
	Art. 5 (1) a), f) GDPR, Art. 9 GDPR, Art. 32 GDPR,	Insufficient TOMs to ensure information security
	Art. 5 (1) c) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) c) GDPR, Art. 13 GDPR	Non-compliance with general data processing principles

	Art. 5 (1) c) GDPR, Art. 6 (1) c) GDPR, Art. 6 (2) GDPR, Art. 6 (3) b) GDPR, Art. 2-ter (1), (3) Codice della privacy	Insufficient legal basis for data processing
	Art. 5 (1) c) GDPR, Art. 6 (1) c), d) GDPR, Art. 6 (2), (3) GDPR, Art. 9 (1), (2), (4) GDPR, Art. 2-ter (1), (2) Codice della privacy, Art. 2-septies (8) Codice della privacy	Insufficient legal basis for data processing
	Art. 5 (1) d), e) GDPR, Art. 5 (2) GDPR, Art. 12 GDPR, Art. 15 GDPR, Art. 24 GDPR	Non-compliance with general data processing principles
	Art. 5 (1) f) GDPR, Art. 13 GDPR, Art. 14 GDPR, Art. 28 GDPR, Art. 30 GDPR, Art. 32 GDPR, Art. 35 GDPR	Non-compliance with general data processing principles
	Art. 5 (1) f) GDPR, Art. 25 GDPR, Art. 32 GDPR	Insufficient TOMs to ensure information security
	Art. 5 (1) f) GDPR, Art. 32 GDPR	Insufficient TOMs to ensure information security
	Art. 5 (1) f) GDPR, Art. 32 GDPR, Art. 35 GDPR	Insufficient TOMs to ensure information security
	Art. 5 (1) f) GDPR, Art. 6 GDPR, Art. 9 GDPR	Insufficient legal basis for data processing
	Art. 5 (1) f) GDPR, Art. 9 GDPR	Insufficient legal basis for data processing
		Non-compliance with general data processing principles
	Art. 5 (1) f) GDPR, Art. 9 GDPR, Art. 32 GDPR	Insufficient TOMs to ensure information security
	Art. 5 (1), (2) GDPR, Art. 6 (1) GDPR, Art. 7 (1) GDPR	Insufficient legal basis for data processing
	Art. 5 (1), (2) GDPR, Art. 6 (1) GDPR, Art. 7 GDPR, Art. 12 (2) GDPR, Art. 14 GDPR, Art. 21 GDPR, Art. 28 GDPR, Art. 29 GDPR	Insufficient legal basis for data processing
	Art. 5 (1), (2) GDPR, Art. 6 (1) GDPR, Art. 7 GDPR, Art. 15 (1) GDPR, Art. 16 GDPR, Art. 21 GDPR, Art. 24 GDPR, Art. 25 (1) GDPR, Art. 32 GDPR, Art. 33 GDPR	Non-compliance with general data processing principles
	Art. 5 (2) a), f) GDPR, Art. 9 GDPR	Non-compliance with general data processing principles
	Art. 5 (2) GDPR, Art. 28 GDPR	Insufficient data processing agreement
	Art. 5 (2) GDPR, Art. 6 (1) a) GDPR, Art. 12 (3) GDPR, Art. 15 GDPR, Art. 17 GDPR, Art. 21 GDPR, Art. 24 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 5 GDPR, Art. 12 GDPR, Art. 13 GDPR, Art. 15 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 5 GDPR, Art. 12 GDPR, Art. 13 GDPR, Art. 15 GDPR, Art. 114 Codice della privacy	Insufficient fulfilment of data subjects' rights
	Art. 5 GDPR, Art. 12 GDPR, Art. 13 GDPR, Art. 25 GDPR, Art. 28 GDPR, Art. 32 GDPR	Non-compliance with general data processing principles
	Art. 5 GDPR, Art. 12 GDPR, Art. 37 GDPR	Non-compliance with general data processing principles
	Art. 5 GDPR, Art. 13 GDPR	Non-compliance with general data processing principles
	Art. 5 GDPR, Art. 13 GDPR, Art. 114 Codice della privacy	Insufficient fulfilment of information obligations
	Art. 5 GDPR, Art. 25 GDPR	Non-compliance with general data processing principles
	Art. 5 GDPR, Art. 25 GDPR, Art. 32 GDPR, Art. 37 GDPR	Insufficient TOMs to ensure information security
	Art. 5 GDPR, Art. 6 GDPR	Insufficient legal basis for data processing
	Art. 5 GDPR, Art. 6 GDPR, Art. 12 GDPR, Art. 13 GDPR, Art. 15 GDPR, Art. 17 GDPR	Insufficient legal basis for data processing
	Art. 5 GDPR, Art. 6 GDPR, Art. 12 GDPR, Art. 15 GDPR, Art. 37 GDPR, Art. 2-ter Codice della privacy	Insufficient legal basis for data processing

	Art. 5 GDPR, Art. 6 GDPR, Art. 12 GDPR, Art. 24 GDPR, Art. 25 GDPR	Insufficient legal basis for data processing
	Art. 5 GDPR, Art. 6 GDPR, Art. 17 GDPR	Insufficient legal basis for data processing
	Art. 5 GDPR, Art. 6 GDPR, Art. 17 GDPR, Art. 21 GDPR	Insufficient legal basis for data processing
	Art. 5 GDPR, Art. 6 GDPR, Art. 17 GDPR, Art. 21 GDPR, Art. 32 GDPR	Insufficient legal basis for data processing
	Art. 5 GDPR, Art. 6 GDPR, Art. 24 GDPR, Art. 25 GDPR	Insufficient legal basis for data processing
	Art. 5 GDPR, Art. 6 GDPR, Art. 28 GDPR, Art. 32 GDPR	Insufficient TOMs to ensure information security
	Art. 5 GDPR, Art. 6 GDPR, Art. 2-ter Codice della privacy	Insufficient legal basis for data processing
	Art. 5 GDPR, Art. 6 GDPR, Art. 30 GDPR	Non-compliance with general data processing principles
	Art. 5 GDPR, Art. 6 GDPR, Art. 30 GDPR, Art. 32 GDPR	Non-compliance with general data processing principles
	Art. 5 GDPR, Art. 6 GDPR, Art. 7 GDPR	Insufficient legal basis for data processing
	Art. 5 GDPR, Art. 6 GDPR, Art. 7 GDPR, Art. 12 GDPR, Art. 13 GDPR, Art. 21 GDPR, Art. 24 GDPR, Art. 25 GDPR, Art. 32 GDPR, Art. 33 (1) GDPR, Art. 34 (1) GDPR	Non-compliance with general data processing principles
	Art. 5 GDPR, Art. 6 GDPR, Art. 7 GDPR, Art. 28 GDPR, Art. 29 GDPR	Insufficient legal basis for data processing
	Art. 5 GDPR, Art. 6 GDPR, Art. 9 GDPR	Insufficient legal basis for data processing
	Art. 5 GDPR, Art. 6 GDPR, Art. 9 GDPR, Art. 2-ter Codice della privacy, Art. 2-sexies Codice della privacy, Art. 2-septies (8) Codice della privacy	Insufficient legal basis for data processing
	Art. 5 GDPR, Art. 6 GDPR, Art. 9 GDPR, Art. 2-ter Codice della privacy, Art. 2-sexies Codice della privacy	Insufficient legal basis for data processing
	Art. 5 GDPR, Art. 9 GDPR	Insufficient legal basis for data processing
		Non-compliance with general data processing principles
	Art. 5 GDPR, Art. 9 GDPR, Art. 12 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 58 (2) GDPR	Insufficient cooperation with supervisory authority
	Art. 6 (1) GDPR, Art. 7 (1) GDPR, Art. 30 GDPR, Art. 31 GDPR	Insufficient legal basis for data processing
	Art. 6 GDPR, Art. 7 GDPR, Art. 15 GDPR, Art. 17 GDPR, Art. 21 GDPR, Art. 130 (3) Codice della privacy, Art. 157 Codice della privacy, Art. 166 (2) Codice della privacy	Insufficient legal basis for data processing
	Art. 9 GDPR	Insufficient legal basis for data processing
ITALY (ENDS)		
LATVIA	Art. 13 GDPR	Insufficient fulfilment of information obligations
	Art. 17 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 5 GDPR, Art. 6 GDPR	Insufficient legal basis for data processing
	Art. 6 (1) GDPR	Insufficient legal basis for data processing
	Art. 6 GDPR	Insufficient legal basis for data processing
LATVIA (ENDS)		
LIECHTENSTEIN	Unknown	Non-compliance with general data processing principles
LIECHTENSTEIN (ENDS)		

LITHUANIA	Art. 32 (1) b), c) GDPR	Insufficient TOMs to ensure information security
	Art. 32 (1) b), d) GDPR	Insufficient TOMs to ensure information security
	Art. 5 (1) a), c) GDPR, Art. 9 (1) GDPR, Art. 13 (1), (2) GDPR, Art. 30 GDPR, Art. 35 (1) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) d) GDPR, Art. 5 (1) f) GDPR	Non-compliance with general data processing principles
	Art. 5 (1), (2) GDPR, Art. 13 GDPR, Art. 24 GDPR, Art. 32 GDPR, Art. 35 GDPR, Art. 58 (2) f) GDPR	Non-compliance with general data processing principles
	Art. 5 GDPR, Art. 13 GDPR, Art. 24 GDPR, Art. 35 GDPR	Non-compliance with general data processing principles
	Art. 5 GDPR, Art. 32 GDPR, Art. 33 GDPR	Insufficient fulfilment of data breach notification obligations
LITHUANIA (ENDS)		
LUXEMBOURG	Art. 37 (7) GDPR, Art. 38 (1), (2) GDPR, Art. 39 (1) b) GDPR	Insufficient involvement of data protection officer
	Art. 38 (1) GDPR, Art. 39 (1) b) GDPR	Insufficient involvement of data protection officer
	Art. 38 (1), (2) GDPR, Art. 39 (1) a) GDPR	Insufficient involvement of data protection officer
	Art. 38 (1), (3) GDPR, Art. 39 (1) a), b) GDPR	Insufficient involvement of data protection officer
	Art. 5 (1) a) GDPR, Art. 12 (1), (7) GDPR, Art. 13 GDPR	Insufficient fulfilment of information obligations
	Art. 5 (1) c) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) c) GDPR, Art. 13 GDPR	Non-compliance with general data processing principles
	Art. 5 (1) c), e) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) c), e) GDPR, Art. 13 GDPR, Art. 32 (1) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) e) GDPR, Art. 13 GDPR	Non-compliance with general data processing principles
	Art. 5 (1) f) GDPR, Art. 32 (1) a), b) GDPR, Art. 33 (1), (5) GDPR	Insufficient TOMs to ensure information security
	Unknown	Non-compliance with general data processing principles
LUXEMBOURG (ENDS)		
MALTA	Art. 5 (1) f) GDPR, Art. 6 (1) GDPR, Art. 9 (1), (2) GDPR, Art. 14 GDPR, Art. 32 GDPR, Art. 33 GDPR, Art. 34 GDPR	Insufficient TOMs to ensure information security
	Art. 5 GDPR, Art. 32 GDPR	Insufficient TOMs to ensure information security
MALTA (ENDS)		
NORWAY	Art. 24 GDPR, Art. 32 (1), (2) GDPR	Insufficient TOMs to ensure information security
	Art. 32 (1) b) GDPR, Art. 24 (1) GDPR, Art. 35 GDPR	Insufficient TOMs to ensure information security
	Art. 32 (1) b), (2) GDPR	Insufficient TOMs to ensure information security
	Art. 32 (1) b), d) GDPR	Insufficient TOMs to ensure information security
	Art. 32 GDPR	Insufficient TOMs to ensure information security
	Art. 32 GDPR, Art. 35 GDPR	Insufficient TOMs to ensure information security
	Art. 5 (1) a) GDPR, Art. 6 (1) GDPR	Insufficient legal basis for data processing
	Art. 5 (1) a) GDPR, Art. 6 GDPR	Insufficient legal basis for data processing
	Art. 5 (1) a) GDPR, Art. 6 (1) GDPR	Insufficient legal basis for data processing
	Art. 5 (1) c), e) GDPR, Art. 6 (1) GDPR, Art. 9 (2) GDPR	Insufficient legal basis for data processing

	Art. 5 (1) f) GDPR, Art. 32 (1) b), d) GDPR	Insufficient TOMs to ensure information security
	Art. 5 (1) f) GDPR, Art. 32 GDPR	Insufficient TOMs to ensure information security
	Art. 5 (1) f) GDPR, Art. 5 (2) GDPR, Art. 28 (3) GDPR, Art. 32 (2) GDPR, Art. 44 GDPR	Non-compliance with general data processing principles
	Art. 5 (1) GDPR, Art. 6 (1) GDPR	Insufficient legal basis for data processing
	Art. 5 (1), (2) GDPR, Art. 6 GDPR, Art. 12 GDPR, Art. 13 GDPR	Insufficient legal basis for data processing
	Art. 5 GDPR, Art. 6 GDPR	Insufficient legal basis for data processing
	Art. 5 GDPR, Art. 6 GDPR, Art. 13 GDPR	Insufficient legal basis for data processing
	Art. 5 GDPR, Art. 6 GDPR, Art. 13 GDPR, Art. 17 GDPR, Art. 21 GDPR	Insufficient legal basis for data processing
	Art. 5 GDPR, Art. 6 GDPR, Art. 32 (1) b) GDPR	Insufficient TOMs to ensure information security
	Art. 5 GDPR, Art. 6 GDPR, Art. 32 (1) b) GDPR, Art. 24 GDPR	Insufficient TOMs to ensure information security
	Art. 5 GDPR, Art. 6 GDPR	Insufficient legal basis for data processing
	Art. 6 (1) e) GDPR	Insufficient legal basis for data processing
	Art. 6 (1) f) GDPR	Insufficient legal basis for data processing
	Art. 6 (1) GDPR	Insufficient legal basis for data processing
	Art. 6 (1) GDPR, Art. 13 GDPR, Art. 21 GDPR	Insufficient legal basis for data processing
	Art. 6 (1) GDPR, Art. 9 (1) GDPR	Insufficient legal basis for data processing
	Art. 6 GDPR	Insufficient legal basis for data processing
	Art. 6 GDPR, Art. 32 (1) b) GDPR	Insufficient TOMs to ensure information security
	Unknown	Unknown
NORWAY (ENDS)		
POLAND	Art. 14 GDPR	Insufficient fulfilment of information obligations
	Art. 24 (1) GDPR, Art. 32 (1), (2) GDPR, Art. 34 (1) GDPR	Insufficient TOMs to ensure information security
	Art. 28 (1), (3), (9) GDPR	Insufficient data processing agreement
	Art. 28 (3) c), f) GDPR, Art. 32 (1), (2) GDPR	Insufficient TOMs to ensure information security
	Art. 28 GDPR	Insufficient data processing agreement
	Art. 31 GDPR, Art. 58 (1) a) GDPR	Insufficient cooperation with supervisory authority
	Art. 31 GDPR, Art. 58 (1) a), e) GDPR	Insufficient cooperation with supervisory authority
	Art. 31 GDPR, Art. 58 (1) e) GDPR	Insufficient cooperation with supervisory authority
	Art. 31 GDPR, Art. 58 GDPR	Insufficient cooperation with supervisory authority
	Art. 32 GDPR	Insufficient TOMs to ensure information security
	Art. 33 (1) GDPR	Insufficient fulfilment of data breach notification obligations
	Art. 33 (1) GDPR, Art. 34 (1) GDPR	Insufficient fulfilment of data breach notification obligations
	Art. 33 GDPR	Insufficient fulfilment of data breach notification obligations
	Art. 33 GDPR, Art. 34 GDPR	Insufficient fulfilment of data breach notification obligations
	Art. 34 (1) GDPR	Insufficient fulfilment of data breach notification obligations
	Art. 34 (1), (2) GDPR, Art. 58 (2) e) GDPR	Insufficient fulfilment of data breach notification obligations

	Art. 5 (1) a) GDPR, Art. 6 GDPR	Insufficient legal basis for data processing
	Art. 5 (1) a), f) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) f) GDPR, Art. 24 (1) GDPR, Art. 25 (1) GDPR, Art. 28 (1) GDPR, Art. 32 (1), (2) GDPR	Insufficient TOMs to ensure information security
	Art. 5 (1) f) GDPR, Art. 25 (1) GDPR, Art. 28 (3) GDPR, Art. 32 (1), (2) GDPR	Insufficient TOMs to ensure information security
	Art. 5 (1) f) GDPR, Art. 25 (1) GDPR, Art. 32 (1) b), d), (2) GDPR	Insufficient TOMs to ensure information security
	Art. 5 (1) f) GDPR, Art. 5 (2) GDPR, Art. 24 (1) GDPR, Art. 25 (1) GDPR, Art. 32 (1), (2) GDPR	Insufficient TOMs to ensure information security
	Art. 5 (1) f) GDPR, Art. 5 (2) GDPR, Art. 25 (1) GDPR, Art. 32 (1), (2) GDPR	Insufficient TOMs to ensure information security
	Art. 5 (1) f), (2) GDPR, Art. 25 (1) GDPR, Art. 32 (1) b), d), (2) GDPR	Insufficient TOMs to ensure information security
	Art. 5 GDPR	Non-compliance with general data processing principles
	Art. 5 GDPR, Art. 6 GDPR	Insufficient legal basis for data processing
	Art. 5 GDPR, Art. 9 GDPR	Insufficient legal basis for data processing
	Art. 6 GDPR	Insufficient legal basis for data processing
POLAND (ENDS)		
PORTUGAL	Art. 13 GDPR	Insufficient fulfilment of information obligations
	Art. 15 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 5 (1) a) GDPR, Art. 9 (1) GDPR, Art. 12 GDPR, Art. 13 GDPR, Art. 28 (1), (6), (7) GDPR, Art. 35 (1), (2), (3) b) GDPR, Art. 44 GDPR, Art. 46 (2) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) a), c), e) GDPR, Art. 6 GDPR, Art. 9 (1) a) GDPR, Art. 13 (1), (2) GDPR, Art. 35 (3) GDPR	Insufficient legal basis for data processing
	Art. 5 (1) e), f) GDPR, Art. 13 (1), (2) GDPR, Art. 37 (1), (7) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) f) GDPR, Art. 32 GDPR	Insufficient TOMs to ensure information security
PORTUGAL (ENDS)		
ROMANIA	Art. 12 (1) GDPR, Art. 58 (1) a), e) GDPR	Insufficient fulfilment of data subjects' rights
	Art. 12 (3) GDPR	Insufficient fulfilment of data subjects' rights
	Art. 12 GDPR, Art. 13 GDPR, Art. 21 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 12 GDPR, Art. 13 GDPR, Art. 5 (1) c) GDPR, Art. 6 GDPR	Insufficient fulfilment of information obligations
	Art. 12 GDPR, Art. 15 GDPR, Art. 17 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 12 GDPR, Art. 17 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 15 (3) GDPR	Insufficient fulfilment of data subjects' rights
	Art. 15 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 15 GDPR, Art. 6 GDPR, Art. 32 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 17 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 21 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 24 GDPR, Art. 32 (1) d) GDPR	Insufficient TOMs to ensure information security

	Art. 25 (1) GDPR, Art. 32 (1) b) GDPR, Art. 32 (2) GDPR	Insufficient TOMs to ensure information security
	Art. 25 (1) GDPR, Art. 32 (1) b), d), e) GDPR	Insufficient TOMs to ensure information security
	Art. 25 (1) GDPR, Art. 32 (1), (2) GDPR	Insufficient TOMs to ensure information security
	Art. 25 (1) GDPR, Art. 32 (1), (2), (4) GDPR	Insufficient TOMs to ensure information security
	Art. 25 (1) GDPR, Art. 5 (1) c) GDPR	Insufficient TOMs to ensure information security
	Art. 28 (1) GDPR, Art. 32 GDPR, Art. 33 GDPR	Insufficient TOMs to ensure information security
	Art. 28 (2) GDPR	Insufficient data processing agreement
	Art. 28 (3) a) GDPR	Insufficient data processing agreement
	Art. 29 GDPR, Art. 32 (1) b) GDPR, Art. 32 (2), (4) GDPR	Insufficient TOMs to ensure information security
	Art. 29 GDPR, Art. 32 (1) b) GDPR, Art. 32 (4) GDPR	Insufficient TOMs to ensure information security
	Art. 29 GDPR, Art. 32 (2), (4) GDPR	Insufficient TOMs to ensure information security
	Art. 29 GDPR, Art. 32 (4) GDPR	Insufficient TOMs to ensure information security
	Art. 31 GDPR, Art. 58 GDPR	Insufficient cooperation with supervisory authority
	Art. 32 (1) b) GDPR	Insufficient TOMs to ensure information security
	Art. 32 (1) b) GDPR, Art. 32 (2) GDPR	Insufficient TOMs to ensure information security
	Art. 32 (1) b) GDPR, Art. 32 (2) GDPR, Art. 3 (1) Law No. 506/2004, Art. 3 (3) a), b) Law No. 506/2004	Insufficient TOMs to ensure information security
	Art. 32 (1) b) GDPR, Art. 32 (2) GDPR, Art. 32 (4) GDPR	Insufficient TOMs to ensure information security
	Art. 32 (1) b), (2) GDPR	Insufficient TOMs to ensure information security
	Art. 32 (1) b), (2) GDPR, Art. 58 (1) a), e) GDPR	Insufficient TOMs to ensure information security
	Art. 32 (1) b), (2), (4) GDPR	Insufficient TOMs to ensure information security
	Art. 32 (1) b), c) GDPR, Art. 32 (2) GDPR	Insufficient TOMs to ensure information security
	Art. 32 (1), (2) GDPR	Insufficient TOMs to ensure information security
	Art. 32 (1), (2) GDPR, Art. 58 (1) a), e) GDPR	Insufficient TOMs to ensure information security
	Art. 32 (1), (2), (4) GDPR	Insufficient TOMs to ensure information security
	Art. 32 (4) GDPR	Insufficient TOMs to ensure information security
	Art. 32 GDPR	Insufficient TOMs to ensure information security
	Art. 32 GDPR, Art. 33 GDPR	Insufficient TOMs to ensure information security
	Art. 5 (1) a) - d) GDPR, Art. 6 (1) GDPR	Insufficient legal basis for data processing
	Art. 5 (1) a) GDPR, Art. 5 (2) GDPR, Art. 6 GDPR	Insufficient legal basis for data processing
	Art. 5 (1) a) GDPR, Art. 6 (1) a) GDPR	Insufficient legal basis for data processing
	Art. 5 (1) a), b), (2) GDPR, Art. 6 (1) GDPR, Art. 13 (1), (2), (3) GDPR, Art. 32 (2) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) a), b), (2) GDPR, Art. 6 (1) GDPR, Art. 14 (1), (4) GDPR	Insufficient legal basis for data processing
	Art. 5 (1) a), b), c), f) GDPR, Art. 5 (2) GDPR, Art. 6 GDPR	Insufficient legal basis for data processing
	Art. 5 (1) a), c), e) GDPR, Art. 5 (2) GDPR, Art. 6 GDPR	Insufficient legal basis for data processing

	Art. 5 (1) a), d), (2) GDPR, Art. 6 GDPR	Insufficient legal basis for data processing
	Art. 5 (1) a), f) GDPR, Art. 6 (1) a) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) b), c) GDPR, Art. 5 (2) GDPR, Art. 6 GDPR	Non-compliance with general data processing principles
	Art. 5 (1) b), c) GDPR, Art. 5 (2) GDPR, Art. 6 GDPR, Art. 7 GDPR	Insufficient legal basis for data processing
	Art. 5 (1) d) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) d), f) GDPR, Art. 5 (2) GDPR, Art. 17 GDPR	Non-compliance with general data processing principles
	Art. 5 (1) e) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) f) GDPR, Art. 32 (1), (2) GDPR	Insufficient TOMs to ensure information security
	Art. 5 (1) f) GDPR, Art. 32 GDPR	Insufficient TOMs to ensure information security
	Art. 5 (1) GDPR, Art. 6 GDPR, Art. 7 GDPR	Non-compliance with general data processing principles
	Art. 5 (1) GDPR, Art. 6 GDPR, Art. 7 GDPR, Art. 9 GDPR	Non-compliance with general data processing principles
	Art. 5 GDPR, Art. 25 GDPR, Art. 32 GDPR, Art. 33 GDPR	Insufficient TOMs to ensure information security
	Art. 5 GDPR, Art. 6 GDPR	Insufficient legal basis for data processing
	Art. 5 GDPR, Art. 6 GDPR, Art. 12 GDPR, Art. 13 GDPR, Art. 25 GDPR, Art. 32 GDPR	Insufficient legal basis for data processing
	Art. 5 GDPR, Art. 6 GDPR, Art. 7 GDPR, Art. 21 GDPR	Insufficient legal basis for data processing
	Art. 5 GDPR, Art. 6 GDPR, Art. 9 GDPR, Art. 33 GDPR	Insufficient legal basis for data processing
	Art. 58 (1) a), e) GDPR	Insufficient cooperation with supervisory authority
	Art. 58 (1) a), e) GDPR, Art. 58 (2) i) GDPR	Insufficient cooperation with supervisory authority
	Art. 58 (1) GDPR	Insufficient cooperation with supervisory authority
	Art. 58 GDPR	Insufficient cooperation with supervisory authority
	Art. 6 (1) a) GDPR	Insufficient legal basis for data processing
	Art. 6 GDPR, Art. 21 GDPR	Insufficient fulfilment of data subjects' rights
		Insufficient legal basis for data processing
	Art. 6 GDPR, Art. 7 GDPR, Art. 9 GDPR	Insufficient legal basis for data processing
	Art. 6 GDPR, Art. 9 GDPR	Insufficient legal basis for data processing
ROMANIA (ENDS)		
SLOVAKIA	Art. 15 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 31 GDPR	Insufficient cooperation with supervisory authority
	Art. 32 GDPR	Insufficient TOMs to ensure information security
	Art. 5 (1) a) GDPR, Art. 5 (2) GDPR, Art. 28 GDPR	Non-compliance with general data processing principles
	Art. 5 (1) a) GDPR, Art. 6 (1) a) GDPR	Insufficient legal basis for data processing
	Art. 5 (1) f) GDPR, Art. 32 GDPR	Insufficient TOMs to ensure information security
	Unknown	Unknown
SLOVAKIA (ENDS)		
SPAIN	Art. 12 GDPR, Art. 13 GDPR, Art. 14 GDPR	Insufficient fulfilment of information obligations

	Art. 13 (2) GDPR	Insufficient fulfilment of information obligations
	Art. 13 GDPR	Insufficient fulfilment of information obligations
	Art. 13 GDPR, Art. 14 GDPR	Insufficient fulfilment of information obligations
	Art. 13 GDPR, Art. 22 (2) LSSI	Insufficient fulfilment of information obligations
	Art. 13 GDPR, Art. 25 GDPR	Insufficient fulfilment of information obligations
	Art. 13 GDPR, Art. 30 GDPR	Insufficient fulfilment of information obligations
	Art. 13 GDPR, Art. 32 GDPR	Insufficient TOMs to ensure information security
	Art. 13 GDPR, Art. 8 (1) GDPR, Art. 6 (1) a) GDPR	Insufficient fulfilment of information obligations
	Art. 15 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 16 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 17 (1) GDPR, Art. 21 LSSI	Insufficient fulfilment of data subjects' rights
	Art. 17 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 17 GDPR, Art. 21 LSSI	Insufficient fulfilment of data subjects' rights
	Art. 21 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 21 GDPR, Art. 21 LSSI	Insufficient fulfilment of data subjects' rights
	Art. 28 (3) GDPR	Insufficient data processing agreement
	Art. 28 GDPR	Insufficient TOMs to ensure information security
	Art. 28 GDPR, Art. 24 GDPR, Art. 44 GDPR, Art. 21 LSSI, Art. 48 (1) b) LGT, Art. 21 GDPR, Art. 23 LOPDGDD	Insufficient fulfilment of data subjects' rights
	Art. 28 GDPR, Art. 48 (1) b) LGT	Insufficient fulfilment of data subjects' rights
	Art. 31 GDPR	Insufficient cooperation with supervisory authority
		Insufficient legal basis for data processing
	Art. 31 GDPR, Art. 58 GDPR	Insufficient cooperation with supervisory authority
	Art. 32 (1) GDPR	Insufficient TOMs to ensure information security
	Art. 32 (1) GDPR, Art. 33 GDPR	Insufficient TOMs to ensure information security
	Art. 32 GDPR	Insufficient TOMs to ensure information security
	Art. 33 GDPR	Insufficient fulfilment of data breach notification obligations
	Art. 35 GDPR	Non-compliance with general data processing principles
	Art. 37 GDPR	Insufficient involvement of data protection officer
	Art. 48 (1) b) LGT, Art. 21 GDPR, Art. 23 (4) LOPDGDD	Insufficient fulfilment of data subjects' rights
	Art. 48 (1) b) LGT, Art. 21 GDPR, Art. 23 LOPDGDD	Insufficient fulfilment of data subjects' rights
	Art. 48 (1) b) LGT, Art. 21 GDPR, Art. 23 LOPDGDD, Art. 28 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 5 (1) a) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) a) GDPR, Art. 6 (1) a) GDPR	Insufficient legal basis for data processing
	Art. 5 (1) a) GDPR, Art. 6 GDPR, Art. 12 GDPR, Art. 13 GDPR, Art. 21 (4) GDPR	Insufficient fulfilment of information obligations

	Art. 5 (1) a GDPR, Art. 7 (3) GDPR	Insufficient fulfilment of information obligations
	Art. 5 (1) a GDPR, Art. 6 GDPR	Insufficient legal basis for data processing
	Art. 5 (1) a, b), c), d) GDPR, Art. 6 (1) GDPR, Art. 14 GDPR	Insufficient legal basis for data processing
	Art. 5 (1) a, b), e) GDPR, Art. 6 (1) GDPR, Art. 8 GDPR, Art. 12 (1), (2) GDPR, Art. 13 GDPR, Art. 25 GDPR, Art. 30 (1) GDPR, Art. 22 (2) LSSI	Non-compliance with general data processing principles
	Art. 5 (1) b) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) b) GDPR, Art. 5 (1) f) GDPR, Art. 32 GDPR	Non-compliance with general data processing principles
	Art. 5 (1) b), c) GDPR, Art. 6 (1) b) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) c) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) c) GDPR, Art. 12 GDPR	Non-compliance with general data processing principles
	Art. 5 (1) c) GDPR, Art. 12 GDPR, Art. 13 GDPR	Non-compliance with general data processing principles
	Art. 5 (1) c) GDPR, Art. 13 GDPR	Non-compliance with general data processing principles
	Art. 5 (1) c) GDPR, Art. 58 (2) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) c) GDPR, Art. 6 GDPR	Non-compliance with general data processing principles
	Art. 5 (1) c) GDPR, Art. 6 GDPR, Art. 9 GDPR, Art. 12 GDPR, Art. 13 GDPR, Art. 25 (1) GDPR, Art. 35 GDPR	Insufficient legal basis for data processing
	Art. 5 (1) c), e) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) d) GDPR	Insufficient fulfilment of data subjects' rights
		Non-compliance with general data processing principles
	Art. 5 (1) d) GDPR, Art. 17 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 5 (1) d), f) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) d), f) GDPR Total	
	Art. 5 (1) e) GDPR, Art. 6 GDPR, Art. 32 (1) b), d) GDPR	Insufficient legal basis for data processing
	Art. 5 (1) f) GDPR	Insufficient legal basis for data processing
		Insufficient TOMs to ensure information security
		Non-compliance with general data processing principles
	Art. 5 (1) f) GDPR, Art. 17 GDPR, Art. 32 GDPR	Insufficient TOMs to ensure information security
	Art. 5 (1) f) GDPR, Art. 32 (1) GDPR	Insufficient TOMs to ensure information security
		Non-compliance with general data processing principles
	Art. 5 (1) f) GDPR, Art. 32 GDPR	Insufficient TOMs to ensure information security
		Non-compliance with general data processing principles
	Art. 5 (1) f) GDPR, Art. 32 GDPR, Art. 21 LSSI	Insufficient TOMs to ensure information security
	Art. 5 (1) f) GDPR, Art. 32 GDPR, Art. 33 GDPR	Insufficient TOMs to ensure information security
	Art. 5 (1) f) GDPR, Art. 5 (2) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) f) GDPR, Art. 6 (1) a) GDPR	Insufficient legal basis for data processing

	Art. 5 GDPR	Non-compliance with general data processing principles
	Art. 5 GDPR, Art. 13 GDPR, Art. 14 GDPR	Non-compliance with general data processing principles
	Art. 5 GDPR, Art. 32 GDPR	Insufficient TOMs to ensure information security
	Art. 5 GDPR, Art. 6 GDPR	Insufficient legal basis for data processing
	Art. 5 GDPR, Art. 6 GDPR, Art. 13 GDPR, Art. 14 GDPR	Non-compliance with general data processing principles
	Art. 5 GDPR, Art. 6 GDPR, Art. 21 GDPR	Insufficient legal basis for data processing
	Art. 5 GDPR, Art. 6 GDPR, Art. 28 (3) g) GDPR	Insufficient legal basis for data processing
	Art. 5 GDPR, Art. 6 GDPR	Insufficient legal basis for data processing
	Art. 58 (1) GDPR	Insufficient cooperation with supervisory authority
	Art. 58 (1) GDPR	Insufficient cooperation with supervisory authority
	Art. 58 (2) GDPR	Insufficient cooperation with supervisory authority
	Art. 58 GDPR	Insufficient cooperation with supervisory authority
	Art. 6 (1) a) GDPR	Insufficient legal basis for data processing
	Art. 6 (1) b) GDPR	Insufficient legal basis for data processing
	Art. 6 (1) e) GDPR, Art. 13 GDPR	Insufficient legal basis for data processing
	Art. 6 (1) f) GDPR	Insufficient legal basis for data processing
	Art. 6 (1) GDPR	Insufficient legal basis for data processing
	Art. 6 (1) GDPR, Art. 10 GDPR, Art. 10 LOPDGDD	Insufficient legal basis for data processing
	Art. 6 (1) GDPR, Art. 13 GDPR	Insufficient legal basis for data processing
	Art. 6 (1) GDPR, Art. 13 GDPR, Art. 21 GDPR	Insufficient legal basis for data processing
	Art. 6 (1) GDPR, Art. 13 GDPR, Art. 22 (2) LSSI	Insufficient fulfilment of information obligations
	Art. 6 (1) GDPR, Art. 13 GDPR, Art. 14 GDPR	Insufficient fulfilment of information obligations
	Art. 6 (1) GDPR, Art. 15 GDPR	Insufficient legal basis for data processing
	Art. 6 (1) GDPR, Art. 17 GDPR	Insufficient legal basis for data processing
	Art. 6 GDPR	Insufficient legal basis for data processing
	Art. 6 GDPR, Art. 12 GDPR, Art. 15 GDPR	Insufficient legal basis for data processing
	Art. 6 GDPR, Art. 13 GDPR	Insufficient fulfilment of information obligations
		Insufficient legal basis for data processing
	Art. 6 GDPR, Art. 13 GDPR, Art. 14 GDPR	Insufficient legal basis for data processing
	Art. 6 GDPR, Art. 17 GDPR	Insufficient legal basis for data processing
	Art. 6 GDPR, Art. 17 GDPR, Art. 28 GDPR	Insufficient legal basis for data processing
	Art. 6 GDPR, Art. 32 GDPR	Insufficient legal basis for data processing
	Art. 6 GDPR, Art. 7 GDPR	Insufficient legal basis for data processing
	Art. 6 GDPR, Art. 9 GDPR	Insufficient legal basis for data processing

	Art. 7 GDPR	Insufficient legal basis for data processing
	Art. 7 GDPR, Art. 12 GDPR, Art. 13 GDPR	Insufficient fulfilment of information obligations
	Art. 7 GDPR, Art. 13 GDPR	Insufficient fulfilment of information obligations
	Art. 9 (2) a) GDPR, Art. 13 GDPR	Insufficient legal basis for data processing
	Art. 6 GDPR	Insufficient legal basis for data processing
SPAIN (ENDS)		
SWEDEN	Art. 32 (1) GDPR	Insufficient TOMs to ensure information security
	Art. 32 GDPR	Insufficient TOMs to ensure information security
	Art. 33 GDPR, Art. 34 GDPR	Insufficient fulfilment of data breach notification obligations
	Art. 5 (1) a) GDPR, Art. 13 GDPR	Insufficient fulfilment of information obligations
	Art. 5 (1) a) GDPR, Art. 13 GDPR, Art. 14 GDPR	Insufficient fulfilment of information obligations
	Art. 5 (1) a) GDPR, Art. 5 (2) GDPR, Art. 12 (1) GDPR, Art. 13 (2) f) GDPR, Art. 14 (2) g) GDPR	Insufficient fulfilment of information obligations
	Art. 5 (1) a), c) GDPR, Art. 32 (1), (4) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) a), c) GDPR, Art. 6 (1) f) GDPR, Art. 13 GDPR	Insufficient legal basis for data processing
	Art. 5 (1) a), f) GDPR, Art. 6 GDPR, Art. 9 (1) GDPR, Art. 13 GDPR, Art. 32 GDPR	Non-compliance with general data processing principles
	Art. 5 (1) c) GDPR, Art. 9 GDPR, Art. 35 GDPR, Art. 36 GDPR	Insufficient legal basis for data processing
	Art. 5 (1) f) GDPR, Art. 32 (1), (2) GDPR	Insufficient TOMs to ensure information security
	Art. 5 (1) f) GDPR, Art. 5 (2) GDPR, Art. 32 (1) GDPR, Art. 32 (2) GDPR	Insufficient TOMs to ensure information security
	Art. 5 (1) f) GDPR, Art. 32 (1) GDPR	Insufficient TOMs to ensure information security
	Art. 5 (1) f) GDPR, Art. 5 (2) GDPR, Art. 32 (1) GDPR, Art. 32 (2) GDPR	Insufficient TOMs to ensure information security
	Art. 5 GDPR, Art. 6 (1) f) GDPR	Insufficient legal basis for data processing
	Art. 5 GDPR, Art. 32 GDPR	Insufficient TOMs to ensure information security
	Art. 5 GDPR, Art. 6 GDPR	Insufficient legal basis for data processing
		Non-compliance with general data processing principles
	Art. 5 GDPR, Art. 6 GDPR, Art. 13 GDPR, Art. 35 GDPR, Art. 36 GDPR	Insufficient legal basis for data processing
	Art. 5 GDPR, Art. 6 GDPR, Art. 17 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 6 GDPR	Insufficient legal basis for data processing
SWEDEN (ENDS)		
THE NETHERLANDS	Art. 12 (2) GDPR	Insufficient fulfilment of data subjects' rights
	Art. 12 GDPR	Insufficient fulfilment of information obligations
	Art. 12 GDPR, Art. 15 GDPR	Insufficient fulfilment of data subjects' rights
	Art. 13 (1) e) GDPR, Art. 32 (1) GDPR	Insufficient TOMs to ensure information security
	Art. 27 GDPR	Non-compliance with general data processing principles

	Art. 32 (1) GDPR	Insufficient TOMs to ensure information security
	Art. 32 (1), (2) GDPR	Insufficient TOMs to ensure information security
	Art. 32 GDPR	Insufficient TOMs to ensure information security
	Art. 33 GDPR	Insufficient fulfilment of data breach notification obligations
	Art. 5 (1) a) GDPR, Art. 6 (1) e) GDPR, Art. 8 Wbp	Insufficient legal basis for data processing
	Art. 5 (1) a) GDPR, Art. 6 (1) GDPR	Insufficient legal basis for data processing
	Art. 5 (1) a), b), d), e) GDPR, Art. 6 (1) GDPR, Art. 32 (1) GDPR, Art. 35 (2) GDPR	Non-compliance with general data processing principles
	Art. 5 GDPR	Non-compliance with general data processing principles
	Art. 5 GDPR, Art. 6 GDPR	Insufficient legal basis for data processing
	Art. 5 GDPR, Art. 9 GDPR	Insufficient legal basis for data processing
	Art. 9 GDPR, Art. 32 GDPR	Insufficient TOMs to ensure information security
THE NETHERLANDS (ENDS)		
UNITED KINGDOM	Art. 32 GDPR	Insufficient TOMs to ensure information security
	Art. 5 (1) a) f) GDPR	Non-compliance with general data processing principles
	Art. 5 (1) a) GDPR, Art. 6 GDPR, Art. 9 GDPR, Art. 13 (1) c) GDPR, Regulation 21 PECR	Insufficient legal basis for data processing
	Art. 5 (1) a), e) GDPR, Art. 6 GDPR, Art. 9 GDPR, Art. 14 GDPR, Art. 15 GDPR, Art. 16 GDPR, Art. 17 GDPR, Art. 21 GDPR, Art. 22 GDPR, Art. 35 GDPR	Non-compliance with general data processing principles
	Art. 5 (1) f) GDPR, Art. 32 (1), (2) GDPR	Insufficient TOMs to ensure information security
	Art. 5 (1) f) GDPR, Art. 32 GDPR	Insufficient TOMs to ensure information security
	Art. 5 (1) f) GDPR, Art. 32 GDPR Total	
UNITED KINGDOM (ENDS)		

Annex 3 - Supervisory authorities – list of public data sources

The following supervisory authorities were contacted for the purposes of this research, though not all provided information. Most regulators' websites include a public page detailing fines issued and decisions.

Austria

Österreichische Datenschutzbehörde
<http://www.dsb.gv.at/>

Belgium

Commission de la protection de la vie privée
<http://www.privacycommission.be/>

Bulgaria

Commission for Personal Data Protection
<http://www.cdpd.bg/>

Croatia

Croatian Personal Data Protection Agency
<http://www.azop.hr/>

Cyprus

Commissioner for Personal Data Protection
<http://www.dataprotection.gov.cy/>

Czech Republic

The Office for Personal Data Protection
<http://www.uoou.cz/>

Denmark

Datatilsynet
<http://www.datatilsynet.dk/>

Estonia

Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon)
<http://www.aki.ee/en>

Finland

Office of the Data Protection Ombudsman
<http://www.tietosuoja.fi/en/>

France

Commission Nationale de l'Informatique et des Libertés – CNIL
<http://www.cnil.fr/>

Germany

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
<http://www.bfdi.bund.de/>

Greece

Hellenic Data Protection Authority
<http://www.dpa.gr/>

Hungary

National Authority for Data Protection and Freedom of Information
<http://www.naih.hu/>

Ireland

Data Protection Commissioner
<http://www.dataprotection.ie/>

Italy

Garante per la protezione dei dati personali
<http://www.garanteprivacy.it/>

Latvia

Data State Inspectorate
<http://www.dvi.gov.lv/>

Lithuania

State Data Protection
<http://www.ada.lt/>

Luxembourg

Commission Nationale pour la Protection des Données
<http://www.cnpd.lu/>

Malta

Office of the Data Protection Commissioner
<http://www.dataprotection.gov.mt/>

Netherlands

Autoriteit Persoonsgegevens
Prins Clauslaan 60
<https://autoriteitpersoonsgegevens.nl/nl>

Poland

The Bureau of the Inspector General for the Protection of Personal Data – GIODO
<http://www.giodo.gov.pl/>

Portugal

Comissão Nacional de Protecção de Dados – CNPD
<http://www.cnpd.pt/>

Romania

The National supervisory authority for Personal Data Processing
<http://www.dataprotection.ro/>

Slovakia

Office for Personal Data Protection of the Slovak Republic
<http://www.dataprotection.gov.sk/>

Slovenia

Information Commissioner
<https://www.ip-rs.si/>

Spain

Agencia de Protección de Datos
<https://www.agpd.es/>

Sweden

Datainspektionen
<http://www.datainspektionen.se/>

United Kingdom

The Information Commissioner's Office
<https://ico.org.uk>

Iceland

Icelandic Data Protection Agency
<https://www.personuvernd.is/>

Liechtenstein

Data Protection Office
<https://www.datenschutzstelle.li/>

Norway

Datatilsynet

<https://www.datatilsynet.no/>

Switzerland

Data Protection and Information Commissioner of Switzerland

<https://www.edoeb.admin.ch/edoeb/en/home.htm>

Annex 4 – URLs to decisions

record_id	URL to decision
1	https://www.dsb.gv.at/documents/22758/116802/Straferkenntnis+DSB-D550.038+0003-DSB+2018.pdf/fb0bb313-8651-44ac-a713-c286d83e3f19
2	https://www.dsb.gv.at/documents/22758/115212/Newsletter_DSB_1_2020.pdf/a640bbb8-9297-4230-86e4-163bc9ccb844
3	https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20180927_DSB_D550_084_0002_DSB_2018_00/DSBT_20180927_DS B_D550_084_0002_DSB_2018_00.pdf
4	https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20181220_DSB_D550_037_0003_DSB_2018_00/DSBT_20181220_DS B_D550_037_0003_DSB_2018_00.pdf
5	https://www.autoriteprotectiondonnees.be/news/lautorite-de-protection-des-donnees-prononce-une-sanction-dans-le-cadre-dune-campagne
6	https://gdprtoolkit.eu/first-gdpr-fine-in-bulgaria/ https://www.cdpd.bg/?p=element_view&aid=2152
7	https://www.cdpd.bg/?p=element_view&aid=2180
8	https://www.cdpd.bg/?p=element&aid=1195
9	https://www.cdpd.bg/?p=element_view&aid=2177
10	https://www.agplaw.com/cyprus-gdpr-commissioner-fines-newspaper-and-hospital/
11	https://www.agplaw.com/cyprus-gdpr-commissioner-fines-newspaper-and-hospital/
12	https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=34464
13	https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=34465
14	https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=34466
15	https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=34467
16	https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=34468
17	https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=34469
18	https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=34470
19	https://www.uoou.cz/kontrola-zpracovani-osobnich-udaju-bankou-unicredit-bank-czech-republic-and-slovakia-a-s/ds-5705/archiv=0&p1=5653
20	https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=34472
21	https://www.datatilsynet.dk/presse-og-nyheder/nyhedarkiv/2019/mar/datatilsynet-indstillertaxaselskab-til-boede-paa-1-2-mio-kr/
22	https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2019/jun/tilsyn-med-iddesigns-behandling-af-personoplysninger/
23	https://www.cnil.fr/en/cnil-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc
24	https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000038552658&fastReqId=119744754&fastPos=1
25	https://www.baden-wuerttemberg.datenschutz.de/ldi-baden-wuerttemberg-verhaengt-sein-erstes-bussgeld-in-deutschland-nach-der-ds-gvo/
26	https://www.heise.de/newsticker/meldung/DSGVO-5000-Euro-Bussgeld-fuer-fehlenden-Auftragsverarbeitungsvertrag-4282737.html https://kolibri-image.com/causa-datenschutz/
27	https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/07/PM-Datenschutzverletzungen-bereiten-zunehmend-Sorge-30.07.2019.pdf
28	https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/01/35.-T%C3%A4tigkeitsbericht-f%C3%BCr-den-Datenschutz-Web.pdf#page=44&zoom=100,0,0
29	Page 134 of the activity report of the Data Protection Commissioner of Hamburg, accessible under https://datenschutz-hamburg.de/assets/pdf/27_Taetigkeitsbericht_Datenschutz_2018_HmbBfDI.pdf
30	https://indd.adobe.com/view/d639298c-3165-4e30-85d8-0730de2a3598
31	https://www.pingdigital.de/blog/2019/03/29/implodierende-aufsichtsbehoerden/1626
32	Page 131 of the activity report of the Data Protection Commissioner of Berlin https://www.zaftda.de/tb-bundeslaender/berlin/695-tb-ldf-berlin-2018-ohne-drs-nr-vom-28-03-2019/file https://www.handelsblatt.com/finanzen/banken-versicherungen/datenspeicherung-schwarze-listen-so-bekam-n26-aerger-mit-datenschuetzern/24204544.html?ticket=ST-2292400-vgiEKfzmY6g2zEmLwLgj-ap1

33	http://www.cms-lawnow.com/ealerts/2019/03/hungary-fines-two-companies-for-gdpr-infringement?cc_lang=en https://www.naih.hu/files/NAIH-2019_363_hatarozat.pdf
34	http://www.cms-lawnow.com/ealerts/2019/03/hungary-fines-two-companies-for-gdpr-infringement?cc_lang=en https://www.naih.hu/files/NAIH-2019-1841_hatarozat.pdf
35	https://www.naih.hu/files/NAIH-2018-5559-H-hatarozat.pdf
36	https://www.naih.hu/files/NAIH-2019-596-hatarozat.pdf http://www.cms-lawnow.com/ealerts/2019/03/hungarys-data-protection-authority-levies-two-eur-3100-fines-for-privacy-violations?cc_lang=en
37	https://www.naih.hu/files/NAIH-2019-2526-2-H-hatarozat.pdf http://www.cms-lawnow.com/ealerts/2019/03/hungarys-data-protection-authority-levies-two-eur-3100-fines-for-privacy-violations?cc_lang=en
38	http://www.cms-lawnow.com/ealerts/2019/04/hungarian-data-authority-investigates-two-cases-of-privacy-breaches?cc_lang=en
39	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9101974
40	https://www.ada.lt/go.php/lit/lmones-atsakomybes-neisvengs--lietuvoje-skirta-zenkli-bauda-uz-bendrojo-duomenu-apsaugos-reglamento-pazeidimus-/1
41	https://www.gvzh.com.mt/malta-news/idpc-fines-lands-authority-data-breach/
42	https://www.datatilsynet.no/en/about-privacy/reports-on-specific-subjects/administrative-fine-of-170.000--imposed-on-bergen-municipality/
43	https://uodo.gov.pl/en/553/1009
44	https://uodo.gov.pl/pl/138/990 https://uodo.gov.pl/decyzje/ZSPR.440.43.2019
45	https://www.cnpd.pt/bin/decisoes/Delib/20_984_2018.pdf
46	https://www.aepd.es/resoluciones/PS-00331-2018_ORI.pdf
47	https://www.eldiario.es/tecnologia/Agencia-Proteccion-Datos-Liga-microfono_0_908859408.html#click=https://t.co/Rl3qZzucaB
48	https://www.aepd.es/resoluciones/PS-00121-2019_ORI.pdf
49	https://www.aepd.es/resoluciones/PS-00411-2018_ORI.pdf
50	https://www.baden-wuerttemberg.datenschutz.de/lfdi-baden-wuerttemberg-verhaengt-erstes-bussgeld-gegen-polizeibeamten/
51	https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000038629823&fastReqId=946473298&fastPos=1
52	http://www.naih.hu/files/NAIH-2019-167-hatarozat.pdf
53	http://www.naih.hu/files/NAIH_2019_133_hatarozat.pdf
54	https://www.cdpd.bg/?p=element_view&aid=2192
55	https://www.cdpd.bg/?p=element_view&aid=2191
56	https://www.aepd.es/resoluciones/PS-00074-2019_ORI.pdf
57	https://www.dataprotection.ro/?page=Comunicat_Amenda_Unicredit&lang=ro
58	https://ico.org.uk/action-weve-taken/enforcement/british-airways/
59	https://www.dataprotection.ro/index.jsp?page=O_noua_amenda_GDPR&lang=ro
60	https://ico.org.uk/media/action-weve-taken/mpns/2618524/marriott-international-inc-mpn-20201030.pdf
61	http://www.naih.hu/files/NAIH-2019-55_hatarozat.pdf
62	https://www.dataprotection.ro/?page=2019%20A%20treia%20amenda%20in%20aplicarea%20RGPD&lang=ro
63	https://autoriteitpersoonsgegevens.nl/nl/nieuws/haga-beboet-voor-onvoldoende-interne-beveiliging-pati%C3%ABntendossiers https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2021:3090
64	https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000038810992
65	https://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/DECISIONS/SUMMARY%20OF%20DECISION%2026_2019%20(EN).PDF
66	https://www.dataprotection.ro/?page=A_patra_amenda&lang=ro
67	https://www.datainspektionen.se/globalassets/dokument/beslut/facial-recognition-used-to-monitor-the-attendance-of-students.pdf
68	https://www.dsb.gv.at/dam/jcr:784483fa-dafb-49bd-8a09-412bb15eb9f9/Newsletter_DSB_4_2019.pdf https://www.ris.bka.gv.at/Dokumente/Bvwtg/BVWGT_20200312_W256_2223922_1_00.pdf
69	https://www.derstandard.at/story/2000107377808/fussballerinnen-nackt-gefilmt-mostviertler-trainer-muss-strafe-zahlen
70	https://www.aepd.es/resoluciones/PS-00159-2019_ORI.pdf
71	https://www.cdpd.bg/index.php?p=news_view&aid=1519

72	https://www.cdpd.bg/index.php?p=news_view&aid=1514
73	https://www.dvi.gov.lv/lv/zinas/datu-valsts-inspekcija-piemero-7000-eiro-lielu-naudas-sodu-internetveikalam-par-personas-datu-apstrades-parkapumiem/
74	https://www.naih.hu/files/NAIH-2019-2471-hatarozat.pdf
75	https://www.datatilsynet.no/contentassets/f7246f38ff394d32bef6895bc65a4b4f/varsel-om-gebyr---oslo-kommune.pdf
76	https://www.cnpd.pt/bin/decisoes/Delib/DEL_2019_21.pdf
77	https://www.cnpd.pt/bin/decisoes/Delib/DEL_2019_222.pdf
78	https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2019/20190919-PM-Bussgelder.pdf
79	https://uodo.gov.pl/decyzje/ZSPR.421.2.2019
80	https://www.sudinfo.be/id141981/Article/2019-09-19/un-commercant-recu-une-amende-de-10000-euros-pour-avoir-voulu-creer-une-carte-de
81	https://theword.iuslaboris.com/hrlaw/insights/spain-video-surveillance-and-data-protection-in-the-workplace
82	http://www.dpa.gr/APDPXPortlets/htdocs/documentSDisplay.jsp?docid=3,241,32,146,79,143,149,112
83	http://www.dpa.gr/APDPXPortlets/htdocs/documentSDisplay.jsp?docid=3,241,32,146,79,143,149,112
84	https://www.dataprotection.ro/?page=Comunicat_Presa_09_10_2019&lang=ro
85	https://www.dataprotection.ro/?page=Comunicat_Presa_09_10_2019&lang=ro
86	https://www.aepd.es/resoluciones/PS-00300-2019_ORI.pdf
87	https://cyprus-mail.com/2019/10/11/doctor-fined-e14000-for-violating-patient-data-on-instagram/
88	https://www.dataprotection.ro/?page=Alta_sanctiune_RGPD&lang=ro
89	https://www.dataprotection.gov.sk/uouu/sites/default/files/sprava_o_stave_ochrany_osobnych_udajov_za_obdobie_25.maj_2018_az_24_maj_2019.pdf
90	https://www.dataprotection.gov.sk/uouu/sites/default/files/sprava_o_stave_ochrany_osobnych_udajov_za_obdobie_25.maj_2018_az_24_maj_2019.pdf
91	https://www.dataprotection.gov.sk/uouu/sites/default/files/sprava_o_stave_ochrany_osobnych_udajov_za_obdobie_25.maj_2018_az_24_maj_2019.pdf
92	https://www.dataprotection.gov.sk/uouu/sites/default/files/sprava_o_stave_ochrany_osobnych_udajov_za_obdobie_25.maj_2018_az_24_maj_2019.pdf
93	https://www.aepd.es/resoluciones/PS-00262-2019_ORI.pdf
94	https://www.aepd.es/resoluciones/PS-00304-2019_ORI.pdf
95	https://www.etrend.sk/ekonomika/gdpr-zacina-hryzt-telekomunikacny-operator-dostal-pokutu-40-tisic-eur.html
96	https://wien.orf.at/stories/3019396/
97	https://uodo.gov.pl/decyzje/ZSPU.421.3.2019
98	https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2019/20191105-PM-Bussgeld_DW.pdf
99	https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2019/20191105-PM-Bussgeld_DW.pdf
100	https://www.aepd.es/resoluciones/PS-00301-2019_ORI.pdf
101	https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/07/PM-Datenschutzverletzungen-bereiten-zunehmend-Sorge-30.07.2019.pdf
102	https://uodo.gov.pl/decyzje/ZSPR.421.7.2019
103	https://www.aepd.es/resoluciones/PS-00268-2019_ORI.pdf
104	https://www.aepd.es/resoluciones/PS-00188-2019_ORI.pdf
105	https://www.aepd.es/resoluciones/PS-00266-2019_ORI.pdf
106	https://www.aepd.es/resoluciones/PS-00291-2019_ORI.pdf
107	https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-dwingt-uwv-met-sanctie-gegevens-beter-te-beveiligen
108	https://www.cnpd.pt/bin/decisoes/Delib/DEL_2019_207.pdf
109	https://www.etrend.sk/ekonomika/socialna-poistovna-porusila-gdpr-pokutu-50-tisic-eur-nechce-zaplatit.html
110	https://www.aepd.es/resoluciones/PS-00174-2019_ORI.pdf
111	https://www.uouu.cz/kontrola-zpracovani-osobnich-udaju-po-odvolani-souhlasu-spolecnost-alza-cz-a-s/ds-5717/archiv=0&p1=5653
112	https://www.uouu.cz/kontrola-zabezpeceni-osobnich-udaju-pri-provozovani-online-hry-fyzicka-osoba-podnikajici/ds-5723/archiv=0&p1=5653

113	https://www.aepd.es/resoluciones/PS-00305-2019_ORI.pdf
114	https://www.aepd.es/resoluciones/PS-00233-2019_ORI.pdf
115	https://www.dataprotection.ro/index.jsp?page=O_noua_amenda_in_baza_RGPD&lang=ro
116	https://www.dataprotection.ro/index.jsp?page=Amenda_pentru_incalcarea_RGPD&lang=ro
117	https://www.aepd.es/resoluciones/PS-00251-2019_ORI.pdf
118	https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000039419459&fastReqId=461698027&fastPos=1
119	https://www.aepd.es/resoluciones/PS-00237-2019_ORI.pdf
120	https://twitter.com/900sekundes/status/1199208013959172096
121	https://www.aepd.es/resoluciones/PS-00127-2019_ORI.pdf
122	https://www.datenschutz.rlp.de/de/aktuelles/detail/news/detail/News/geldbusse-gegen-krankenhaus-aufgrund-von-datenschutz-defiziten-beim-patientenmanagement/
123	https://www.autoriteprotectiondonnees.be/news/la-chambre-contentieuse-sanctionne-deux-candidats-aux-elections-communales-de-2018
124	https://www.autoriteprotectiondonnees.be/news/la-chambre-contentieuse-sanctionne-deux-candidats-aux-elections-communales-de-2018
125	https://www.dataprotection.ro/?page=Sanctiune_CN_TAROM&lang=ro
126	https://www.dataprotection.ro/?page=Amenda_ING_RGPD&lang=ro
127	https://www.dataprotection.ro/index.jsp?page=alta_sanctiune_Royal_President&lang=ro
128	https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2019/30_BfDIverh%C3%A4ngtGeldbu%C3%9Fe1u1.html
129	https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2019/30_BfDIverh%C3%A4ngtGeldbu%C3%9Fe1u1.html
130	https://www.aepd.es/resoluciones/PS-00087-2019_ORI.pdf
131	https://www.aepd.es/resoluciones/PS-00092-2019_ORI.pdf
132	https://www.aepd.es/resoluciones/PS-00212-2019_ORI.pdf
133	https://www.aepd.es/resoluciones/PS-00173-2019_ORI.pdf
134	https://www.aepd.es/resoluciones/PS-00205-2019_ORI.pdf
135	https://www.aepd.es/resoluciones/PS-00064-2019_ORI.pdf
136	https://www.aepd.es/resoluciones/PS-00150-2019_ORI.pdf
137	https://www.aepd.es/resoluciones/PS-00050-2019_ORI.pdf
138	https://www.aepd.es/resoluciones/PS-00135-2019_ORI.pdf
139	https://www.naih.hu/files/NAIH-2019-2076-hatarozat.pdf
140	https://www.cdpb.bg/?p=element_view&aid=2226
141	https://www.aepd.es/resoluciones/PS-00140-2019_ORI.pdf
142	https://www.aepd.es/resoluciones/PS-00265-2019_ORI.pdf
143	https://www.faz.net/aktuell/gesellschaft/kriminalitaet/polizisten-nutzen-daten-um-minderjaehrige-maedchen-zu-kontaktieren-16227841.html
144	https://www.datainspektionen.se/globalassets/dokument/beslut/beslut-tillsyn-mrkoll.pdf
145	https://www.dataprotection.ro/?page=Alta_amenda_pentru_incalcarea_GDPR&lang=en
146	https://www.aepd.es/resoluciones/PS-00250-2019_ORI.pdf
147	https://www.aepd.es/es/documento/ps-00279-2019.pdf
148	https://www.dataprotection.ro/index.jsp?page=Noi_amenzi_in_aplicarea_RGPD&lang=ro
149	https://www.dataprotection.ro/index.jsp?page=Noi_amenzi_in_aplicarea_RGPD&lang=ro
150	https://www.naih.hu/files/NAIH-2019-2485-hatarozat.pdf
151	https://www.aepd.es/resoluciones/PS-00236-2019_ORI.pdf
152	https://www.aepd.es/resoluciones/PS-00140-2019_ORI.pdf
153	https://www.aepd.es/resoluciones/PS-00249-2019_ORI.pdf
154	https://autoriteitpersoonsgegevens.nl/nl/nieuws/sancties-voor-menzis-en-vgz-voor-overtreding-van-de-privacywet
155	http://www.dpa.gr/APDPXPortlets/htdocs/documentDisplay.jsp?docid=146,94,80,247,188,211,182,68

156	https://www.dataprotection.ro/?page=O_noua_amenda_pentru_incalcare RGPD_comunicat_decembrie&lang=ro
157	https://naih.hu/files/NAIH-2019-51-hatarozat.pdf
158	https://ico.org.uk/media/action-weve-taken/enforcement-notice/2616741/doorstop-en-20191217.pdf
159	https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/DEQF_13-2019_FR_ANO.pdf
160	https://www.dataprotection.ro/?page=Amenda_asociatie_proprietari&lang=ro
161	https://www.aepd.es/es/documento/ps-00320-2019.pdf
162	https://www.cdpd.bg/index.php?p=element&aid=1219
163	https://www.cdpd.bg/index.php?p=element&aid=1219
164	https://www.cdpd.bg/index.php?p=element&aid=1219
165	https://www.cdpd.bg/index.php?p=element&aid=1219
166	https://www.cdpd.bg/index.php?p=element&aid=1219
167	https://www.cdpd.bg/index.php?p=element&aid=1219
168	https://www.cdpd.bg/index.php?p=element&aid=1219
169	https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/BETG_12-2019_NL.PDF
170	https://www.handelsblatt.com/politik/deutschland/dsgvo-datenschutz-verstoesse-zahl-der-bussgelder-ist-drastisch-gestiegen/25364576.html?ticket=ST-45092061-7c0aydLKNr5gZlxMtwWk-ap1
171	https://www.aepd.es/es/documento/ps-00093-2019.pdf
172	https://www.aepd.es/es/documento/ps-00445-2019.pdf
173	https://www.aepd.es/es/documento/ps-00109-2019.pdf
174	https://www.aepd.es/es/documento/ps-00025-2019.pdf
175	https://www.aepd.es/es/documento/ps-00231-2019.pdf
176	https://www.dataprotection.ro/?page=Alta_amenda_pentru_incalcare RGPD_2020_1&lang=ro
177	https://www.dataprotection.ro/?page=sanctiune_pentru_incalcare RGPD_2020_2&lang=ro
178	http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/all/ACDFDC478581BEE1C22584EE002EE9C2?OpenDocument
179	http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/all/ACDFDC478581BEE1C22584EE002EE9C2/\$file/2019-apofasi%20bradford%20system%20%CE%91%CE%9D%CE%A9%CE%9D%CE%A5%CE%9C%CE%9F%CE%A0.pdf?openelement
180	http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/all/ACDFDC478581BEE1C22584EE002EE9C2/\$file/2019-apofasi%20bradford%20system%20%CE%91%CE%9D%CE%A9%CE%9D%CE%A5%CE%9C%CE%9F%CE%A0.pdf?openelement
181	http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/all/ACDFDC478581BEE1C22584EE002EE9C2/\$file/2019-apofasi%20bradford%20system%20%CE%91%CE%9D%CE%A9%CE%9D%CE%A5%CE%9C%CE%9F%CE%A0.pdf?openelement
182	http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/all/ACDFDC478581BEE1C22584EE002EE9C2?OpenDocument
183	http://www.dpa.gr/APDPXPortlets/htdocs/documentDisplay.jsp?docid=126,92,211,86,111,236,222,151
184	https://www.dataprotection.ro/index.jsp?page=O_noua_sanctiune_pentru_incalcare RGPD_2020_3&lang=ro
185	https://www.dataprotection.ro/index.jsp?page=O_noua_sanctiune_pentru_incalcare RGPD_2020_3&lang=ro
186	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9244365
187	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9244358
188	http://www.dpa.gr/APDPXPortlets/htdocs/documentDisplay.jsp?docid=205,136,113,56,60,108,243,88
189	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9256486
190	https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/01/35.-T%C3%A4tigkeitsbericht-f%C3%BCr-den-Datenschutz-Web.pdf#page=44&zoom=100,0,0
191	https://www.aepd.es/es/documento/ps-00397-2019.pdf
192	https://www.aepd.es/es/documento/ps-00227-2019.pdf
193	https://www.aepd.es/es/documento/ps-00270-2019.pdf
194	https://www.aepd.es/es/documento/ps-00405-2019.pdf

195	https://www.aepd.es/es/documento/ps-00275-2019.pdf
196	https://www.aepd.es/es/documento/ps-00402-2019.pdf
197	https://www.aepd.es/es/documento/ps-00278-2019.pdf
198	https://www.aepd.es/es/documento/ps-00400-2019.pdf
199	https://www.aepd.es/es/documento/ps-00259-2019.pdf
200	https://www.aepd.es/es/documento/ps-00292-2019.pdf
201	https://www.aepd.es/es/documento/ps-00427-2018.pdf
202	https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9261227
203	https://datenschutz-hamburg.de/assets/pdf/28._Taetigkeitsbericht_Datenschutz_2019_HmbBfDI.pdf
204	https://datenschutz-hamburg.de/assets/pdf/28._Taetigkeitsbericht_Datenschutz_2019_HmbBfDI.pdf
205	https://datenschutz-hamburg.de/assets/pdf/28._Taetigkeitsbericht_Datenschutz_2019_HmbBfDI.pdf
206	https://www.aepd.es/es/documento/ps-00298-2019.pdf
207	https://www.aepd.es/es/documento/ps-00466-2019.pdf
208	https://www.aepd.es/es/documento/ps-00423-2019.pdf
209	https://www.aepd.es/es/documento/ps-00181-2019.pdf
210	https://www.aepd.es/es/documento/ps-00471-2019.pdf
211	https://www.aepd.es/es/documento/ps-00385-2019.pdf
212	https://www.garantepriacy.it/web/guest/home/docweb/-/docweb-display/docweb/9269629
213	https://www.garantepriacy.it/web/guest/home/docweb/-/docweb-display/docweb/9269618
214	https://www.aepd.es/es/documento/ps-00235-2019.pdf
215	https://www.aepd.es/es/documento/ps-00212-2019.pdf
216	https://www.aepd.es/es/documento/ps-00187-2019.pdf
217	https://www.aepd.es/es/documento/ps-00369-2019.pdf
218	https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_knlbtb.pdf
219	https://www.aepd.es/es/documento/ps-00455-2019.pdf
220	https://www.aepd.es/es/documento/ps-00469-2019.pdf
221	https://www.aepd.es/es/documento/ps-00474-2019.pdf
222	https://www.aepd.es/es/documento/ps-00421-2019.pdf
223	https://www.aepd.es/es/documento/ps-00426-2019.pdf
224	https://uodo.gov.pl/decyzje/ZSZS.440.768.2018 , http://orzeczenia.nsa.gov.pl/doc/2A2CFDE9D2
225	https://www.aepd.es/es/documento/ps-00429-2019.pdf
226	https://www.garantepriacy.it/web/guest/home/docweb/-/docweb-display/docweb/9283029
227	https://www.garantepriacy.it/web/guest/home/docweb/-/docweb-display/docweb/9283014
228	https://www.aepd.es/es/documento/ps-00293-2019.pdf
229	https://www.aepd.es/es/documento/ps-00358-2019.pdf
230	https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2020/mar/to-kommuner-indstillet-til-boede/
231	https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2020/mar/to-kommuner-indstillet-til-boede/
232	https://www.datainspektionen.se/globalassets/dokument/beslut/2020-03-11-beslut-google.pdf
233	https://www.personuvernd.is/urlausnir/nr/2882
234	https://www.personuvernd.is/urlausnir/nr/2885
235	https://www.datatilsynet.no/contentassets/bc26a2a8b78b4b30b4b060a4cac80d90/varsel-ralingen.pdf
236	https://www.datenschutz.saarland.de/fileadmin/user_upload/uds/tberichte/tb28_2019.pdf
237	https://www.datatilsynet.no/contentassets/8dbf5b4b2a33471aacf375b1f0032347/varsel-om-overtredelsesgebyr.pdf
238	https://www.youtube.com/watch?v=wFBrgJlkDwI
239	https://azop.hr/aktualno/detaljnije/rjesenje-kojim-se-izrice-upravno-novcana

240	https://www.aepd.es/es/documento/ps-00351-2019.pdf
241	https://www.dataprotection.ro/?page=sanctiune_vodafone_februarie_2020&lang=ro
242	http://www.dpa.gr/APDPXPortlets/htdocs/documentDisplay.jsp?docid=158,220,63,69,45,69,224,53
243	https://www.aepd.es/es/documento/ps-00425-2019.pdf
244	https://www.aepd.es/es/documento/ps-00335-2019.pdf
245	https://www.aepd.es/es/documento/ps-00360-2019.pdf
246	https://www.aepd.es/es/documento/ps-00272-2019.pdf
247	https://www.aepd.es/es/documento/ps-00317-2019.pdf
248	https://www.aepd.es/es/documento/ps-00008-2020.pdf
249	https://www.garantepriacy.it/web/guest/home/docweb/-/docweb-display/docweb/9283121
250	http://www.dpa.gr/APDPXPortlets/htdocs/documentDisplay.jsp?docid=89,253,106,96,141,223,198,107
251	https://www.naih.hu/files/NAIH-2019-3854_hatarozat.pdf
252	https://www.naih.hu/files/NAIH_2019_1859_hatarozat.pdf
253	https://www.naih.hu/files/NAIH_2019_1598_hatarozat.pdf
254	https://www.naih.hu/files/NAIH-2019-2402_hatarozat.pdf
255	https://www.naih.hu/files/NAIH_2019_1837_hatarozat.pdf
256	https://www.naih.hu/files/NAIH-2019-2472_hatarozat.pdf
257	https://www.naih.hu/files/NAIH_2019_2466_hatarozat.pdf
258	https://www.naih.hu/files/NAIH-2019-1590-hatarozat.pdf
259	https://www.naih.hu/files/NAIH-2019-769-hatarozat.pdf
260	https://www.naih.hu/files/NAIH-2020-32-4-hatarozat.pdf
261	https://www.dataprotection.ro/index.jsp?page=Comunicat_amenda_asociatia_sos_infertilitatea&lang=ro
262	https://www.dataprotection.ro/index.jsp?page=Comunicat_amenda_enel_martie_2020&lang=ro
263	https://www.dataprotection.ro/index.jsp?page=Comunicat_noua_amenda_vodafone&lang=ro
264	https://www.dataprotection.ro/index.jsp?page=Comunicat_amenda_dante_international_martie_2020&lang=ro
265	https://www.garantepriacy.it/web/guest/home/docweb/-/docweb-display/docweb/9285411
266	https://www.aepd.es/es/documento/ps-00436-2019.pdf
267	https://uodo.gov.pl/decyzje/ZSPR.421.19.2019
268	http://www.cdpd.bg/download.php?part=rubric_element&aid=4563
269	http://www.cdpd.bg/download.php?part=rubric_element&aid=4563
270	http://www.cdpd.bg/download.php?part=rubric_element&aid=4563
271	https://www.lda.brandenburg.de/media_fast/4055/TB_2019_Datenschutz.pdf
272	https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-18-2020.pdf
273	https://www.datainspektionen.se/globalassets/dokument/beslut/beslut-tillsyn-ssc-20200428.pdf
274	https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_vingerafdrukken_personeel.pdf
275	https://www.dataprotection.ro/?page=Sanctiune_pentru_incalcarea_RGPD_BCR&lang=ro
276	https://www.datainspektionen.se/globalassets/dokument/beslut/beslut-tillsyn-region-orebro-2020-05-11.pdf
277	https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2020/maj/jobteam-indstillet-til-boede/
278	https://www.irishtimes.com/news/crime-and-law/tusla-becomes-first-organisation-fined-for-gdpr-rule-breach-1.4255692?mode=amp
279	https://tietosuoja.fi/documents/6927448/22406974/Henkilötietojen+käsittelyn+läpinäkyvyys+ja+rekisteröidylle+toimitettavat+tiedot.pdf/b869b7ba-1a05-572e-d97a-9c8a56998fc1/Henkilötietojen+käsittelyn+läpinäkyvyys+ja+rekisteröidylle+toimitettavat+tiedot.pdf
280	https://tietosuoja.fi/documents/6927448/22406974/Työntekijöiden+sijaintitietojen+käsittely+ja+vaikutustenarviointi.pdf/2d04e545-d427-8a0d-3f4d-967de7b428ac/Työntekijöiden+sijaintitietojen+käsittely+ja+vaikutustenarviointi.pdf
281	https://tietosuoja.fi/documents/6927448/22406974/Työnhakijoiden+henkilötietojen+kerääminen+tarpeettomasti.pdf/6cedce13-60cd-c6f9-60cf-b9c8e17db10a/Työnhakijoiden+henkilötietojen+kerääminen+tarpeettomasti.pdf
282	https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/Beslissing_GK_28-2020_NL.pdf

283	https://tietosuoja.fi/documents/6927448/22406974/Päätös+henkilötietojen+käsittelyn+lainmukaisuudesta/60115710-2513-a359-6261-e821818b9ee1/Päätös+henkilötietojen+käsittelyn+lainmukaisuudesta.pdf
284	https://www.naih.hu/files/NAIH-2020-2555-hatarozat.pdf
285	https://www.aepd.es/es/documento/ps-00434-2019.pdf
286	https://www.aepd.es/es/documento/ps-00433-2019.pdf
287	https://www.aepd.es/es/documento/ps-00373-2019.pdf
288	https://www.aepd.es/es/documento/ps-00451-2019.pdf
289	https://www.aepd.es/es/documento/ps-00033-2020.pdf
290	https://www.aepd.es/es/documento/ps-00417-2019.pdf
291	https://www.aepd.es/es/documento/ps-00444-2019.pdf
292	https://www.datatilsynet.no/contentassets/fd5c454b4eae4924af94943ba68002bf/20_02181-3-vedtak-om-overtredelsesgebyr---bergen-kommune.pdf
293	https://www.aepd.es/es/documento/ps-00453-2019.pdf
294	https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/varsel-om-irettesettelse-mot-telenor-norge-as/
295	https://www.cdpd.bg/?p=element&aid=1247
296	https://www.dataprotectionauthority.be/sites/privacycommission/files/documents/Beslissing_GK_25-2020_EN.pdf
297	https://www.dataprotection.ro/?page=Amenda_pentru_incalcarea_RGPD_iunie_2020&lang=ro
298	https://www.aepd.es/es/documento/ps-00048-2020.pdf
299	https://www.aepd.es/es/documento/ps-00390-2019.pdf
300	https://www.aepd.es/es/documento/ps-00359-2019.pdf
301	https://www.dataprotection.ro/?page=O_noua_sanctiune_pentru_incalcarea_RGPD_iunie_2020&lang=ro
302	https://www.aki.ee/sites/default/files/ettekirjutused/2019/ettekirjutus-hoiatus_isikuandmete_kaitse_asjas_30.04.2020_nr_2.1.-6-20-19_korteriuhistu_outokumpu_19.pdf
303	https://www.naih.hu/files/NAIH-2020-32-4-hatarozat.pdf
304	https://www.naih.hu/files/NAIH-2020-200-hatarozat.pdf
305	https://www.naih.hu/files/NAIH-2020-1137-hatarozat.pdf
306	https://www.baden-wuerttemberg.datenschutz.de/lfdi-baden-wuerttemberg-verhaengt-bussgeld-gegen-aok-baden-wuerttemberg-wirksamer-datenschutz-erfordert-regelmaessige-kontrolle-und-anpassung/
307	http://www.poderjudicial.es/cgpj/es/Poder-Judicial/Noticias-Judiciales/El-Tribunal-Supremo-confirma-la-multa-de-7-500-euros-a-una-empresa-de-bromas-telefonicas-por-infraccion-de-la-ley-de-Proteccion-Datos
308	https://www.aepd.es/es/documento/ps-00273-2019.pdf
309	https://www.aepd.es/es/documento/ps-00306-2019.pdf
310	https://www.dataprotection.ro/index.jsp?page=Amenda_pentru%20incalcarea_RGPD_Enel_iunie2020&lang=ro
311	https://www.aepd.es/es/documento/ps-00415-2019.pdf
312	https://www.dataprotection.ro/?page=O_noua_sanctiune_pentru_incalcarea_RGPD_iunie_2020&lang=ro
313	https://www.naih.hu/files/NAIH-2020-1160-10-hatarozat.pdf
314	https://www.datainspektionen.se/globalassets/dokument/beslut/2020-06-16-kamerabevakning-hos-brf.pdf
315	https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/Beslissing_GK_33-2020_NL.pdf
316	https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/Décision_CC_32-2020_FR.pdf
317	https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/Decision_CC_30-2020_FR.pdf
318	https://www.inforights.im/media/1840/dha_penaltynotice_20mar2020_website.pdf
319	https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2020/jun/lejr-kommune-indstilles-til-boede
320	https://www.irishlegal.com/Article/tusla-fined-40-000-in-second-gdpr-breach
321	https://www.datatilsynet.no/contentassets/a42cee6c37084047ac14489dcc318c75/varsel-om-palegg-og-overtredelsesgebyr-200653_13_1.pdf
322	https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/varsel-om-gebyr-aquateknikk/
323	https://www.aepd.es/es/documento/ps-00415-2019.pdf
324	https://www.garantepriacy.it/web/guest/home/docweb/-/docweb-display/docweb/9302897
325	https://www.garantepriacy.it/web/guest/home/docweb/-/docweb-display/docweb/9361186

326	https://www.aepd.es/es/documento/ps-00102-2020.pdf
327	https://www.aepd.es/es/documento/ps-00475-2019.pdf
328	https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/varsel-om-overtredelsesgebyr-til-odin-flissenter-as/
329	https://www.aepd.es/es/documento/ps-00122-2020.pdf
330	https://www.aepd.es/es/documento/ps-00090-2020.pdf
331	https://www.dataprotection.ro/index.jsp?page=Comunicat_09_07_20&lang=ro
332	https://uodo.gov.pl/decyzje/DKE.561.1.2020
333	https://www.datatilsynet.no/contentassets/9d5792264c884f3a903d3981c38812ac/~-20_02191-1-vedtak-om-overtredelsesgebyr--ralingen-kommune-202444_10_1.pdf
334	https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit_bkr_30_juli_2019.pdf
335	https://www.garantprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9435774
336	https://www.garantprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9435753
337	https://www.garantprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9435807
338	https://www.aepd.es/es/documento/ps-00004-2020.pdf
339	https://www.aepd.es/es/documento/ps-00149-2020.pdf
340	https://www.aepd.es/es/documento/ps-00139-2020.pdf
341	https://www.aepd.es/es/documento/ps-00296-2020.pdf
342	https://www.aepd.es/es/documento/ps-00135-2020.pdf
343	https://www.aepd.es/es/documento/ps-000104-2020.pdf
344	https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-37-2020.pdf
345	https://www.aepd.es/es/documento/ps-00068-2020.pdf
346	https://www.aepd.es/es/documento/ps-00060-2020.pdf
347	https://www.aepd.es/es/documento/ps-00459-2019.pdf
348	http://www.dpa.gr/APDPXPortlets/htdocs/documentDisplay.jsp?docid=252,140,181,222,128,166,229,159
349	https://www.aepd.es/es/documento/ps-00452-2019.pdf
350	https://www.aepd.es/es/documento/ps-000450-2019.pdf
351	https://www.aepd.es/es/documento/ps-000422-2019.pdf
352	https://www.aepd.es/es/documento/ps-000114-2019.pdf
353	https://www.aepd.es/es/documento/ps-00010-2020.pdf
354	https://www.aepd.es/es/documento/ps-00014-2020.pdf
355	https://www.aepd.es/es/documento/ps-00115-2020.pdf
356	https://www.aepd.es/es/documento/ps-00134-2020.pdf
357	https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-36-2020.pdf
358	https://www.dataprotection.ro/index.jsp?page=Amenda_pentru_incalcarea_RGPD_Viva_Credit_IFN&lang=ro
359	https://www.dataprotection.ro/index.jsp?page=Sanctiune_pentru_incalcarea_RGPD_Posta_Romana&lang=ro
360	https://www.dataprotection.ro/index.jsp?page=Sanctiune%20pentru%20incalcare%20RGPD%2027_07_20&lang=ro
361	https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2020/jul/arp-hansen-hotel-group-a/s-indstilles-til-boede
362	https://www.cnil.fr/fr/spartoo-sanction-de-250-000-euros-et-injonction-sous-astreinte-de-se-conformer-au-rgpd
363	https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2020/aug/datatilsynet-indstiller-privatbo-til-boede
364	https://www.aepd.es/es/documento/ps-00092-2020.pdf
365	https://www.aepd.es/es/documento/ps-00009-2020.pdf
366	https://www.garantprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9446730
367	https://www.garantprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9446659
368	https://www.garantprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9445710
369	https://www.aepd.es/es/documento/ps-00036-2020.pdf

370	https://tietosuoja.fi/-/yritykselle-seuraamusmaksu-sahkoisen-suoramarkkinoinnin-harjoittamisesta-ilman-ennalta-annettua-suostumusta-ja-rekisteroidyn-oikeuksien-laiminlyonnista
371	https://www.aepd.es/es/documento/ps-00479-2019.pdf
372	https://www.dsb.gv.at/documents/22758/115212/Newsletter_DSB_3_2020.pdf/90579856-6cb5-4206-823a-cacc724cf94e
373	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9445324
374	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9445180
375	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9445550
376	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9445567
377	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9440000
378	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9361186
379	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9440075
380	https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-39-2020.pdf
381	https://uodo.gov.pl/decyzje/DKE.561.3.2020
382	https://www.aepd.es/es/documento/ps-00168-2020.pdf
383	https://www.aepd.es/es/documento/ps-00449-2019.pdf
384	https://www.aki.ee/et/uudised/uudishimuparing-toi-vaartotrahvi
385	https://www.aepd.es/es/documento/ps-00076-2020.pdf
386	https://www.aepd.es/es/documento/ps-00200-2020.pdf
387	https://uodo.gov.pl/decyzje/DKN.5112.13.2020
388	https://www.aepd.es/es/documento/ps-00031-2020.pdf
389	https://www.aepd.es/es/documento/ps-00198-2020.pdf
390	https://www.aepd.es/es/documento/ps-00188-2020.pdf
391	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9445180
392	https://www.uodo.gov.pl/decyzje/ZSO?S.421.25.2019
393	https://www.dpa.gr/portal/page?_pageid=33,15048&_dad=portal&_schema=PORTAL
394	https://www.naih.hu/files/NAIH-2020-1154-9-hatarozat.pdf
395	https://www.dataprotection.ro/?page=Comunicat_Presa_01_09_2020&lang=ro
396	https://www.aepd.es/es/documento/ps-00186-2020.pdf
397	https://www.aepd.es/es/documento/ps-00311-2019.pdf
398	https://www.aepd.es/es/documento/ps-00034-2020.pdf
399	https://www.aepd.es/es/documento/ps-00051-2020.pdf
400	http://www.dpa.gr/APDPXPortlets/htdocs/documentDisplay.jsp?docid=44,255,240,178,22,240,143,187
401	https://www.dataprotection.ro/?page=Comunicat_Presa_08_/09/_20&lang=ro
402	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9451734
403	https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-53-2020.pdf
404	https://www.aepd.es/es/documento/ps-00079-2020.pdf
405	https://datenschutz-hamburg.de/pressemitteilungen/2020/10/2020-10-01-h-m-verfahren
406	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9461168
407	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9461321
408	https://www.aepd.es/es/documento/ps-00024-2020.pdf
409	https://www.naih.hu/files/NAIH-2020-5553-hatarozat.pdf
410	https://uodo.gov.pl/decyzje/DKE.561.2.2020
411	https://www.aepd.es/es/documento/ps-00069-2020.pdf
412	https://www.dataprotection.ro/?page=Comunicat_Presa_01_/10/_2020&lang=ro
413	https://www.dataprotection.ro/?page=Comunicat_Presa_01_/10/_2020&lang=ro

414	https://www.aepd.es/es/documento/ps-00249-2020.pdf
415	https://www.aepd.es/es/documento/ps-00035-2020.pdf
416	https://www.datatilsynet.no/contentassets/44c6c9df0ee64fdc9f704f8ca930d4ce/vedtak-om-otg-odin-flissenter.pdf
417	https://www.aepd.es/es/documento/ps-00312-2019.pdf
418	https://www.aepd.es/es/documento/ps-00206-2019.pdf
419	https://www.aepd.es/es/documento/ps-00058-2019.pdf
420	https://www.dataprotection.ro/?page=Amenda_pentru_incalcare RGPD_15_/10_/2020&lang=ro
421	http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/B64595978C98EFCEC2258606003EC47E?OpenDocument
422	http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/B64595978C98EFCEC2258606003EC47E?OpenDocument
423	https://www.aepd.es/es/documento/ps-00245-2020.pdf
424	https://www.aepd.es/es/documento/ps-00028-2020.pdf
425	https://www.dataprotection.ro/index.jsp?page=Alta_amenda_pentru_incalcare RGPD_oct_2020&lang=ro
426	https://www.aepd.es/es/documento/ps-00234-2020.pdf
427	https://www.naih.hu/files/NAIH-2020-193-hatarozat.pdf
428	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9468523
429	https://vdai.lrv.lt/lt/naujienos/pagal-bendraj-i-duomenu-apsaugos-reglamenta-skirta-bauda-del-netinkamai-tvarkomu-ivaikinto-vaiko-tevu-asmens-duomenu https://edpb.europa.eu/news/national-news/2020/lithuanian-dpa-imposes-fine-improperly-processed-personal-data-parents_en
430	https://www.naih.hu/files/NAIH-2020-2204-8-hatarozat.pdf
431	https://www.aepd.es/es/documento/ps-00303-2020.pdf
432	http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/all/B64595978C98EFCEC2258606003EC47E/\$file/??????%20??????%20??????%2068-2017.pdf?openelement
433	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9469345
434	https://www.aepd.es/es/documento/ps-00003-2020.pdf
435	https://www.aepd.es/es/documento/ps-00341-2020.pdf
436	https://www.aepd.es/es/documento/ps-00182-2020.pdf
437	https://www.aepd.es/es/documento/ps-00308-2020.pdf
438	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9485681
439	https://www.aepd.es/es/documento/ps-00365-2019.pdf
440	https://ico.org.uk/media/action-weve-taken/2618609/ticketmaster-uk-limited-mpn.pdf
441	https://www.aepd.es/es/documento/ps-00185-2020.pdf
442	https://www.aepd.es/es/documento/ps-00247-2020.pdf
443	https://www.aepd.es/es/documento/ps-00251-2020.pdf
444	https://www.aepd.es/es/documento/ps-00348-2020.pdf
445	https://www.aepd.es/es/documento/ps-00353-2019.pdf
446	https://www.aepd.es/es/documento/ps-00356-2020.pdf
447	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9483375
448	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9486531
449	https://www.irishexaminer.com/news/arid-40075673.html
450	https://www.aepd.es/es/documento/ps-00227-2020.pdf
451	https://www.dataprotection.ro/?page=Comunicat_de_presa_23_/11_/2020&lang=ro
452	https://www.aepd.es/es/documento/ps-00189-2020.pdf
453	https://www.dataprotection.ro/?page=Comunicat_Presa_24_11_2020&lang=ro
454	https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042564657
455	https://www.datainspektionen.se/globalassets/dokument/beslut/beslut-tillsyn-stockholms-stad.pdf
456	https://www.datainspektionen.se/globalassets/dokument/beslut/beslut-tillsyn-gnosjo-2020-11-25.pdf

457	https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042563756
458	https://www.aepd.es/es/documento/ps-00416-2019.pdf
459	https://www.garanteproperty.it/web/guest/home/docweb/-/docweb-display/docweb/9474649
460	https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-74-2020.pdf
461	https://www.ris.bka.gv.at/Dokument.wxe?ResultFunctionToken=f40e6a89-d994-4e49-af4a-fcf3d89c1ccd&Position=1&Abfrage=Dsk&Entscheidungsart=Undefined&Organ=Undefined&SucheNachRechtssatz=True&SucheNachText=True&GZ=&VonDatum=01.01.1990&BisDatum=&Norm=&ImRisSeitVonDatum=&ImRisSeitBisDatum=&ImRisSeit=Undefined&ResultPageSize=100&Suchworte=&Dokumentnummer=DSBT_20201019_2020_0_111_488_00
462	https://www.ris.bka.gv.at/Dokument.wxe?ResultFunctionToken=3e78f5a9-f724-41df-a8b6-4f95524b02a4&Position=1&SkipToDocumentPage=True&Abfrage=Dsk&Entscheidungsart=Undefined&Organ=Undefined&SucheNachRechtssatz=True&SucheNachText=True&GZ=&VonDatum=01.10.2020&BisDatum=03.12.2020&Norm=&ImRisSeitVonDatum=&ImRisSeitBisDatum=&ImRisSeit=Undefined&ResultPageSize=100&Suchworte=&Dokumentnummer=DSBT_20201019_2020_0_550_322_00
463	https://www.aepd.es/es/documento/ps-00320-2020.pdf
464	https://www.aepd.es/es/documento/ps-00287-2020.pdf
465	https://www.aepd.es/es/documento/ps-00141-2020.pdf
466	https://www.datainspektionen.se/globalassets/dokument/beslut/beslut-tillsyn-aleris-sjukvard-di-2019-3844.pdf
467	https://www.datainspektionen.se/globalassets/dokument/beslut/beslut-tillsyn-aleris-narsjukvard-di-2019-3842.pdf
468	https://www.aepd.es/es/documento/ps-00317-2020.pdf
469	https://www.datainspektionen.se/globalassets/dokument/beslut/beslut-tillsyn-region-ostergotland-di-2019-3843.pdf
470	https://www.datainspektionen.se/globalassets/dokument/beslut/beslut-tillsyn-region-vasterbotten-di-2019-3841.pdf
471	https://www.datainspektionen.se/globalassets/dokument/beslut/beslut-tillsyn-sahlgrenska-universitetssjukhuset-di-2019-3840.pdf
472	https://www.datainspektionen.se/globalassets/dokument/beslut/beslut-tillsyn-karolinska-universitetssjukhuset-di-2019-3839.pdf
473	https://www.datainspektionen.se/globalassets/dokument/beslut/beslut-tillsyn-capio-st-gorans-sjukhus-di-2019-3846.pdf
474	https://www.datatilsynet.no/contentassets/1679986c04f54694b734ab883eebfde1/endelig-vedtak-til-indre-ostfold-kommune.pdf
475	https://www.aepd.es/es/documento/ps-00278-2020.pdf
476	https://www.aepd.es/es/documento/ps-00322-2020.pdf
477	https://www.aepd.es/es/documento/ps-00262-2020.pdf
478	https://www.aepd.es/es/documento/ps-00324-2020.pdf
479	https://gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-73-2020.pdf
480	https://www.aepd.es/es/documento/ps-00332-2020.pdf
481	https://www.aepd.es/es/documento/ps-00070-2019.pdf
482	https://www.datainspektionen.se/globalassets/dokument/beslut/2020-12-10-beslut-tillsyn-umea-universitet.pdf
483	https://www.uodo.gov.pl/decyzje/DKN.5112.1.2020
484	http://www.dpa.gr/APDPXPortlets/htdocs/documentDisplay.jsp?docid=89,72,206,138,129,101,238,220
485	https://edpb.europa.eu/sites/edpb/files/decisions/final_decision_-_in-19-1-1_9.12.2020.pdf
486	https://www.datainspektionen.se/globalassets/dokument/beslut/2020-12-14-beslut-tillsyn-uppsalahem.pdf
487	https://www.dvi.gov.lv/lv/zinas/datu-valsts-inspekcija-internetveikalam-piemero-eur-15-000-naudas-sodu/
488	https://www.dvi.gov.lv/lv/zinas/datu-valsts-inspekcija-par-neatbilstosu-personas-datu-apstradi-darba-devejam-piemero-eur-6250-lielu-naudas-sodu/
489	https://www.dataprotection.ro/?page=Comunicat_17_12_2020&lang=ro
490	https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042675720 https://www.cnil.fr/fr/violations-de-donnees-de-sante-la-cnil-sanctionne-deux-medecins

491	https://www.cnil.fr/fr/violations-de-donnees-de-sante-la-cnil-sanctionne-deux-medecins https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042676787
492	https://www.aepd.es/es/documento/ps-00438-2019.pdf
493	https://www.naih.hu/files/NAIH-2020-2729-15-hatarozat.pdf
494	https://www.naih.hu/files/NAIH-2020-0066-21-hatarozat.pdf
495	https://www.naih.hu/files/NAIH-2020-0066-21-hatarozat.pdf
496	https://www.aepd.es/es/documento/ps-00219-2019.pdf
497	https://www.aepd.es/es/documento/ps-00368-2020.pdf
498	https://www.dataprotection.ro/?page=Comunicat_Presa_22_12_2020&lang=ro
499	https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-81-2020.pdf
500	https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-81-2020.pdf
501	https://uodo.gov.pl/decyzje/DKN.5131.5.2020
502	https://www.garantepriacy.it/web/guest/home/docweb/-/docweb-display/docweb/9509558
503	https://www.garantepriacy.it/web/guest/home/docweb/-/docweb-display/docweb/9509515
504	https://www.dataprotection.ro/?page=Comunicat_Presa_29_12_2020&lang=ro
505	https://www.dataprotection.ro/?page=Comunicat_presa_30_12_2020&lang=ro
506	https://www.aepd.es/es/documento/ps-00415-2020.pdf
507	https://www.datatilsynet.no/contentassets/004f43fe684445c29e4fc8393a9a714d/varsel-om-overtredelsesgebyr---innovasjon-norge.pdf
508	https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042774286?isSuggest=true https://www.cnil.fr/fr/prospection-commerciale-sanction-publique-lencontre-de-la-societe-performelic
509	https://uodo.gov.pl/decyzje/DKN.5130.1354.2020
510	https://uodo.gov.pl/decyzje/DKN.5131.5.20200
511	https://www.cnil.fr/fr/prospection-commerciale-sanction-de-20-000-euros-lencontre-de-la-societe-neslor https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000042848036
512	http://orzeczenia.nsa.gov.pl/doc/942DE6198F
513	https://www.uoou.cz/vismo/dokumenty2.asp?id_org=200144&id=47199
514	https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2021/lindstrand-trading-as-far-overtredelsesgebyr/
515	https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2021/gveik-as-far-gebyr/
516	https://www.aki.ee/et/uudised/andmekaitse-inspektsioon-kohustas-e-apteeke-lopetama-koheselt-ligipaas-teise-inimese
517	https://www.aki.ee/et/uudised/andmekaitse-inspektsioon-kohustas-e-apteeke-lopetama-koheselt-ligipaas-teise-inimese
518	https://www.aki.ee/et/uudised/andmekaitse-inspektsioon-kohustas-e-apteeke-lopetama-koheselt-ligipaas-teise-inimesee
519	https://lfd.niedersachsen.de/startseite/infothek/presseinformationen/lfd-niedersachsen-verhangt-bussgeld-uber-10-4-millionen-euro-gegen-notebooksbilliger-de-196019.html
520	https://www.garantepriacy.it/web/guest/home/docweb/-/docweb-display/docweb/9518890
521	https://www.garantepriacy.it/web/guest/home/docweb/-/docweb-display/docweb/9518849
522	https://www.aepd.es/es/documento/ps-00477-2019.pdf
523	https://www.naih.hu/files/NAIH-2020-3479-hatarozat.pdf
524	https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/avgjorelser-fra-datatilsynet/2021/far-gebyr-for-videresending-av-e-post/
525	https://www.datatilsynet.no/contentassets/5cd2e76bd5d2481f9578ffe721b7e24d/vedtak-om-overtredelsesgebyr-til-coop-finnmark-sa.pdf
526	https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-02-2021.pdf
527	https://uodo.gov.pl/decyzje/DKN.5131.6.2020
528	https://www.aepd.es/es/documento/ps-00215-2020.pdf
529	https://www.aepd.es/es/documento/ps-00232-2020.pdf
530	https://www.datatilsynet.no/contentassets/c5f433a97050467497810b9e891d5b83/vedtak-om-palegg-og-overtredelsesgebyr---aquateknikk-as.pdf
531	https://www.garantepriacy.it/web/guest/home/docweb/-/docweb-display/docweb/9524175

532	https://www.garantepivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9525315
533	https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-05-2021.pdf
534	https://www.aepd.es/es/documento/ps-00235-2020.pdf
535	https://www.cnil.fr/fr/credential-stuffing-la-cnil-sanctionne-un-responsable-de-traitement-et-son-sous-traitant
536	https://www.cnil.fr/fr/credential-stuffing-la-cnil-sanctionne-un-responsable-de-traitement-et-son-sous-traitant
537	https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-04-2021.pdf
538	https://www.uodo.gov.pl/decyzje/DKE.561.13.2020%20
539	https://www.garantepivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9529527
540	https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/avgjorelser-fra-datatilsynet/2021/cyberbook-as-far-gebyr/
541	https://www.aepd.es/es/documento/ps-00433-2020.pdf
542	https://www.aepd.es/es/documento/ps-00335-2020.pdf
543	https://www.garantepivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9533587
544	https://www.aepd.es/es/documento/ps-00220-2020.pdf
545	https://www.aepd.es/es/documento/ps-00270-2020.pdf
546	https://www.aepd.es/es/documento/ps-00440-2020.pdf
547	https://www.aepd.es/es/documento/ps-00253-2020.pdf
548	https://www.aepd.es/es/documento/ps-00062-2020.pdf
549	https://www.aepd.es/es/documento/ps-00026-2021.pdf
550	https://www.dataprotection.ro/?page=Comunicat_Presa_10_/_02/_21&lang=ro
551	https://uodo.gov.pl/decyzje/DKE.561.11.2020
552	https://www.dataprotection.ie/sites/default/files/uploads/2021-02/Inquiry%20University%20College%20Dublin_0.pdf
553	https://www.dvi.gov.lv/lv/zinas/datu-valsts-inspekcija-internetveikalam-piemero-eur-15-000-naudas-sodu/
554	https://www.aepd.es/es/documento/ps-00430-2020.pdf
555	https://autoriteitpersoonsgegevens.nl/nl/nieuws/ziekenhuis-olvg-beboet-om-onvoldoende-beveiliging-medische-dossiers https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_olvg.pdf
556	https://www.garantepivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9538748
557	https://www.aepd.es/es/documento/ps-00469-2019.pdf
558	https://www.garantepivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9542071
559	https://www.garantepivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9544504
560	https://www.garantepivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9544457
561	https://www.garantepivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9544092
562	https://www.garantepivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9542096
563	https://www.garantepivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9542155
564	https://www.uodo.gov.pl/decyzje/DKN.5130.2024.2020
565	https://www.aepd.es/es/documento/ps-00191-2020.pdf
566	https://azop.hr/izdana-nova-upravna-novcana-kazna/
567	https://www.aepd.es/es/documento/ps-00502-2020.pdf
568	https://naih.hu/hatarozatok-vegzesek?download=326:babavaro-kolcsonnel-osszefuggesben-vegzett-adatkezeles-varandosgondozasi-konyvekrol-valo-masolatkeszites-jogszerusege
569	https://naih.hu/hatarozatok-vegzesek?download=325:1-rendszeres-szocialis-osztondijakkal-kapcsolatos-adatkezeles-a-budapesti-muszaki-es-gazdasagtudomanyi-egyetemem-modositasokkal-egyseges-szerkezetben
570	https://www.dataprotection.ie/sites/default/files/uploads/2021-02/12.08.2020_Decision_Tusla_IN-18-11-04.pdf
571	https://vdai.lrv.lt/lt/naujienos/skirta-bauda-del-bendrojo-duomenu-apsaugos-reglamento-pazeidimu-
572	https://vdai.lrv.lt/lt/naujienos/skirta-bauda-del-bendrojo-duomenu-apsaugos-reglamento-pazeidimu-programeleje-karantinas
573	https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/avgjorelser-fra-datatilsynet/2021/far-gebyr-for-ulovleg-vidaresending-av-e-post/
574	https://www.aepd.es/es/documento/ps-00279-2020.pdf

575	https://twitter.com/EinRobert1/status/1367163781508440066
576	https://vdai.lrv.lt/lt/naujienos/skirta-bauda-del-bendrojo-duomenu-apsaugos-reglamento-pazeidimu-registru-centre
577	https://www.aepd.es/es/documento/ps-00197-2020.pdf
578	http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/B0CED3EDDC2EE5EDC225868D0037E7A4?OpenDocument
579	http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/B0CED3EDDC2EE5EDC225868D0037E7A4?OpenDocument
580	http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/B0CED3EDDC2EE5EDC225868D0037E7A4?OpenDocument
581	http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/B0CED3EDDC2EE5EDC225868D0037E7A4?OpenDocument
582	https://www.dataprotection.ro/?page=Comunicat_Presa_04_03_2021&lang=ro
583	https://uodo.gov.pl/decyzje/DKE.561.16.2020
584	https://www.uodo.gov.pl/decyzje/DKN.5131.7.2020
585	https://www.aepd.es/es/documento/ps-00378-2019.pdf
586	https://www.baden-wuerttemberg.datenschutz.de/vfb-stuttgart-bussgeld-erlassen/
587	https://www.aepd.es/es/documento/ps-00074-2020.pdf
588	https://www.aepd.es/es/documento/ps-00136-2020.pdf
589	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9557753
590	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9557593
591	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9556958
592	https://www.aepd.es/es/documento/ps-00406-2020.pdf
593	https://www.aepd.es/es/documento/ps-00448-2020.pdf
594	https://www.aepd.es/es/documento/ps-00059-2020.pdf
595	https://www.aepd.es/es/documento/ps-00193-2020.pdf
596	https://www.aepd.es/es/documento/ps-00061-2021.pdf
597	https://www.aepd.es/es/documento/ps-00417-2020.pdf
598	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9557793
599	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9556625
600	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9542113
601	https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-36-2021.pdf
602	https://www.aepd.es/es/documento/ps-00405-2020.pdf
603	https://www.aepd.es/es/documento/ps-00375-2020.pdf
604	https://www.aepd.es/es/documento/ps-00483-2020.pdf
605	https://www.aepd.es/es/documento/ps-00484-2020.pdf
606	https://www.dataprotection.ro/?page=Comunicat_Presa_23_03_2021&lang=ro
607	https://www.aepd.es/es/documento/ps-00295-2020.pdf
608	https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2021/gebyr-til-alesund-kommune-for-bruk-av-strava/
609	https://www.aepd.es/es/documento/ps-00179-2020.pdf
610	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9565258
611	https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2021/dragefossen-as-far-gebyr/
612	https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit_boete_booking.pdf
613	https://www.dataprotection.ro/?page=Comunicat_30_03_2021&lang=ro
614	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9567429
615	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9567489
616	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9568244
617	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9562852

618	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9562831
619	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9565218
620	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9570997
621	https://www.aepd.es/es/documento/ps-00464-2020.pdf
622	https://www.aepd.es/es/documento/ps-00054-2021.pdf
623	https://www.aepd.es/es/documento/ps-00437-2020.pdf
624	https://www.aepd.es/es/documento/ps-00087-2021.pdf
625	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9561792
626	https://www.dpa.gr/sites/default/files/2021-04/7_2021anonym.pdf
627	https://www.datatilsynet.no/contentassets/65e913da425949d985baf76849a5929b/vedtak-om-overtredelsesgebyr---asker-kommune.pdf
628	https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2021/miljo--og-kvalitetsledelse-as-far-gebyr/
629	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9574789
630	https://www.aepd.es/es/documento/ps-00473-2020.pdf
631	https://www.uoou.cz/kamery-na-verejnem-prostranstvi-uoou-00811-20/ds-6532/archiv=1&p1=5649
632	https://www.uoou.cz/kontrola-zpracovani-osobnich-udaju-prostrednictvim-kopii-obcanskych-prukazu/ds-6267/archiv=1&p1=5649
633	https://www.dataprotection.ro/?page=Comunicat_Presa_15_/04/_2021&lang=ro
634	https://www.dpa.gr/sites/default/files/2021-04/12_2021anonym.pdf
635	https://www.aepd.es/es/documento/ps-00151-2020.pdf
636	https://www.aepd.es/es/documento/ps-00085-2021.pdf
637	https://www.dataprotection.ro/?page=Comunicat_presa_19_/04/_2021&lang=ro
638	https://www.aepd.es/es/documento/ps-00293-2020.pdf
639	https://www.uoou.cz/kontrola-zabezpeci-internetovych-stranek-v-souvislosti-s-predavanim-vysledku-zdravotnich-vysetreni/ds-6254/archiv=1&p1=5649
640	https://www.uoou.cz/kontrola-zpracovani-osobnich-udaju-pri-telemarketingu/ds-6269/archiv=1&p1=5649
641	https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=49126
642	https://www.aepd.es/es/documento/ps-00491-2020.pdf
643	https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2021/gebyr-til-basaren-drift-as/
644	https://www.aepd.es/es/documento/ps-00359-2020.pdf
645	https://www.aepd.es/es/documento/ps-00102-2021.pdf
646	https://www.dpa.gr/sites/default/files/2021-04/7_2021anonym_0.pdf
647	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9578258
648	https://www.uoou.cz/kontrola-zpracovani-osobnich-udaju-v-ramci-prijimaciho-rizeni-na-vysokou-skolu/ds-6252/archiv=0&p1=5649
649	https://www.uoou.cz/kontrola-zpracovani-osobnich-udaju-v-ambulantnim-informacnim-systemu/ds-6277/archiv=0&p1=5649
650	https://www.uoou.cz/kontrola-zpracovani-osobnich-udaju-potencialnich-klientu-spolecnosti-se-zvlastnim-zamerenim-na-overovani-jejich-totoznosti-a-porizovani-kopii-prukazu-totoznosti-pri-zrizovani-bankovniho-uctu-uoou-02511-19/ds-6487/archiv=0&p1=5649
651	https://www.uoou.cz/kontrola-vyuziti-biometriky-u-klientu-uoou-09654-18/ds-6546/archiv=0&p1=5649
652	https://www.uoou.cz/kontrola-pouzivani-cookies-uoou-00374-20/ds-6500/archiv=0&p1=5649
653	https://www.uoou.cz/kontrola-zpracovani-osobnich-udaju-v-aplikaci-mobilni-rozhlas-uoou-01419-20/ds-6478/archiv=0&p1=5649
654	https://www.uoou.cz/kontrola-zverejnovani-fotografii-zamestnancu-na-internetovych-strankach-zamestnavatele-uoou-03225-19/ds-6474/archiv=0&p1=5649
655	https://www.uoou.cz/zpracovani-osobnich-udaju-na-webovych-strankach-formou-preklapeni-udaju-z-verejnych-rejstrik-uoou-00196-20/ds-6496/archiv=0&p1=5649
656	https://www.aepd.es/es/documento/ps-00240-2019.pdf
657	https://www.aepd.es/es/documento/ps-00107-2021.pdf
658	https://www.aepd.es/es/documento/ps-00055-2021.pdf

659	https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_ap_gemeente_enschede.pdf
660	https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9577065
661	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9577371
662	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9577323
663	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9577346
664	https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-56-2021.pdf
665	https://tietosuojafi.fi/documents/6927448/58640544/Seuraamuskollegion+p%C3%A4%C3%A4t%C3%B6s_henkil%C3%B6tietojen+k%C3%A4sittely+pys%C3%A4k%C3%B6ninnvalvontamaksujen+yhteydess%C3%A4.pdf/9b105604-51e0-7beb-e21b-df1b504843e6/Seuraamuskollegion+p%C3%A4%C3%A4t%C3%B6s_henkil%C3%B6tietojen+k%C3%A4sittely+pys%C3%A4k%C3%B6ninnvalvontamaksujen+yhteydess%C3%A4.pdf?t=1619763172841
666	https://naih.hu/hatarozatok-vegzesek?download=354:bfkh-xi-keruleti-hivatalanal-bekovetkezett-egeszseguyi-adatokat-erinto-adatvedelmi-incidens-es-adatbiztonsagi-hianyossagok
667	https://www.datatilsynet.no/contentassets/8311c84c085b424d8d5c55dd4c9e2a4a/advance-notification-of-an-administrative-fine--disqus-inc.pdf
668	https://www.dataprotection.ro/?page=Comunicat_07_/05_/2021&lang=ro
669	https://www.personuvernd.is/information-in-english/greinar/personal-data-breach-in-the-information-system-mentor-administrative-fine
670	https://www.aepd.es/es/documento/ps-00037-2020.pdf
671	https://www.aepd.es/es/documento/ps-00236-2020.pdf
672	https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boete_pvv_overijssel.pdf
673	https://www.aepd.es/es/documento/ps-00113-2021.pdf
674	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9584421
675	https://www.dataprotection.ro/?page=Comunicat_Presa_14_/05_/2021&lang=ro
676	https://www.dataprotection.ro/?page=Comunicat_Presa_13_/05_/2021&lang=ro
677	https://www.aepd.es/es/documento/ps-00123-2021.pdf
678	https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/20210512_boetebesluit_ap_locatefamily.pdf
679	https://naih.hu/hatarozatok-vegzesek?download=380:kamerak-uzemeltetese-idosek-otthonaban
680	https://www.dpa.gr/sites/default/files/2021-05/17_2021anonym.pdf
681	https://www.uodo.gov.pl/decyzje/DKN.5130.3114.2020
682	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9567489
683	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9587637
684	https://www.dataprotection.ro/?page=Comunicat_Presa_19_/05_/2021_1&lang=ro
685	https://www.dataprotection.ro/?page=Comunicat_Presa_19_05_2021_2&lang=ro
686	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9587053
687	https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boete_cpa_verzuimregistratie.pdf
688	https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/avgjorelser-fra-datatilsynet/2021/overtredelsesgebyr-til-oslo-kommune/
689	https://www.dataprotection.ie/sites/default/files/uploads/2021-05/Redacted_23.03.2021_Decision_IN-19-7-2.pdf
690	https://www.aepd.es/es/documento/ps-00066-2021.pdf
691	https://www.aepd.es/es/documento/ps-00036-2021.pdf
692	https://naih.hu/hatarozatok-vegzesek?download=381:diszpecseri-munkakort-betolto-munkavallaloval-folytatott-telefonhivas-rogzitese
693	https://naih.hu/hatarozatok-vegzesek?download=381:diszpecseri-munkakort-betolto-munkavallaloval-folytatott-telefonhivas-rogzitese
694	https://www.aepd.es/es/documento/ps-00030-2021.pdf
695	https://www.aepd.es/es/documento/ps-00378-2020.pdf
696	https://www.aepd.es/es/documento/ps-00316-2020.pdf
697	https://www.aepd.es/es/documento/ps-00155-2021.pdf
698	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9590711

699	https://www.dpa.gr/sites/default/files/2021-05/21_2021anonym.pdf
700	https://www.datatilsynet.no/contentassets/ecc60fae5be740da81468d4eb23c43a3/vedtak-om-overtredelsesgebyr-til-innovasjon-norge.pdf
701	https://www.aepd.es/es/documento/ps-00401-2020.pdf
702	https://www.aepd.es/es/documento/ps-00156-2020.pdf
703	https://www.dpa.gr/sites/default/files/2021-05/20_2021anonym.pdf
704	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9591223
705	https://www.aepd.es/es/documento/ps-00135-2021.pdf
706	https://www.aepd.es/es/documento/ps-00116-2021.pdf
707	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9592133
708	https://www.aepd.es/es/documento/ps-00126-2021.pdf
709	https://www.aepd.es/es/documento/ps-00140-2021.pdf
710	https://www.aepd.es/es/documento/ps-00261-2020.pdf
711	https://cnpd.public.lu/content/dam/cnpd/fr/decisions-fr/2021/Decision-17FR-2021-sous-forme-anonymisee.pdf
712	https://cnpd.public.lu/content/dam/cnpd/fr/decisions-fr/2021/Decision-15FR-2021-sous-forme-anonymisee.pdf
713	https://cnpd.public.lu/content/dam/cnpd/fr/decisions-fr/2021/Decision-14FR-2021-sous-forme-anonymisee.pdf
714	https://cnpd.public.lu/content/dam/cnpd/fr/decisions-fr/2021/Decision-16FR-2021-sous-forme-anonymisee.pdf
715	https://www.imy.se/globalassets/dokument/beslut/2021/2021-06-07-beslut-region-sormland.pdf
716	https://www.imy.se/globalassets/dokument/beslut/2021/2021-06-07-beslut-region-varmland.pdf
717	https://www.imy.se/globalassets/dokument/beslut/2021/2021-06-07-beslut-region-stockholm.pdf
718	https://www.imy.se/globalassets/dokument/beslut/2021/2021-06-07-beslut-medhelp.pdf
719	https://www.imy.se/globalassets/dokument/beslut/2021/2021-06-07-beslut-voice-integrate.pdf
720	https://www.dataprotection.ro/?page=Comunicat_Presa_09_06_2021&lang=ro
721	https://uodo.gov.pl/decyzje/DKE.561.23.2020
722	https://www.imy.se/globalassets/dokument/beslut/2021/2021-06-09-beslut-raddningstjanst-ostra-skaraborg.pdf
723	https://www.datatilsynet.no/contentassets/28e9c4b1562743debffbc9ab253f3db2/vedtak-om-overtredelsesgebyr---brabankasa.pdf
724	https://www.datenschutzstelle.li/application/files/8816/2246/5791/Taetigkeitsbericht_-_2020.pdf
725	https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boete_orthodontiepraktijk.pdf
726	https://cnpd.public.lu/content/dam/cnpd/fr/decisions-fr/2021/Decision-18FR-2021-sous-forme-anonymisee.pdf
727	https://www.aepd.es/es/documento/ps-00177-2021.pdf
728	https://www.dataprotection.ro/?page=Comunicat_Presa_16_06_2021&lang=ro
729	https://www.uodo.gov.pl/decyzje/DKE.561.25.2020
730	https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2021/jun/vejle-kommune-indstilles-til-boede
731	https://www.dpa.gr/sites/default/files/2021-06/23_2021anonym.pdf
732	https://vdai.lrv.lt/lt/naujienos/sporto-klubui-skirta-bauda-uz-bendrojo-duomenu-apsaugos-reglamento-pazeidimus-tvarkant-klientu-ir-darbuotoju-pirstu-atspaudus
733	https://www.imy.se/globalassets/dokument/beslut/2021/2021-06-21-beslut-sl.pdf
734	https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000043668709
735	https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2021/gebyr-for-innsyn-i-tidligere-ansatts-e-postkasse-og-manglende-avslutning-av-e-postkassen/
736	https://www.aepd.es/es/documento/ps-00301-2020.pdf
737	https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9670025
738	https://www.datatilsynet.no/contentassets/e7e029cdedec4c4e8907aef6bb08590c/20_02165-9-vedtak-om-overtredelsesgebyr--moss-kommune-236334_9_1.pdf
739	https://vdai.lrv.lt/uploads/vdai/documents/files/2020%20m_%20asmens%20duomenu%20apsaugos%20Lietuvoje%20a-pzvalga.pdf
740	https://www.personuvernd.is/urlausnir/huppis-ehf.-sektud-vegna-voktunar-med-eftirlitsmyndavelum-i-starfsmannarymi-1
741	https://www.uodo.gov.pl/decyzje/DKN.5131.3.2021

742	https://cnpd.public.lu/content/dam/cnpd/fr/decisions-fr/2021/Decision-11FR-2021-sous-forme-anonymisee.pdf
743	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9675440
744	https://finlex.fi/fi/viranomaiset/tsv/2021/20210863
745	https://azop.hr/izdane-nove-upravne-novcane-kazne/
746	https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2021/jul/privat-virksomhed-indstillet-til-boede
747	https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9669974
748	https://cnpd.public.lu/content/dam/cnpd/fr/decisions-fr/2021/Decision-22FR-2021-sous-forme-anonymisee.pdf
749	https://cnpd.public.lu/content/dam/cnpd/fr/decisions-fr/2021/Decision-21FR-2021-sous-forme-anonymisee.pdf
750	https://gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9677521
751	https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boete_uwv_beveiliging_groepsberichten.pdf
752	https://ico.org.uk/media/action-weve-taken/mpns/2620171/mermaids-mpn-20210705.pdf
753	https://cnpd.public.lu/content/dam/cnpd/fr/decisions-fr/2021/Decision-20FR-2021-sous-forme-anonymisee-.pdf
754	https://www.aepd.es/es/documento/ps-00259-2020.pdf
755	https://www.aepd.es/es/documento/ps-00459-2020.pdf
756	https://azop.hr/izdane-nove-upravne-novcane-kazne/
757	https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2021/jul/medicals-nordic-is-indstillet-til-boede
758	https://www.lida.bayern.de/media/baylda_report_10.pdf
759	https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2021/jul/region-syddanmark-indstilles-til-boede
760	https://cnpd.public.lu/content/dam/cnpd/fr/decisions-fr/2021/Decision-24FR-2021-sous-forme-anonymisee.pdf
761	https://www.aepd.es/es/documento/ps-00435-2020.pdf
762	https://www.aepd.es/es/documento/ps-00151-2021.pdf
763	https://www.aepd.es/es/documento/ps-00410-2020.pdf
764	https://www.aepd.es/es/documento/ps-00364-2020.pdf
765	https://www.aepd.es/es/documento/ps-00060-2021.pdf
766	https://www.aepd.es/es/documento/ps-00205-2021.pdf
767	https://www.dpa.gr/sites/default/files/2021-07/26_2021anonym.pdf
768	https://www.aepd.es/es/documento/ps-00180-2021.pdf
769	https://uodo.gov.pl/decyzje/DKN.5131.11.2020
770	https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boete_tiktok.pdf
771	https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000043829617?isSuggest=true
772	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9682619
773	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9682641
774	https://www.aepd.es/es/documento/ps-00197-2021.pdf
775	https://www.aepd.es/es/documento/ps-00202-2021.pdf
776	https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000043860997 https://www.cnil.fr/fr/fichier-de-lobbying-sanction-de-400-000-euros-lencontre-de-la-societe-monsanto
777	https://www.aepd.es/es/documento/ps-00120-2021.pdf
778	https://www.sec.gov/ix?doc=/Archives/edgar/data/0001018724/000101872421000020/amzn-20210630.htm#i5986f88ea1e04d5c91ff09fed8d716f0_103
779	https://www.aepd.es/es/documento/ps-00310-2021.pdf
780	https://www.aepd.es/es/documento/ps-00015-2021.pdf
781	https://www.aepd.es/es/documento/ps-00157-2021.pdf
782	https://www.aepd.es/es/documento/ps-00488-2020.pdf
783	https://www.aepd.es/es/documento/ps-00277-2021.pdf
784	https://www.aepd.es/es/documento/ps-00396-2020.pdf

785	https://www.aepd.es/es/documento/ps-00394-2020.pdf
786	https://tietosuoja.fi/-/korkeakoululle-seuraamusmaksu-tietosuojarikkomuksista-tyoajanseurannassa-kertyneiden-sijaintitietojen-kasittelyssa https://tietosuoja.fi/documents/6927448/58640544/TSV+Päätös+3843.163.20.docx.pdf/111b7673-9399-1cbc-bd0f-3ba937042d54/TSV+Päätös+3843.163.20.docx.pdf?t=1627454928275
787	https://www.dataprotection.ro/?page=Comunicat_Presa_30_07_2021&lang=ro
788	https://www.aepd.es/es/documento/ps-00467-2020.pdf
789	https://www.aepd.es/es/documento/ps-00044-2021.pdf
790	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9685994
791	https://fd.niedersachsen.de/download/169169 , https://www.heise.de/news/DSGVO-Bussgeld-wegen-des-Betriebs-einer-Website-mit-veralteter-Software-6154208.html
792	https://www.heise.de/news/Rewe-wird-fuer-Kunden-Profiling-in-Oesterreich-bestaft-6153577.html https://www.derstandard.at/story/2000128639162/joe-bonusclub-soll-millionenstrafe-zahlen
793	https://www.aepd.es/es/documento/ps-00147-2021.pdf
794	https://www.aepd.es/es/documento/ps-00148-2021.pdf
795	https://www.aepd.es/es/documento/ps-00146-2021.pdf
796	https://www.aepd.es/es/documento/ps-00476-2020.pdf
797	https://www.aepd.es/es/documento/ps-00424-2020.pdf
798	https://www.aepd.es/es/documento/ps-00360-2020.pdf
799	https://www.aepd.es/es/documento/ps-00106-2021.pdf
800	https://www.aepd.es/es/documento/ps-00228-2020.pdf
801	https://www.aepd.es/es/documento/ps-00097-2021.pdf
802	https://www.aepd.es/es/documento/ps-00200-2021.pdf
803	https://www.aepd.es/es/documento/ps-00206-2021.pdf
804	https://www.aepd.es/es/documento/ps-00264-2021.pdf
805	https://www.aepd.es/es/documento/ps-00209-2021.pdf
806	https://www.aepd.es/es/documento/ps-00251-2021.pdf
807	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9685922
808	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9685947
809	https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2021/gebyr-til-waxing-palace-as/
810	https://www.aepd.es/es/documento/ps-00213-2021.pdf
811	https://www.aepd.es/es/documento/ps-00188-2021.pdf
812	https://www.naih.hu/hatarozatok-vegzesek?download=408:elszamoltathatosag-elvenek-megsertese
813	https://www.naih.hu/hatarozatok-vegzesek?download=405:erintetti-jogok-biztositasanak-kotelezettsege-nem-ugyfelerintettek-reszere
814	https://www.aepd.es/es/documento/ps-00506-2020.pdf
815	https://www.aepd.es/es/documento/ps-00237-2021.pdf
816	https://www.dataprotection.ro/?page=Comunicat_Presa_24_08_2021&lang=ro
817	https://www.uodo.gov.pl/decyzje/DKN.5131.22.2021
818	https://www.aepd.es/es/documento/ps-00345-2020.pdf
819	https://www.aepd.es/es/documento/ps-00362-2021.pdf
820	https://edpb.europa.eu/system/files/2021-09/dpc_final_decision_redacted_for_issue_to_edpb_01-09-21_en.pdf https://dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-whatsapp-inquiry
821	https://www.aepd.es/es/documento/ps-00462-2019.pdf
822	https://www.aepd.es/es/documento/ps-00164-2021.pdf
823	https://www.aepd.es/es/documento/ps-00259-2021.pdf
824	https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2021/sep/region-midtjylland-indstillet-til-boede
825	https://dataprotection.ie/en/news-media/data-protection-commission-welcomes-outcome-prosecution-proceedings-taken-against-three-ireland

826	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9697724 , https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9698442
827	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9698724 https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9698442
828	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9698558 , https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9698442
829	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9698597 , https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9698442
830	http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/57759977195D3477C225874800434764?OpenDocument , http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/FD9FF8C6CB04DA6CC22587290043314D?OpenDocument
831	http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/57759977195D3477C225874800434764?OpenDocument , http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/FD9FF8C6CB04DA6CC22587290043314D?OpenDocument
832	http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/57759977195D3477C225874800434764?OpenDocument , http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/FD9FF8C6CB04DA6CC22587290043314D?OpenDocument
833	https://www.aepd.es/es/documento/ps-00302-2021.pdf
834	https://www.aepd.es/es/documento/ps-00226-2021.pdf
835	https://www.aepd.es/es/documento/ps-00156-2021.pdf
836	https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2021/sep/favrskov-kommune-indstilles-til-boede-
837	https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000044043045 , https://www.cnil.fr/fr/sanction-de-3-000-euros-lencontre-de-la-societe-nouvelle-de-lannuaire-francais-snaf
838	https://www.aepd.es/es/documento/ps-00093-2021.pdf
839	https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2021/sep/region-syddanmark-indstillet-til-boede
840	https://www.dpa.gr/sites/default/files/2021-09/36_2021anonym.pdf
841	https://www.dpa.gr/sites/default/files/2021-09/36_2021anonym.pdf
842	https://www.dpa.gr/sites/default/files/2021-09/39_2021anonym.pdf
843	https://www.dpa.gr/sites/default/files/2021-09/37_2021anonym.pdf
844	https://www.aepd.es/es/documento/ps-00262-2021.pdf
845	https://www.aepd.es/es/documento/ps-00193-2021.pdf
846	https://www.heise.de/news/DSGVO-Vattenfall-muss-900-000-Euro-nach-Bonushopper-Auslese-zahlen-6200668.html
847	https://www.inforights.im/media/1903/cosmedltd_pn_11dec2020_website.pdf
848	https://www.aepd.es/es/documento/ps-00227-2021.pdf
849	https://www.aepd.es/es/documento/ps-00189-2021.pdf
850	https://www.aepd.es/es/documento/ps-00190-2021.pdf
851	https://www.datatilsynet.no/contentassets/7121f4f2de614186bc535823c9da7102/20_01727-3vedtak-om-overtredelsesgebyr---ferde-as.pdf
852	https://www.aepd.es/es/documento/ps-00191-2021.pdf
853	https://www.aepd.es/es/documento/ps-00192-2021.pdf
854	https://www.aepd.es/es/documento/ps-00236-2021.pdf
855	https://www.aepd.es/es/documento/ps-00244-2021.pdf
856	https://www.aepd.es/es/documento/ps-00231-2021.pdf
857	https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2021/sep/kraeftens-bekaempelse-indstillet-til-boede
858	https://www.datatilsynet.no/contentassets/d01675e54b9447298952002ff1c208fb/vedtak-om-overtredelsesgebyr---hoylandet-kommune.pdf
859	https://www.datatilsynet.no/contentassets/447e5ad0c7f346fc9cc1c0d62d023bba/vedtak-om-overtredelsesgebyr---st.-olavs-hospital-hf.pdf
860	https://www.aepd.es/es/documento/ps-00471-2020.pdf
861	https://www.aepd.es/es/documento/ps-00187-2021.pdf
862	https://www.aepd.es/es/documento/ps-00243-2021.pdf

863	https://www.datatilsynet.no/contentassets/53bc6882df7e426299e6d551428fc811/vedtak-om-overtredelsesgebyr--ultra-technology-as.pdf
864	https://www.aepd.es/es/documento/ps-00245-2021.pdf
865	https://www.aepd.es/es/documento/ps-00260-2021.pdf
866	https://cnpd.public.lu/content/dam/cnpd/fr/decisions-fr/2021/Decision-31FR-2021-sous-forme-anonymisee.pdf
867	https://www.aepd.es/es/documento/ps-00471-2020.pdf
868	https://www.aepd.es/es/documento/ps-00104-2021.pdf
869	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9705632
870	https://www.aepd.es/es/documento/ps-00111-2021.pdf
871	https://news.post.at/presse/de/post/id/1711838/DATENSCHUTZVERFAHREN%20DER%20ÖSTERREICHISCHEN%20POST, https://www.derstandard.at/story/2000130022725/post-ag-muss-fuer-datenskandal-9-5-millionen-euro-strafe
872	https://www.dsb.gv.at/dam/jcr:1360e98b-d22a-4a49-b3bd-6afca2f86d4c/Datenschutzbericht_2021.pdf
873	https://www.derstandard.at/story/2000130047781/post-und-joe-im-visier-der-datenschutzbehoerde
874	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9705650
875	https://noyb.eu/sites/default/files/2021-10/IN%2018-5-5%20Draft%20Decision%20of%20the%20IE%20SA.pdf
876	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9703988
877	https://www.garantepriacy.it/web/guest/home/docweb/-/docweb-display/docweb/9706389, https://www.garantepriacy.it/home/docweb/-/docweb-display/docweb/9708780
878	https://www.datatilsynet.no/contentassets/4609027cf9504e9aa12c3f05b45bdcf7/varsel-om-vedtak-om-overtredelsesgebyr-og-palegg.pdf
879	https://www.aepd.es/es/documento/ps-00142-2021.pdf
880	https://www.dataprotection.ro/?page=Comunicat_Presa_21.10.2021_2&lang=ro
881	https://www.aepd.es/es/documento/ps-00352-2021.pdf
882	https://www.aepd.es/es/documento/ps-00163-2021.pdf
883	https://ico.org.uk/media/action-weve-taken/mpns/4018736/mpn-hiv-scotland-20211018.pdf, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/10/ico-warning-after-scottish-charity-reveals-personal-data-in-email-error/
884	https://www.aepd.es/es/documento/ps-00500-2020.pdf
885	https://www.aepd.es/es/documento/ps-00239-2021.pdf
886	https://www.aepd.es/es/documento/ps-00249-2021.pdf
887	https://www.aepd.es/es/documento/ps-00050-2021.pdf
888	https://www.aepd.es/es/documento/ps-00195-2021.pdf
889	https://www.aepd.es/es/documento/ps-00242-2021.pdf
890	https://www.dataprotection.ro/?page=Comunicat_Presa_01_11_2021_2&lang=ro
891	https://www.dataprotection.ro/index.jsp?page=Comunicat_Presa_01_11_2021_1&lang=ro
892	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9704069
893	https://www.dataprotection.ie/sites/default/files/uploads/2021-11/IN-20-7-1%20Move%20Irl%20Final%20Decision.pdf, https://www.dataprotection.ie/sites/default/files/uploads/2021-11/IN-20-7-1%20MOVE%20Irl%20Final%20Decision%20EN.pdf
894	https://cnpd.public.lu/content/dam/cnpd/fr/decisions-fr/2021/Decision-35FR-2021-sous-forme-anonymisee.pdf
895	https://cnpd.public.lu/content/dam/cnpd/fr/decisions-fr/2021/Decision-36FR-2021-sous-forme-anomyisee.pdf
896	https://cnpd.public.lu/content/dam/cnpd/fr/decisions-fr/2021/Decision-38FR-2021-sous-forme-anonymisee.pdf
897	https://www.dpa.gr/sites/default/files/2021-11/44_2021anonym.pdf
898	https://www.dataprotection.ro/?page=Comunicat_Presa_11_11_2021&lang=ro
899	https://www.aepd.es/es/documento/ps-00307-2021.pdf
900	https://www.aepd.es/es/documento/ps-00240-2021.pdf
901	https://uodo.gov.pl/decyzje/DKN.5131.16.2021
902	https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boete_transavia.pdf https://autoriteitpersoonsgegevens.nl/en/news/dutch-dpa-fines-transavia-poor-personal-data-security
903	https://www.aepd.es/es/documento/ps-00149-2021.pdf

904	https://www.aepd.es/es/documento/ps-00351-2021.pdf
905	https://www.aepd.es/es/documento/ps-00312-2021.pdf
906	https://www.cpdp.bg/download.php?part=rubric_element&aid=4786
907	https://www.aepd.es/es/documento/ps-00339-2021.pdf
908	https://www.aepd.es/es/documento/ps-00268-2021.pdf
909	https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/D7D2A1120DDE670AC225878B0040D4E7?OpenDocument
910	https://www.cnil.fr/fr/fichiers-devaluation-des-agents-sanction-de-400-000-euros-lencontre-de-la-ratp https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000044286815?init=true&page=1&query=san-2021-019&searchField=ALL&tab_selection=all
911	https://www.aepd.es/es/documento/ps-00165-2021.pdf
912	https://www.aepd.es/es/documento/ps-00346-2021.pdf
913	https://www.aepd.es/es/documento/ps-00289-2021.pdf
914	https://www.aepd.es/es/documento/ps-00269-2021.pdf
915	https://www.dataprotection.ro/?page=Comunicat_Presa_26_11_2021_Amenda&lang=ro
916	https://www.personuvernd.is/urlausnir/akvordun-um-sekt-vegna-ferdagjafar-stjornvalda
917	https://www.personuvernd.is/urlausnir/akvordun-um-sekt-vegna-ferdagjafar-stjornvalda
918	https://www.aepd.es/es/documento/ps-00467-2021.pdf
919	https://www.dpa.gr/sites/default/files/2021-11/48_2021anonym.pdf
920	https://cnpd.public.lu/content/dam/cnpd/fr/decisions-fr/2021/Decision-40FR-2021-sous-forme-anonymisee.pdf
921	https://www.aepd.es/es/documento/ps-00489-2021.pdf
922	https://www.aepd.es/es/documento/ps-00305-2021.pdf
923	https://www.aepd.es/es/documento/ps-00349-2021.pdf
924	https://www.aepd.es/es/documento/ps-00417-2021.pdf
925	https://www.aepd.es/es/documento/ps-00010-2021.pdf
926	https://www.aepd.es/es/documento/ps-00424-2021.pdf
927	https://vdai.lrv.lt/lt/naujienos/automobiliu-nuomos-bendrovei-skirta-bauda-del-duomenu-saugumo-pazeidimo-pagal-bendraji-duomenu-apsaugos-reglamenta
928	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9721784
929	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9721758
930	https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/12/cabinet-office-fined-500-000-for-new-year-honours-data-breach/ https://ico.org.uk/media/action-weve-taken/mpns/4019105/cabinet-office-mpn-202112.pdf
931	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9720448
932	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9722265
933	https://www.aepd.es/es/documento/ps-00459-2021.pdf
934	https://www.aepd.es/es/documento/ps-00384-2021.pdf
935	https://www.aepd.es/es/documento/ps-00280-2021.pdf
936	https://www.aepd.es/es/documento/ps-00269-2021.pdf
937	https://www.aepd.es/es/documento/ps-00452-2021.pdf
938	https://fragenstaat.de/anfrage/einsatz-von-dashcams-12/#nachricht-541947
939	https://fragenstaat.de/anfrage/einsatz-von-dashcams-12/#nachricht-541947
940	https://fragenstaat.de/anfrage/einsatz-von-dashcams-12/#nachricht-541947
941	https://www.zaftda.de/tb-bundeslaender/sachsen/landesdatenschutzbeauftragter-6/750-20-tb-lfd-sachsen-2019-o-drs-nr-vom-22-12-2020/file
942	https://www.zaftda.de/tb-bundeslaender/sachsen/landesdatenschutzbeauftragter-6/750-20-tb-lfd-sachsen-2019-o-drs-nr-vom-22-12-2020/file
943	https://www.zaftda.de/tb-bundeslaender/niedersachsen/748-25-tb-lfd-niedersachsen-2019-o-drs-nr-vom-03-09-2020/file
944	https://www.aepd.es/es/documento/ps-00306-2021.pdf

945	https://www.aepd.es/es/documento/ps-00487-2021.pdf
946	https://autoriteitpersoonsgegevens.nl/nl/nieuws/boete-belastingdienst-voor-discriminerende-en-onrechtmatige-werkwijze https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_belastingdienst.pdf
947	https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-137-2021.pdf
948	https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2021/vedtak-om-overtredelsesgebyr-til-statens-pensjonskasse/
949	https://www.dataprotection.ro/?page=Comunicat_Presa_13_12_2021&lang=ro
950	https://www.datatilsynet.no/contentassets/8ad827efefcb489ab1c7ba129609edb5/administrative-fine--grindr-llc.pdf
951	https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20210212_2020_0_582_166_00/DSBT_20210212_2020_0_582_166_00.html
952	https://finlex.fi/fi/viranomaiset/tsv/2021/20211183
953	https://www.aepd.es/es/documento/ps-00294-2021.pdf
954	https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2021/dec/frederiksberg-kommune-indstilles-til-boede
955	https://naih.hu/hatarozatok-vegzesek?download=469:jogos-erdekre-alapitott-ugyfelelegedettseg-meres-adatvedelmi-megfelelesenek-ertekelese
956	https://www.aepd.es/es/documento/ps-00324-2021.pdf
957	https://www.dpa.gr/sites/default/files/2021-12/52_2021anonym.pdf
958	https://www.aepd.es/es/documento/ps-00350-2021.pdf
959	https://www.aepd.es/es/documento/ps-00300-2021.pdf
960	https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/avgjorelser-fra-datatilsynet/2021/gebyr-og-palegg-om-a-etablere-rutiner-etter-urettmessig-kredittvurdering/
961	https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20210805_2021_0_518_795_00/DSBT_20210805_2021_0_518_795_00.html
962	https://www.aepd.es/es/documento/ps-00416-2021.pdf
963	https://www.aepd.es/es/documento/ps-00468-2021.pdf
964	https://www.aepd.es/es/documento/ps-00389-2021.pdf
965	https://www.aepd.es/es/documento/ps-00204-2021.pdf
966	https://www.aepd.es/es/documento/ps-00536-2021.pdf
967	https://www.aepd.es/es/documento/ps-00537-2021.pdf
968	https://www.aepd.es/es/documento/ps-00427-2021.pdf
969	https://www.aepd.es/es/documento/ps-00404-2021.pdf
970	https://www.aepd.es/es/documento/ps-00493-2020.pdf
971	https://www.cnil.fr/fr/node/121960 https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000044609709
972	https://www.cnil.fr/fr/node/121974 https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000044810599?isSuggest=true
973	https://www.aepd.es/es/documento/ps-00390-2021.pdf
974	https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/avgjorelser-fra-datatilsynet/2022/gebyr-til-elektro--automasjon-systemer-as/
975	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9733053
976	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9722894
977	https://www.dataprotection.ro/?page=Comunicat_Presa_06_12_2021_2&lang=ro
978	https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000044840532 https://www.cnil.fr/fr/cookies-la-cnil-sanctionne-google-hauteur-de-150-millions-deuros
979	https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000044840532 https://www.cnil.fr/fr/cookies-la-cnil-sanctionne-google-hauteur-de-150-millions-deuros
980	https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000044840532 https://www.cnil.fr/fr/cookies-sanction-de-60-millions-deuros-lencontre-de-facebook-ireland-limited
981	https://www.dpa.gr/sites/default/files/2022-01/1_2022%20anonym.pdf
982	https://www.aepd.es/es/documento/ps-00448-2021.pdf
983	https://www.aepd.es/es/documento/ps-00119-2021.pdf
984	https://uodo.gov.pl/decyzje/DKN.5130.2559.2020 https://www.uodo.gov.pl/pl/138/2248
985	https://www.dpa.gr/sites/default/files/2022-01/57_2021anonym.pdf
986	https://www.dpa.gr/sites/default/files/2022-01/56_2021anonym.pdf

987	https://www.dataprotection.ie/sites/default/files/uploads/2022-01/Redacted%20Final%20Decision%20The%20Teaching%20Council_20-04-01.pdf
988	https://noe.orf.at/stories/3138575/
989	https://www.aepd.es/es/documento/ps-00224-2021.pdf
990	https://www.dpa.gr/el/enimerwtiko/prakseisArxis/peristatiko-parabiasis-dedomenon-prosopikoy-haraktira-apoyoyrgeio
991	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9734934
992	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9734884
993	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9732967
994	https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-141-2021.pdf
995	https://www.cnpd.pt/comunicacao-publica/noticias/cnpd-aplica-sancao-ao-municipio-de-lisboa/
996	https://idpc.org/mt/idpc-publications/idpc-issues-decision-on-cplanet-data-breach/
997	https://www.aepd.es/es/documento/ps-00501-2021.pdf
998	https://www.aepd.es/es/documento/ps-00356-2021.pdf
999	https://www.aepd.es/es/documento/ps-00433-2021.pdf
1000	https://www.aepd.es/es/documento/ps-00409-2021.pdf
1001	https://cnpd.public.lu/content/dam/cnpd/fr/decisions-fr/2021/Decision-47FR-2021-sous-forme-anonymisee.pdf
1002	https://www.aepd.es/es/documento/ps-00375-2021.pdf
1003	https://cnpd.public.lu/content/dam/cnpd/fr/decisions-fr/2021/Decision-44FR-2021-sous-forme-anonymisee.pdf
1004	https://www.aepd.es/es/documento/ps-00490-2021.pdf
1005	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9735672
1006	https://www.dataprotection.ro/?page=Comunicat_Presa_20_01_2022&lang=ro
1007	https://www.aepd.es/es/documento/ps-00431-2021.pdf
1008	https://www.aepd.es/es/documento/ps-00518-2021.pdf
1009	https://www.dataprotection.ie/sites/default/files/uploads/2022-01/Limerick%20Council%20Decision%20Summary%20EN.pdf , https://www.dataprotection.ie/sites/default/files/uploads/2022-01/REDACTED_091221_Final%20DecisionLimerick_03-SIU-2018%20PDF%20FINAL.pdf
1010	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9739586
1011	https://tietosuoja.fi/-/matkatoimistolle-seuraamusmaksu-tietosuojalainsaadannon-rikkomisesta https://tietosuoja.fi/documents/6927448/0/TSV+Päätös+4282.161.21.pdf/8679d1a1-c3ae-a820-143c-5ae0cabfc6ff/TSV+Päätös+4282.161.21.pdf?t=1643272760189
1012	https://tietosuoja.fi/-/liikennevakuutuskeskukselle-seuraamusmaksu-tarpeettoman-laajasta-potilastietojen-keraamisesta https://tietosuoja.fi/documents/6927448/105358665/TSV+Päätös+4431.161.21+(1).pdf/9afd15dd-1e8d-c6b5-3ca0-51b4329d577e/TSV+Päätös+4431.161.21+(1).pdf?t=1643273113940
1013	https://www.imy.se/globalassets/dokument/beslut/2022/beslut-regionstyrelsen-region-uppsala.pdf https://www.imy.se/nyheter/sanktionsavgift-mot-region-uppsala-som-brustit-i-sin-sakerhet/
1014	https://www.imy.se/globalassets/dokument/beslut/2022/beslut-sjukhusstyrelsen-region-uppsala.pdf https://www.imy.se/nyheter/sanktionsavgift-mot-region-uppsala-som-brustit-i-sin-sakerhet/
1015	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9739609
1016	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9739653
1017	https://naih.hu/hatarozatok-vezesek?download=483:bunugyi-szemelyes-adatok-kezelese-maganvadlo-altal
1018	https://www.dataprotection.ro/?page=Comunicat_Presa_01_02_2022_2&lang=ro
1019	https://www.aepd.es/es/documento/ps-00458-2021.pdf
1020	https://www.aepd.es/es/documento/ps-00535-2021.pdf
1021	https://www.aepd.es/es/documento/ps-00469-2021.pdf
1022	https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-13-2022.pdf https://www.autoriteprotectiondonnees.be/citoyen/sanction-pour-traitement-massif-de-donnees-twitter-liees-a-laffaire-benalla-a-des-fins-de-profilage-politique
1023	https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-13-2022.pdf https://www.autoriteprotectiondonnees.be/citoyen/sanction-pour-traitement-massif-de-donnees-twitter-liees-a-laffaire-benalla-a-des-fins-de-profilage-politique
1024	https://www.dpa.gr/sites/default/files/2022-01/4_2022%20anonym%20%282%29_0.pdf

1025	https://www.dpa.gr/sites/default/files/2022-01/4_2022%20anonym%20%28%29_0.pdf
1026	https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9741157 https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9737185
1027	https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9741157 https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9736961
1028	https://www.datenschutz.saarland.de/fileadmin/user_upload/uds/tberichte/tb29_DS_2020.pdf
1029	https://www.datenschutz.saarland.de/fileadmin/user_upload/uds/tberichte/tb29_DS_2020.pdf
1030	https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/HBDI_49_Ta%CC%88tigkeitsbericht_2020.pdf
1031	https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2021/02/LfDI-BW_36_Ta%CC%88tigkeitsbericht_2020_WEB.pdf
1032	https://www.lda.brandenburg.de/sixcms/media.php/9/TB_2020_web.pdf
1033	https://www.lda.brandenburg.de/sixcms/media.php/9/TB_2020_web.pdf
1034	https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/HBDI_49_Ta%CC%88tigkeitsbericht_2020.pdf
1035	https://datenschutz-hamburg.de/assets/pdf/29._taetigkeitsbericht_datenschutz_2020.PDF
1036	https://datenschutz-hamburg.de/assets/pdf/29._taetigkeitsbericht_datenschutz_2020.PDF
1037	https://datenschutz-hamburg.de/assets/pdf/29._taetigkeitsbericht_datenschutz_2020.PDF
1038	https://datenschutz-hamburg.de/assets/pdf/29._taetigkeitsbericht_datenschutz_2020.PDF
1039	https://datenschutz-hamburg.de/assets/pdf/29._taetigkeitsbericht_datenschutz_2020.PDF
1040	https://datenschutz-hamburg.de/assets/pdf/29._taetigkeitsbericht_datenschutz_2020.PDF
1041	https://datenschutz-hamburg.de/assets/pdf/29._taetigkeitsbericht_datenschutz_2020.PDF
1042	https://datenschutz-hamburg.de/assets/pdf/29._taetigkeitsbericht_datenschutz_2020.PDF
1043	https://datenschutz-hamburg.de/assets/pdf/29._taetigkeitsbericht_datenschutz_2020.PDF
1044	https://datenschutz-hamburg.de/assets/pdf/29._taetigkeitsbericht_datenschutz_2020.PDF
1045	https://datenschutz-hamburg.de/assets/pdf/29._taetigkeitsbericht_datenschutz_2020.PDF
1046	https://datenschutz-hamburg.de/assets/pdf/29._taetigkeitsbericht_datenschutz_2020.PDF
1047	https://www.aepd.es/es/documento/ps-00221-2021.pdf
1048	https://datenschutz-hamburg.de/assets/pdf/29._taetigkeitsbericht_datenschutz_2020.PDF
1049	https://datenschutz-hamburg.de/assets/pdf/29._taetigkeitsbericht_datenschutz_2020.PDF
1050	https://datenschutz-hamburg.de/assets/pdf/29._taetigkeitsbericht_datenschutz_2020.PDF
1051	https://www.dataprotectionauthority.be/iab-europe-held-responsible-for-a-mechanism-that-infringes-the-gdpr https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-21-2022.pdf
1052	https://www.aepd.es/es/documento/ps-00460-2021.pdf
1053	https://www.aepd.es/es/documento/ps-00322-2021.pdf
1054	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9742435
1055	https://www.aepd.es/es/documento/ps-00001-2021.pdf
1056	https://www.aepd.es/es/documento/ps-00046-2021.pdf
1057	https://www.aepd.es/es/documento/ps-00022-2021.pdf
1058	https://www.aepd.es/es/documento/ps-00027-2021.pdf
1059	https://www.aepd.es/es/documento/ps-00021-2021.pdf
1060	https://www.aepd.es/es/documento/ps-00494-2021.pdf
1061	https://www.aepd.es/es/documento/ps-00505-2021.pdf
1062	https://www.aepd.es/es/documento/ps-00337-2021.pdf
1063	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9742468
1064	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9742908
1065	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9742959
1066	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9742923
1067	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9744655
1068	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9744496
1069	https://uodo.gov.pl/decyzje/DKE.561.16.2021

1070	https://www.datatilsynet.no/contentassets/81543616aa3049f8be77b0b3ab66d353/vedtak-om-palegg-og-overtredelesgebyr---etterforsker1.pdf
1071	https://www.aepd.es/es/documento/ps-00540-2021.pdf
1072	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9745262
1073	https://www.aepd.es/es/documento/ps-00267-2020.pdf
1074	https://www.aepd.es/es/documento/ps-00432-2021.pdf
1075	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9745807
1076	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9746047
1077	https://www.dpa.gr/sites/default/files/2022-02/61_2021anonym.pdf
1078	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9746068
1079	https://www.aepd.es/es/documento/ps-00408-2021.pdf
1080	https://www.aepd.es/es/documento/ps-00463-2021.pdf
1081	https://www.aepd.es/es/documento/ps-00517-2021.pdf
1082	https://www.dataprotection.ro/?page=Comunicat_Presa_22_02_2022_2&lang=ro
1083	https://www.dataprotection.ro/?page=Comunicat_Presa_22_02_2022_1&lang=ro
1084	https://www.aepd.es/es/documento/ps-00551-2021.pdf
1085	https://www.uodo.gov.pl/pl/138/2303 https://www.uodo.gov.pl/decyzje/DKN.5131.33.2021
1086	https://www.aepd.es/es/documento/ps-00488-2021.pdf
1087	https://www.aepd.es/es/documento/ps-00558-2021.pdf
1088	https://tietosuoja.fi/-/laakariklinikalle-seuraamusmaksu-puutteista-rekisteroidyn-oikeuksien-toteutuksessa
1089	https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_dpg.pdf https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-boete-dpg-media-voor-onnodig-opvragen-identiteitsbewijs
1090	https://www.aepd.es/es/documento/ps-00545-2021.pdf
1091	https://twitter.com/einrobert1/status/1320069240494432260?s=21
1092	https://azop.hr/izrecene-upravne-novcane-kazne-u-ukupnom-iznosu-od-1-6-milijuna-kuna/
1093	https://azop.hr/izrecene-upravne-novcane-kazne-u-ukupnom-iznosu-od-1-6-milijuna-kuna/
1094	https://dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-meta-facebook-inquiry
1095	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9751137
1096	https://www.dataprotection.ro/?page=Comunicat_Presa_10_03_2022_3&lang=ro
1097	https://www.personuvernd.is/urlausnir/sofnun-personuupplýsinga-vegna-kaupa-a-adgongumida-a-vidburd-i-horpu-sektarakvordun
1098	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9751362 https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9751323
1099	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9754355
1100	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9751498
1101	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9754332
1102	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9751549
1103	https://www.datenschutz.bremen.de/sixcms/media.php/13/Pressemitteilung%20lfdl%20Bremen.pdf
1104	https://www.uodo.gov.pl/pl/138/2304 https://www.uodo.gov.pl/decyzje/DKN.5130.2215.2020
1105	https://www.uodo.gov.pl/pl/138/2304 https://uodo.gov.pl/decyzje/DKN.5130.2215.2020
1106	https://www.datatilsynet.dk/presse-og-nyheder/nyhedersarkiv/2022/mar/nationalt-genom-center-indstilles-til-boede https://ngc.dk/nyheder/2022/marts/datatilsynet
1107	https://www.dpa.gr/el/enimerwtiko/prakseisArxis/epiboli-dioikitikoy-prostimoy-se-ergodotria-gia-mi-ikanopoiisi
1108	https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/A6CFBF507FD03C3CC225880F004565E1/\$file/?????%20?????%20?????%2022-03-2022.pdf
1109	https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/A6CFBF507FD03C3CC225880F004565E1/\$file/?????%20ESSA%2021-03-2022.pdf
1110	https://www.dataprotection.ro/?page=Comunicat_Presa_25_03_2022_1&lang=ro
1111	https://www.dataprotection.ro/?page=Comunicat_Presa_28_03_2022&lang=ro

1112	https://www.imy.se/nyheter/sanktionsavgift-mot-klarna-efter-granskning/ https://www.imy.se/globalassets/dokument/beslut/2022/beslut-tillsyn-klarna.pdf
1113	https://edpb.europa.eu/news/national-news/2022/greek-sa-fine-imposed-employer-failure-satisfy-right-object-and-unlawful_en https://www.dpa.gr/sites/default/files/2022-03/12_2022anonym_0.pdf
1114	https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/apr/danske-bank-indstilles-til-boede
1115	https://www.independent.ie/business/technology/bank-of-ireland-fined-over-errors-reporting-details-of-47000-customers-loans-41522333.html#:~:text=Bank%20of%20Ireland%20has%20been,have%20affected%20their%20credit%20ratings https://www.rte.ie/news/business/2022/0405/1290503-bank-of-ireland-fined-by-dpc/
1116	https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-48-2022.pdf
1117	https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-47-2022.pdf
1118	https://www.autoriteprotectiondonnees.be/citoyen/controles-de-temperature-lapd-met-les-aeroports-de-zaventem-et-charleroi-a-lamende
1119	https://autoriteitpersoonsgegevens.nl/nl/nieuws/boete-voor-buitenlandse-zaken-visumaanvragen-slecht-beveiligd-informatie-over-delen https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit_bz_24_februari_2022_openbare_versie_d_efinitief.pdf
1120	https://www.dataprotection.ro/?page=Comunicat_Presa_07_04_2022&lang=ro
1121	https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-46-2022.pdf
1122	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9756853
1123	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9756869
1124	https://autoriteitpersoonsgegevens.nl/nl/nieuws/boete-belastingdienst-voor-zwarte-lijst-fsv https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit_boete_belastingdienst_fsv.pdf
1125	https://www.aepd.es/es/documento/ps-00043-2021.pdf
1126	https://www.dataprotection.ro/?page=Comunicat_Presa_18_04_2022&lang=ro
1127	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9762945
1128	https://www.aepd.es/es/documento/ps-00019-2022.pdf
1129	https://www.aepd.es/es/documento/ps-00476-2021.pdf
1130	https://www.aepd.es/es/documento/ps-00483-2021.pdf
1131	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9763051
1132	https://www.dpa.gr/el/enimerwtiko/prakseisArxis/epiboli-prostimoy-gia-synehizomeno-peristatiko-parabiasis-prosopikon
1133	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9761383
1134	https://www.aepd.es/es/documento/ps-00482-2021.pdf
1135	https://www.aepd.es/es/documento/ps-00603-2021.pdf
1136	https://www.cnil.fr/fr/fuite-de-donnees-de-sante-sanction-de-15-million-deuros-lencontre-de-la-societe-dedalus-biologie https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000045614368?init=true&page=1&query=san-2022-009&searchField=ALL&tab_selection=all
1137	https://www.dpa.gr/el/enimerwtiko/prakseisArxis/epiboli-prostimoy-gia-diabibasi-dedomenon-prosopikoy-harakтира-pros
1138	https://naih.hu/hatarozatok-vegzesek?download=513:szemelyes-adatok-nyilvanossagra-hozatala-online-tudakozoban
1139	https://www.aepd.es/es/documento/ps-00008-2022.pdf
1140	https://www.aepd.es/es/documento/ps-00533-2021.pdf
1141	https://www.aepd.es/es/documento/ps-00451-2021.pdf
1142	https://www.aepd.es/es/documento/ps-00199-2021.pdf
1143	https://www.aepd.es/es/documento/ps-00078-2022.pdf
1144	https://www.aepd.es/es/documento/ps-00323-2021.pdf
1145	https://www.dataprotection.ro/?page=Comunicat_Presa_03_05_2022&lang=ro
1146	https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/all/0F2FBFF02DD16959C2258833003EF69E/\$file/?????%20(??)%20Mediterranean%20Hospital.pdf?openelement
1147	https://www.aepd.es/es/documento/ps-00395-2021.pdf
1148	https://www.dataprotection.ro/?page=Comunicat_Presa_04_05_2022&lang=ro
1149	https://www.datatilsynet.no/contentassets/425ef2f0fb5e4af3ac8e0cd97da648b8/vedtak-om-overtredelsesgebyr---melding-om-avvik---lillestrom-kommune-sentraladministrasjonen.pdf

1150	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9767635
1151	https://www.auroriteprotectiondonnees.be/publications/decision-quant-au-fond-n-71-2022.pdf
1152	https://www.aepd.es/es/documento/ps-00534-2021.pdf
1153	https://www.aepd.es/es/documento/ps-00261-2021.pdf
1154	https://www.personuvernd.is/urlausnir/notkun-seesaw-nemendakerfisins-i-grunnskolum-reykjavikur-sektarakvordun-1
1155	https://www.aepd.es/es/documento/ps-00563-2021.pdf
1156	https://www.aepd.es/es/documento/ps-00037-2022.pdf
1157	https://www.aepd.es/es/documento/ps-00496-2021.pdf
1158	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9763968
1159	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9768363 https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9768702
1160	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9768387 https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9768702
1161	https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/maj/civilstyrelsen-indstilles-til-boede
1162	https://www.aepd.es/es/documento/ps-00579-2021.pdf
1163	https://www.dataprotection.ro/?page=Comunicat_Presa_12_05_2022&lang=ro
1164	https://www.aepd.es/es/documento/ps-00550-2021.pdf
1165	https://www.aepd.es/es/documento/ps-00539-2021.pdf
1166	https://www.aepd.es/es/documento/ps-00523-2021.pdf
1167	https://cnpd.public.lu/content/dam/cnpd/fr/decisions-fr/2022/decision-3fr-2022-sous-forme-anonymisee.pdf
1168	https://www.aepd.es/es/documento/ps-00267-2021.pdf
1169	https://naih.hu/hatarozatok-vegzesek?download=521:munkahelyi-kameras-megfigyeles-jogalapjanak-es-arrol-valo-tajekoztatasnak-jogszerusege
1170	https://www.dataprotection.ro/?page=Comunicat_Presa_18_05_2022&lang=ro
1171	https://www.dataprotection.ro/?page=Comunicat_Presa_17_05_2022&lang=ro
1172	https://www.aepd.es/es/documento/ps-00544-2021.pdf
1173	https://www.aepd.es/es/documento/ps-00061-2022.pdf
1174	https://www.aepd.es/es/documento/ps-00098-2022.pdf
1175	https://www.aepd.es/es/documento/ps-00519-2021.pdf
1176	https://www.aepd.es/es/documento/ps-00140-2020.pdf
1177	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9771574
1178	https://www.aepd.es/es/documento/ps-00583-2021.pdf
1179	https://www.aepd.es/es/documento/ps-00111-2022.pdf
1180	https://www.dataprotection.ro/?page=Comunicat_Presa_24_05_2022&lang=ro
1181	https://www.datatilsynet.no/contentassets/08439c79981a499f86fd9faebac1855d/20-02368-8-sladdet-versjon.pdf https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/avgjorelser-fra-datatilsynet/2022/gebyr-for-automatisk-videresending-av-e-post/
1182	https://www.aepd.es/es/documento/ps-00628-2021.pdf
1183	https://www.aepd.es/es/documento/ps-00513-2021.pdf
1184	https://www.aepd.es/es/documento/ps-00542-2021.pdf
1185	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9771545 https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9771607
1186	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9771529 https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9771607
1187	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9771122 https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9771607
1188	https://ico.org.uk/media/action-weve-taken/mpns/4019746/tuckers-mpn-20220228.pdf
1189	https://finlex.fi/fi/viranomaiset/tsv/2022/20221403
1190	https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2022/05/ico-fines-facial-recognition-database-company-clearview-ai-inc/ https://ico.org.uk/media/action-weve-taken/mpns/4020436/clearview-ai-inc-mpn-20220518.pdf

1191	https://www.autoriteprotectiondonnees.be/citoyen/enquete-cookies-sur-les-sites-de-presse-roularta-mis-a-lamende https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-85-2022.pdf
1192	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9774680
1193	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9776444
1194	https://www.aepd.es/es/documento/ps-00632-2021.pdf
1195	https://www.aepd.es/es/documento/ps-00516-2021.pdf
1196	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9776406
1197	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9771184
1198	https://www.dataprotection.ro/?page=Comunicat_Presa_03_06_2022&lang=ro
1199	https://www.aepd.es/es/documento/ps-00586-2021.pdf
1200	https://www.aepd.es/es/documento/ps-00608-2021.pdf
1201	https://www.dataprotection.ro/?page=Comunicat_Presa_08_06_2022&lang=ro
1202	https://www.aepd.es/es/documento/ps-00393-2021.pdf
1203	https://www.uodo.gov.pl/pl/138/2393 https://www.uodo.gov.pl/decyzje/DKN.5110.12.2021
1204	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9777200
1205	https://www.zaftda.de/tb-bundeslaender/hessen/landesdatenschutzbeauftragter-2/807-50-tb-lfd-hessen-2022-20-8296-vom-08-06-2022/file
1206	https://www.zaftda.de/tb-bundeslaender/hessen/landesdatenschutzbeauftragter-2/807-50-tb-lfd-hessen-2022-20-8296-vom-08-06-2022/file
1207	https://www.zaftda.de/tb-bundeslaender/hessen/landesdatenschutzbeauftragter-2/807-50-tb-lfd-hessen-2022-20-8296-vom-08-06-2022/file
1208	https://www.zaftda.de/tb-bundeslaender/hessen/landesdatenschutzbeauftragter-2/807-50-tb-lfd-hessen-2022-20-8296-vom-08-06-2022/file
1209	https://www.zaftda.de/tb-bundeslaender/hessen/landesdatenschutzbeauftragter-2/807-50-tb-lfd-hessen-2022-20-8296-vom-08-06-2022/file
1210	https://www.zaftda.de/tb-bundeslaender/berlin/802-tb-lfd-berlin-2021-ohne-drs-nr-vom-24-05-2022/file
1211	https://www.zaftda.de/tb-bundeslaender/berlin/802-tb-lfd-berlin-2021-ohne-drs-nr-vom-24-05-2022/file
1212	https://www.zaftda.de/tb-bundeslaender/berlin/802-tb-lfd-berlin-2021-ohne-drs-nr-vom-24-05-2022/file
1213	https://www.zaftda.de/tb-bundeslaender/berlin/802-tb-lfd-berlin-2021-ohne-drs-nr-vom-24-05-2022/file
1214	https://www.zaftda.de/tb-bundeslaender/berlin/802-tb-lfd-berlin-2021-ohne-drs-nr-vom-24-05-2022/file
1215	https://www.zaftda.de/tb-bundeslaender/berlin/802-tb-lfd-berlin-2021-ohne-drs-nr-vom-24-05-2022/file
1216	https://www.zaftda.de/tb-bundeslaender/berlin/802-tb-lfd-berlin-2021-ohne-drs-nr-vom-24-05-2022/file
1217	https://www.zaftda.de/tb-bundeslaender/berlin/802-tb-lfd-berlin-2021-ohne-drs-nr-vom-24-05-2022/file
1218	https://www.zaftda.de/tb-bundeslaender/berlin/802-tb-lfd-berlin-2021-ohne-drs-nr-vom-24-05-2022/file
1219	https://www.zaftda.de/tb-bundeslaender/berlin/802-tb-lfd-berlin-2021-ohne-drs-nr-vom-24-05-2022/file
1220	https://www.zaftda.de/tb-bundeslaender/berlin/802-tb-lfd-berlin-2021-ohne-drs-nr-vom-24-05-2022/file
1221	https://www.zaftda.de/tb-bundeslaender/berlin/802-tb-lfd-berlin-2021-ohne-drs-nr-vom-24-05-2022/file
1222	https://www.zaftda.de/tb-bundeslaender/berlin/802-tb-lfd-berlin-2021-ohne-drs-nr-vom-24-05-2022/file
1223	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9777127
1224	https://www.zaftda.de/tb-bundeslaender/brandenburg/landesdatenschutzbeauftragte/797-23-tb-lfd-brandenburg-2021-o-drs-nr-vom-09-05-2022/file
1225	https://www.zaftda.de/tb-bundeslaender/brandenburg/landesdatenschutzbeauftragte/797-23-tb-lfd-brandenburg-2021-o-drs-nr-vom-09-05-2022/file
1226	https://www.aepd.es/es/documento/ps-00591-2021.pdf
1227	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9779082
1228	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9779098
1229	https://www.zaftda.de/tb-bundeslaender/brandenburg/landesdatenschutzbeauftragte/797-23-tb-lfd-brandenburg-2021-o-drs-nr-vom-09-05-2022/file
1230	https://www.dataprotection.ro/?page=Comunicat_Presa_15_06_2022&lang=ro
1231	https://www.aepd.es/es/documento/ps-00327-2021.pdf
1232	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9779025

1233	https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-103-2022.pdf
1234	https://www.datatilsynet.no/contentassets/ac275106cc11481eaaf0dbd0d011a347/~-13262-20_02875-10-1-hoveddokument-308867_1_2.pdf
1235	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9779057
1236	https://www.aepd.es/es/documento/ps-00025-2022.pdf
1237	https://www.aepd.es/es/documento/ps-00585-2021.pdf
1238	https://www.dataprotection.ro/?page=Comunicat_Presa_20_06_2022_1&lang=ro
1239	https://www.dataprotection.ro/?page=Comunicat_Presa_20_06_2022_2&lang=ro
1240	https://www.aepd.es/es/documento/ps-00052-2022.pdf
1241	https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/jun/gyldendal-indstilles-til-boede
1242	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9782434
1243	https://www.uodo.gov.pl/pl/138/2401 https://www.uodo.gov.pl/decyzje/DKN.5131.51.2021
1244	https://naih.hu/hatarozatok-vezesek?download=517:mesterseges-intelligencia-alkalmazasanak-adatvedelmi-kerdesei
1245	https://www.aepd.es/es/documento/ps-00565-2021.pdf
1246	https://www.aepd.es/es/documento/ps-00192-2022.pdf
1247	https://www.aepd.es/es/documento/ps-00198-2022.pdf
1248	https://www.dataprotection.ro/?page=Comunicat_Presa_30_06_2022&lang=ro
1249	https://www.aepd.es/es/documento/ps-00313-2021.pdf
1250	https://ico.org.uk/media/action-weve-taken/mpns/4020812/the-tavistock-portman-nhs-foundation-trust-mpn.pdf https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/06/ico-sets-out-revised-approach-to-public-sector-enforcement/
1251	https://www.dpa.gr/sites/default/files/2022-07/28_2022%20anonym.pdf
1252	https://www.aepd.es/es/documento/ps-00593-2021.pdf
1253	https://www.aepd.es/es/documento/ps-00036-2022.pdf
1254	https://tietosuoja.fi/-/otavamedialle-seuraamusmaksu-puutteista-tietosuojaioikeuksien-toteutuksessa https://tietosuoja.fi/documents/6927448/105358665/TSV+Päätös+6097.161.21.pdf/0a52609b-43f2-30a5-2360-321651096f5a/TSV+Päätös+6097.161.21.pdf?t=1657013988942
1255	https://www.dpa.gr/el/enimerwtiko/prakseisArxis/epiboli-prostimoy-gia-paranomi-epexergasia-prosopikon-dedomenon-pros-ton
1256	https://www.dpa.gr/el/enimerwtiko/prakseisArxis/epiboli-prostimoy-gia-mi-ikanopoiisi-dikaiomatos-prosbasis-0
1257	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9784482
1258	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9784626
1259	https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2022/overtredsesgebyr-til-stortinget/ https://www.datatilsynet.no/contentassets/338d64f46fbb436aa61b0fc4d7b794da/stortinget-vedtak.pdf
1260	https://www.aepd.es/es/documento/ps-00611-2021.pdf
1261	https://www.aepd.es/es/documento/ps-00627-2021.pdf
1262	https://www.aepd.es/es/documento/ps-00609-2021.pdf
1263	https://www.cnil.fr/fr/prospection-commerciale-et-droits-des-personnes-sanction-de-1-million-deuros-lencontre-de https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000045975295?init=true&page=1&query=San-2022-011&searchField=ALL&tab_selection=all
1264	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9788970
1265	https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/1978BD92BBEDDA44C225887F002107BD?OpenDocument https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/1978BD92BBEDDA44C225887F002107BD/\$file/??????%20??????%20?.?.%20?????????.pdf
1266	https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/1978BD92BBEDDA44C225887F002107BD?OpenDocument
1267	https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/1978BD92BBEDDA44C225887F002107BD?OpenDocument https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/1978BD92BBEDDA44C225887F002107BD/\$file/??????%20????????%20?.?.%20?????????.pdf
1268	https://www.dpa.gr/el/enimerwtiko/prakseisArxis/epiboli-prostimoy-stin-etaireia-clearview-ai-inc
1269	https://www.uodo.gov.pl/decyzje/DKN.5131.27.2022
1270	https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/jul/sirius-advokater-indstilles-til-boede

1271	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9790111
1272	https://www.aepd.es/es/documento/ps-00630-2021.pdf
1273	https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/1978BD92BBEDDA44C225887F002107BD?OpenDocument https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/all/1978BD92BBEDDA44C225887F002107BD/\$file/?????%20??%20????????%20????????%20?????.pdf?openelement
1274	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9781947
1275	https://www.zaftda.de/tb-bundeslaender/brandenburg/landesdatenschutzbeauftragte/797-23-tb-lfd-brandenburg-2021-o-drs-nr-vom-09-05-2022/file
1276	https://www.zaftda.de/tb-bundeslaender/brandenburg/landesdatenschutzbeauftragte/797-23-tb-lfd-brandenburg-2021-o-drs-nr-vom-09-05-2022/file
1277	https://www.zaftda.de/tb-bundeslaender/brandenburg/landesdatenschutzbeauftragte/797-23-tb-lfd-brandenburg-2021-o-drs-nr-vom-09-05-2022/file
1278	https://www.garantepivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9556172
1279	https://www.zaftda.de/tb-bundeslaender/brandenburg/landesdatenschutzbeauftragte/797-23-tb-lfd-brandenburg-2021-o-drs-nr-vom-09-05-2022/file
1280	https://www.zaftda.de/tb-bundeslaender/brandenburg/landesdatenschutzbeauftragte/797-23-tb-lfd-brandenburg-2021-o-drs-nr-vom-09-05-2022/file
1281	https://www.zaftda.de/tb-bundeslaender/brandenburg/landesdatenschutzbeauftragte/797-23-tb-lfd-brandenburg-2021-o-drs-nr-vom-09-05-2022/file
1282	https://www.zaftda.de/tb-bundeslaender/hamburg/796-30-tb-lfd-hamburg-2021-o-drs-nr-vom-06-04-2022/file
1283	https://www.aepd.es/es/documento/ps-00080-2022.pdf
1284	https://www.aepd.es/es/documento/ps-00007-2022.pdf
1285	https://www.aepd.es/es/documento/ps-00580-2021.pdf
1286	https://www.aepd.es/es/documento/ps-00450-2021.pdf
1287	https://www.aepd.es/es/documento/ps-00422-2021.pdf
1288	https://www.aepd.es/es/documento/ps-00421-2021.pdf
1289	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9789899
1290	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9781242
1291	https://www.garantepivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9583865
1292	https://azop.hr/izrecene-dvije-upravne-novcane-kazne-u-ukupnom-iznosu-218-milijuna-kuna/
1293	https://azop.hr/izrecene-dvije-upravne-novcane-kazne-u-ukupnom-iznosu-218-milijuna-kuna/
1294	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9789564
1295	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9789541
1296	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9789409
1297	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9790365
1298	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9789972
1299	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9788986
1300	https://www.zaftda.de/tb-bundeslaender/hamburg/796-30-tb-lfd-hamburg-2021-o-drs-nr-vom-06-04-2022/file
1301	https://www.zaftda.de/tb-bundeslaender/hamburg/796-30-tb-lfd-hamburg-2021-o-drs-nr-vom-06-04-2022/file
1302	https://www.zaftda.de/tb-bundeslaender/hamburg/796-30-tb-lfd-hamburg-2021-o-drs-nr-vom-06-04-2022/file
1303	https://www.zaftda.de/tb-bundeslaender/hamburg/796-30-tb-lfd-hamburg-2021-o-drs-nr-vom-06-04-2022/file
1304	https://www.aepd.es/es/documento/ps-00394-2021.pdf
1305	https://lfd.niedersachsen.de/startseite/infotehk/presseinformationen/1-1-millionen-euro-bussgeld-gegen-volkswagen-213835.html
1306	https://cnpd.public.lu/content/dam/cnpd/fr/decisions-fr/2022/decision-12fr-2022-sous-forme-anonymisee.pdf
1307	https://cnpd.public.lu/content/dam/cnpd/fr/decisions-fr/2022/decision-13fr-2022-sous-forme-anonymisee.pdf
1308	https://www.aepd.es/es/documento/ps-00043-2022.pdf
1309	https://cnpd.public.lu/content/dam/cnpd/fr/decisions-fr/2022/decision-15fr-2022-sous-forme-anonymisee.pdf
1310	https://cnpd.public.lu/content/dam/cnpd/fr/decisions-fr/2022/decision-14fr-2022-sous-forme-anonymisee.pdf
1311	https://www.aepd.es/es/documento/ps-00005-2022.pdf

1312	https://www.aepd.es/es/documento/ps-00017-2022.pdf
1313	https://lfd.niedersachsen.de/startseite/infothek/presseinformationen/900-000-euro-bussgeld-gegen-kreditinstitut-wegen-profilbildung-zu-werbezwecken-213925.html
1314	https://www.aepd.es/es/documento/ps-00486-2021.pdf
1315	https://www.aepd.es/es/documento/ps-00290-2021.pdf
1316	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9719797
1317	https://uodo.gov.pl/decyzje/DKN.5131.34.2021 https://www.uodo.gov.pl/pl/138/2428
1318	https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000046070924?init=true&page=1&query=%2A&searchField=ALL&tab_selection=cnil https://www.cnil.fr/en/geolocation-rental-vehicles-ubeeqo-international-fined-175000-euros
1319	https://www.aepd.es/es/documento/ps-00613-2021.pdf
1320	https://www.aepd.es/es/documento/ps-00142-2022.pdf
1321	https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/avgjorelser-fra-datatilsynet/2022/gebyr-til-kroatjonnvegen-15-as/
1322	https://www.dataprotection.ro/?page=Comunicat_Presa_04_08_2022&lang=ro
1323	https://www.aepd.es/es/documento/ps-00622-2021.pdf
1324	https://www.aepd.es/es/documento/ps-00581-2021.pdf
1325	https://www.aepd.es/es/documento/ps-00105-2022.pdf
1326	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9794895
1327	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9678535
1328	https://www.dataprotection.ro/?page=Comunicat_Presa_09.08.2022_1&lang=ro
1329	https://www.aepd.es/es/documento/ps-00617-2021.pdf
1330	https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/aug/lolland-kommune-indstilles-til-boede
1331	https://www.dataprotection.ro/?page=Comunicat_Presa_09.08.2022&lang=ro
1332	https://www.aepd.es/es/documento/ps-00118-2022.pdf
1333	https://www.aepd.es/es/documento/ps-00086-2022.pdf
1334	https://www.aepd.es/es/documento/ps-00180-2022.pdf
1335	https://www.zaftda.de/tb-bundeslaender/niedersachsen/805-27-tb-lfd-niedersachsen-2021-o-dr-nr-vom-02-06-2022/file
1336	https://www.zaftda.de/tb-bundeslaender/niedersachsen/805-27-tb-lfd-niedersachsen-2021-o-dr-nr-vom-02-06-2022/file
1337	https://www.zaftda.de/tb-bundeslaender/niedersachsen/805-27-tb-lfd-niedersachsen-2021-o-dr-nr-vom-02-06-2022/file
1338	https://www.zaftda.de/tb-bundeslaender/niedersachsen/805-27-tb-lfd-niedersachsen-2021-o-dr-nr-vom-02-06-2022/file
1339	https://www.zaftda.de/tb-bundeslaender/sachsen/landesdatenschutzbeauftragter-6/804-22-tb-lfd-sachsen-2021-o-drs-nr-vom-25-05-2022/file
1340	https://www.zaftda.de/tb-bundeslaender/sachsen/landesdatenschutzbeauftragter-6/804-22-tb-lfd-sachsen-2021-o-drs-nr-vom-25-05-2022/file
1341	https://www.aepd.es/es/documento/ps-00124-2022.pdf
1342	https://www.zaftda.de/tb-bundeslaender/sachsen/landesdatenschutzbeauftragter-6/804-22-tb-lfd-sachsen-2021-o-drs-nr-vom-25-05-2022/file
1343	https://www.zaftda.de/tb-bundeslaender/sachsen/landesdatenschutzbeauftragter-6/804-22-tb-lfd-sachsen-2021-o-drs-nr-vom-25-05-2022/file
1344	https://www.zaftda.de/tb-bundeslaender/sachsen/landesdatenschutzbeauftragter-6/804-22-tb-lfd-sachsen-2021-o-drs-nr-vom-25-05-2022/file
1345	https://www.zaftda.de/tb-bundeslaender/schleswig-holstein/landesdatenschutzbeauftragter-8/790-40-tb-lfd-schleswig-holstein-2021-19-3545-vom-22-02-2022/file
1346	https://www.zaftda.de/tb-bundeslaender/schleswig-holstein/landesdatenschutzbeauftragter-8/790-40-tb-lfd-schleswig-holstein-2021-19-3545-vom-22-02-2022/file
1347	https://www.zaftda.de/tb-bundeslaender/schleswig-holstein/landesdatenschutzbeauftragter-8/790-40-tb-lfd-schleswig-holstein-2021-19-3545-vom-22-02-2022/file
1348	https://www.zaftda.de/tb-bundeslaender/schleswig-holstein/landesdatenschutzbeauftragter-8/790-40-tb-lfd-schleswig-holstein-2021-19-3545-vom-22-02-2022/file
1349	https://www.zaftda.de/tb-bundeslaender/saarland/landesdatenschutzbeauftragte-1/808-30-tb-lfd-saarland-2021-17-09-vom-22-06-2022/file

1350	https://www.zaftda.de/tb-bundeslaender/saarland/landesdatenschutzbeauftragte-1/808-30-tb-ldf-saarland-2021-17-09-vom-22-06-2022/file
1351	https://www.aepd.es/es/documento/ps-00618-2021.pdf
1352	https://www.inforights.im/media/2021/manx_care_penalty_notice_13july2022_web.pdf https://www.inforights.im/organisations/latest-news-updates/2022/aug/penalty-imposed-on-manx-care/
1353	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9718901
1354	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9681085
1355	https://www.aepd.es/es/documento/ps-00400-2021.pdf
1356	https://www.aepd.es/es/documento/ps-00089-2022.pdf
1357	https://www.aepd.es/es/documento/ps-00094-2022.pdf
1358	https://dataprotection.gov.sk/uouu/sites/default/files/sprava_o_stave_ochrany_osobnych_udajov_za_rok_2021.pdf
1359	https://dataprotection.gov.sk/uouu/sites/default/files/sprava_o_stave_ochrany_osobnych_udajov_za_rok_2021.pdf
1360	https://dataprotection.gov.sk/uouu/sites/default/files/sprava_o_stave_ochrany_osobnych_udajov_za_rok_2021.pdf
1361	https://www.cnil.fr/fr/prospection-commerciale-et-droits-des-personnes-sanction-de-600-000-euros-lencontre-daccor https://www.cnil.fr/sites/default/files/atoms/files/deliberation_de_la_formation_restreinte_no_san-2022-017_du_3_aout_2022_concernant_la_societe_accor_sa.pdf
1362	https://www.dpa.gr/el/enimerwtiko/prakseisArxis/epiboli-prostimoy-gia-ti-mi-lipsi-katallilon-tehnikon-organotikon-metron
1363	https://www.dpa.gr/el/enimerwtiko/prakseisArxis/epiboli-dioikitikoy-prostimoy-gia-paranomi-epexergasia-prosopikon
1364	https://www.aepd.es/es/documento/ps-00135-2022.pdf
1365	https://www.aepd.es/es/documento/ps-00070-2022.pdf
1366	https://www.aepd.es/es/documento/ps-00053-2022.pdf
1367	https://www.aepd.es/es/documento/ps-00029-2022.pdf
1368	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9794913
1369	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9795350
1370	https://www.dataprotection.ro/index.jsp?page=Comunicat_Presa_22_08_2022&lang=ro
1371	https://www.dataprotection.ro/?page=Comunicat_Presa_07_07_2022_02&lang=ro
1372	https://www.aepd.es/es/documento/ps-00626-2021.pdf
1373	https://edpb.europa.eu/system/files/2022-09/edpb_bindingdecision_20222_ie_sa_instagramchildusers_en.pdf https://dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-instagram-inquiry
1374	https://www.aepd.es/es/documento/ps-00151-2022.pdf
1375	https://www.aepd.es/es/documento/ps-00148-2022.pdf
1376	https://www.aepd.es/es/documento/ps-00346-2022.pdf
1377	https://www.dataprotection.ro/?page=Comunicat_Presa_29_08_2022&lang=ro
1378	https://www.aepd.es/es/documento/ps-00141-2022.pdf
1379	https://www.aepd.es/es/documento/ps-00278-2022.pdf
1380	https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/avgjorelser-fra-datatilsynet/2022/recover-as-far-overtredelsesgebyr/
1381	https://www.aepd.es/es/documento/ps-00069-2022.pdf
1382	https://www.cnil.fr/fr/sanction-de-250-000-euros-lencontre-dinfogreffe https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000046280956?init=true&page=1&query=san-2022-018&searchField=ALL&tab_selection=all
1383	https://www.aepd.es/es/documento/ps-00150-2022.pdf
1384	https://www.aepd.es/es/documento/ps-00071-2022.pdf
1385	https://www.dataprotection.ro/?page=Comunicat_Presa_09.09.2022&lang=ro
1386	https://www.aepd.es/es/documento/ps-00261-2022.pdf
1387	https://www.aepd.es/es/documento/ps-00178-2022.pdf
1388	https://www.aepd.es/es/documento/ps-00177-2022.pdf
1389	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9803345

1390	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9803309
1391	https://www.aepd.es/es/documento/ps-00050-2022.pdf
1392	https://www.aepd.es/es/documento/ps-00066-2022.pdf
1393	https://www.dataprotection.ro/?page=Comunicat_Presa_08_09_2022&lang=ro
1394	https://www.aepd.es/es/documento/ps-00100-2022.pdf
1395	https://www.aepd.es/es/documento/ps-00186-2022.pdf
1396	https://www.aepd.es/es/documento/ps-00521-2021.pdf
1397	https://www.aepd.es/es/documento/ps-00600-2021.pdf
1398	https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2022/20220920-BlnBDI-PM-Bussgeld-DSB.pdf
1399	https://www.baden-wuerttemberg.datenschutz.de/bussgeld-daten-aus-dem-grundbuch-stehen-nicht-zur-freien-verfuegung/
1400	https://www.aepd.es/es/documento/ps-00203-2022.pdf
1401	https://www.aepd.es/es/documento/ps-00115-2022.pdf
1402	https://www.aepd.es/es/documento/ps-00356-2022.pdf
1403	https://www.dataprotection.ro/?page=Comunicat_Presa_19_09_2022&lang=ro
1404	https://www.aepd.es/es/documento/ps-00379-2021.pdf
1405	https://www.uodo.gov.pl/decyzje/DKN.5131.29.2022
1406	https://naih.hu/hatarozatok-vegzesek?download=554:hangfelvetel-keszites-szerelesi-munkak-soran
1407	https://naih.hu/hatarozatok-vegzesek?download=557:erintetti-jogok-biztositasanak-serelme-a-vakcina-regisztracio-lekerdez-es-vakcinareg-neak-gov-hu-kapcsan
1408	https://www.baden-wuerttemberg.datenschutz.de/bussgeld-daten-aus-dem-grundbuch-stehen-nicht-zur-freien-verfuegung/
1409	https://www.dataprotection.ro/?page=Comunicat_Presa_22_09_2022&lang=ro
1410	https://www.aepd.es/es/documento/ps-00316-2022.pdf
1411	https://www.aepd.es/es/documento/ps-00093-2022.pdf
1412	https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2022/sep/hoersholm-kommune-idoemt-boede-paa-50000-kr
1413	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9809504
1414	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9810045
1415	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9809466
1416	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9809520
1417	https://www.aepd.es/es/documento/ps-00246-2022.pdf
1418	https://www.dsb.gv.at/dam/jcr:1360e98b-d22a-4a49-b3bd-6afca2f86d4c/Datenschutzbericht_2021.pdf
1419	https://www.dsb.gv.at/dam/jcr:1360e98b-d22a-4a49-b3bd-6afca2f86d4c/Datenschutzbericht_2021.pdf
1420	https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2021/aug/udlaendingestyrelsen-indstilles-til-boede
1421	https://www.aepd.es/es/documento/ps-00004-2022.pdf
1422	https://ico.org.uk/media/action-weve-taken/mpns/4021801/easylyfe-limited-mpn-Article-5-1-a-20221004.pdf https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/10/catalogue-retailer-easylyfe-fined-148-million/
1423	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9810028 https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9809282
1424	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9809998 https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9809282
1425	https://www.aepd.es/es/documento/ps-00145-2022.pdf
1426	https://www.aepd.es/es/documento/ps-00275-2022.pdf
1427	https://www.aki.ee/et/uudised/uudishimuparing-toi-vaarteotrahvi
1428	https://www.personuvernd.is/urlausnir/vinnsla-a-personuupplysingum-og-afgreidsla-adgangsbeidni-hja-hei-medical-travel-sektarakvordun-1
1429	https://www.aepd.es/es/documento/ps-00370-2022.pdf
1430	https://www.aepd.es/es/documento/ps-00595-2021.pdf
1431	https://www.aepd.es/es/documento/ps-00002-2022.pdf

1432	https://www.aepd.es/es/documento/ps-00401-2022.pdf
1433	https://www.aepd.es/es/documento/ps-00146-2022.pdf
1434	https://www.dataprotection.ro/?page=Comunicat_Presa_03.10.2022&lang=ro
1435	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9811361
1436	https://www.dataprotection.ro/?page=Comunicat_Presa_21_09_2022&lang=ro
1437	https://www.dpa.gr/sites/default/files/2022-09/47_2022%20anonym.pdf
1438	https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-127-2022.pdf
1439	https://www.dpa.gr/sites/default/files/2022-08/41_2022%20anonym.pdf
1440	https://naih.hu/hatarozatok-vegzesek?download=564:hitelbiralatot-megelozo-elobiralat-jogalapja-es-az-ahhoz-kapcsolodo-tajekoztatas
1441	https://www.aepd.es/es/documento/ps-00520-2021.pdf
1442	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9811300
1443	https://naih.hu/hatarozatok-vegzesek?download=570:egeszsegugyi-dokumentacio-masolatanak-kiadasa
1444	https://www.aepd.es/es/documento/ps-00352-2022.pdf
1445	https://www.garantepivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9809201
1446	https://www.aepd.es/es/documento/ps-00101-2022.pdf
1447	https://www.aepd.es/es/documento/ps-00567-2021.pdf
1448	https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000046444859?isSuggest=true https://www.cnil.fr/en/facial-recognition-20-million-euros-penalty-against-clearview-ai
1449	https://www.dataprotection.ro/index.jsp?page=Comunicat_Presa_18_10_2022&lang=ro
1450	https://www.dataprotection.ro/index.jsp?page=Comunicat_Presa_18_10_2022&lang=ro
1451	https://www.aepd.es/es/documento/ps-00188-2022.pdf
1452	https://www.garantepivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9815745
1453	https://www.dpa.gr/el/enimerwtiko/prakseisArxis/epiboli-prostimoy-gia-mi-ikanopoiisi-dikaiomatos-prosbasis-se-yliko
1454	https://www.dpa.gr/index.php/el/enimerwtiko/prakseisArxis/epiboli-dioikitikoy-prostimoy-gia-leitoyrgia-systimatos-binteopitirisis
1455	https://www.dpa.gr/el/enimerwtiko/prakseisArxis/epexergasia-dedomenon-meso-pistotikhreostikon-karton-apo-tin-trapeza-1
1456	https://www.dpa.gr/el/enimerwtiko/prakseisArxis/epexergasia-dedomenon-meso-pistotikhreostikon-karton-apo-tin-trapeza-0
1457	https://www.dpa.gr/el/enimerwtiko/prakseisArxis/epexergasia-dedomenon-meso-pistotikhreostikon-karton-apo-tin-trapeza
1458	https://www.dpa.gr/el/enimerwtiko/prakseisArxis/epexergasia-dedomenon-meso-pistotikhreostikon-karton-apo-tin-ethniki
1459	https://www.aepd.es/es/documento/ps-00219-2022.pdf
1460	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9815947
1461	https://ico.org.uk/media/action-weve-taken/mpns/4021951/interserve-group-limited-monetary-penalty-notice.pdf https://ico.org.uk/action-weve-taken/enforcement/interserve-group-limited/
1462	https://www.garantepivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9817058
1463	https://www.garantepivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9811271
1464	https://www.garantepivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9811732
1465	https://www.garantepivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9813326
1466	https://www.aepd.es/es/documento/ps-00108-2022.pdf
1467	https://www.aepd.es/es/documento/ps-00212-2022.pdf
1468	https://www.aepd.es/es/documento/ps-00354-2022.pdf
1469	https://www.garantepivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9815665
1470	https://www.aepd.es/es/documento/ps-00099-2022.pdf
1471	https://www.aepd.es/es/documento/ps-00047-2022.pdf
1472	https://www.aepd.es/es/documento/ps-00104-2022.pdf
1473	https://www.garantepivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9795404

1474	https://www.aepd.es/es/documento/ps-00341-2022.pdf
1475	https://www.aepd.es/es/documento/ps-00134-2022.pdf
1476	https://www.aepd.es/es/documento/ps-00117-2022.pdf
1477	https://www.aepd.es/es/documento/ps-00375-2022.pdf
1478	https://www.aepd.es/es/documento/reposicion-ps-00183-2022.pdf
1479	https://www.dataprotection.ro/?page=Comunicat_Presa_07_11_2022&lang=ro
1480	https://www.aepd.es/es/documento/ps-00164-2022.pdf
1481	https://www.dataprotection.ro/?page=Comunicat_Presa_08_11_2022&lang=ro
1482	https://www.dataprotection.ro/?page=Comunicat_Presa_09.11.2022&lang=ro
1483	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9817535
1484	https://www.aepd.es/es/documento/ps-00097-2022.pdf
1485	https://www.aepd.es/es/documento/ps-00211-2022.pdf
1486	https://www.aepd.es/es/documento/ps-00555-2021.pdf
1487	https://www.aepd.es/es/documento/ps-00280-2022.pdf
1488	https://www.aepd.es/es/documento/ps-00060-2022.pdf
1489	https://www.aepd.es/es/documento/ps-00256-2022.pdf
1490	https://www.aepd.es/es/documento/ps-00419-2022.pdf
1491	https://www.aepd.es/es/documento/ps-00310-2022.pdf
1492	https://www.aepd.es/es/documento/ps-00634-2021.pdf
1493	https://naih.hu/hatarozatok-vezesek?download=573:kozvetlen-uzletszeressel-kapcsolatos-adatkezes-jogszerusege
1494	https://www.uodo.gov.pl/decyzje/DKN.5131.8.2022 https://uodo.gov.pl/pl/138/2487
1495	https://www.dataprotection.ro/?page=Comunicat_Presa_16_11_2022&lang=ro
1496	https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000046562676?init=true&page=1&query=discord%20inc&searchField=ALL&tab_selection=all https://www.cnil.fr/fr/sanction-de-800-000-euros-lencontre-de-la-societe-discord-inc
1497	https://www.dataprotection.ro/?page=Comunicat_Presa_18_11_2022&lang=ro
1498	https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/122026 https://www.cnpd.pt/comunicacao-publica/noticias/cnpd-aplica-primeira-sancao-por-falta-de-epd/
1499	https://www.aepd.es/es/documento/ps-00161-2022.pdf
1500	https://www.dataprotection.ro/index.jsp?page=Comunicat_Presa_21_11_2022&lang=ro
1501	https://www.dataprotection.ro/?page=Comunicat_Presa_24_11_2022&lang=ro
1502	https://dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-in-facebook-data-scraping-inquiry https://www.theguardian.com/technology/2022/nov/28/meta-fined-265m-over-data-breach-affecting-more-than-500m-users
1503	https://www.dataprotection.ro/?page=Comunicat_Presa_25_11_2022&lang=ro
1504	https://www.aepd.es/es/documento/ps-00378-2022.pdf
1505	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9826417 https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9826440
1506	https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000046650733?isSuggest=true https://www.cnil.fr/fr/prospection-commerciale-et-droits-des-personnes-sanction-de-600-000-euros-lencontre-dedf
1507	https://www.aepd.es/es/documento/ps-00335-2022.pdf
1508	https://www.aepd.es/es/documento/ps-00113-2022.pdf
1509	https://www.aepd.es/es/documento/ps-00262-2022.pdf
1510	https://www.aepd.es/es/documento/ps-00322-2022.pdf
1511	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9828901
1512	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9827402
1513	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9827119
1514	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9826440 https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9819792
1515	https://www.aepd.es/es/documento/ps-00404-2022.pdf

1516	https://www.aepd.es/es/documento/ps-00264-2022.pdf
1517	https://www.aepd.es/es/documento/ps-00438-2022.pdf
1518	https://www.aepd.es/es/documento/ps-00485-2021.pdf
1519	https://www.dataprotection.ie/sites/default/files/uploads/2022-03/Final%20Decision%20in%20Inquiry%20IN-19-7-5_Slane%20Credit%20Union.pdf
1520	https://www.dataprotection.ro/?page=Comunicat_Presa_09_12_2022&lang=ro
1521	https://www.aepd.es/es/documento/ps-00240-2022.pdf
1522	https://www.aepd.es/es/documento/ps-00459-2022.pdf
1523	https://www.aepd.es/es/documento/ps-00143-2022.pdf
1524	https://www.cnpd.pt/comunicacao-publica/noticias/cnpd-sanciona-ine-por-cinco-contrordenacoes/ https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/122033
1525	https://www.aepd.es/es/documento/ps-00296-2022.pdf
1526	https://tietosuojafi/-/viking-linelle-seuraamusmaksu-tyontekijoiden-terveystietojen-lainvastasesta-kasittelysta https://tietosuojafi/documents/6927448/105358665/P%C3%A4%C3%A4t%C3%B6s_8492.163.2020.pdf/ff41c103-ee7-c4f2-810f-ea19dd15a7d9/P%C3%A4%C3%A4t%C3%B6s_8492.163.2020.pdf?t=1671004323352
1527	https://www.cnil.fr/fr/securite-des-donnees-et-droits-des-personnes-sanction-de-300-000-euros-lencontre-de-la-societe-free https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000046693390?init=true&page=1&query=san-2022-022&searchField=ALL&tab_selection=all
1528	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9828965
1529	https://www.aepd.es/es/documento/ps-00295-2022.pdf
1530	https://www.aepd.es/es/documento/ps-00290-2022.pdf
1531	https://www.dataprotection.ro/?page=Comunicat_Presa_15_12_2022&lang=ro
1532	https://www.aepd.es/es/documento/ps-00204-2022.pdf
1533	https://www.aepd.es/es/documento/ps-00344-2022.pdf
1534	https://www.aepd.es/es/documento/ps-00272-2022.pdf
1535	https://www.aepd.es/es/documento/ps-00125-2022.pdf
1536	https://www.aepd.es/es/documento/ps-00566-2021.pdf
1537	https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9833616 https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9833530
1538	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9834986
1539	https://www.dataprotection.ro/?page=Comunicat_Presa_22_12_2022&lang=ro
1540	https://www.dataprotection.ro/?page=Comunicat_Presa_27_12_2022&lang=ro
1541	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9832979 https://www.gdpd.it/home/docweb/-/docweb-display/docweb/9834373
1542	https://www.gdpd.it/web/guest/home/docweb/-/docweb-display/docweb/9832838 https://www.gdpd.it/home/docweb/-/docweb-display/docweb/9834373
1543	https://dataprotection.ie/en/news-media/data-protection-commission-announces-conclusion-two-inquiries-meta-ireland
1544	https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9834477
1545	https://www.dataprotection.ro/?page=Comunicat_Presa_03_01_2023&lang=ro
1546	https://www.dataprotection.ro/?page=Comunicat_Presa_04.01.2023&lang=ro
1547	https://www.aepd.es/es/documento/ps-00376-2022.pdf
1548	https://www.aepd.es/es/documento/ps-00169-2022.pdf
1549	https://www.aepd.es/es/documento/ps-00342-2022.pdf
1550	https://www.aepd.es/es/documento/ps-00126-2022.pdf
1551	https://www.aepd.es/es/documento/ps-00436-2022.pdf

Annex 5 – GDPR Articles addressed in the DPPA

Mapping of GDPR Articles requiring PbDD implementation.

The following table lists the GDPR Articles addressed by the DPPA that must be considered in the implementation of PbDD (operationalisation of the GDPR):

GDPR Article	Addressing
5	Principles relating to personal data processing
6	Lawfulness of processing
7	Conditions for consent
8	Conditions applicable to child's consent in relation to information society services
9	Processing of special categories of personal data
10	Processing of data relating to criminal convictions and offences
12	Transparent information, communication, and modalities for exercising the rights of the data subject
13	Information to be provided where personal data are collected from the data subject
14	Information to be provided where personal data have not been obtained from the data subject
15	Right of access by the data subject
16	Right to rectification
17	Right to erasure ("right to be forgotten")
18	Right to restriction of processing
19	Notification obligation regarding rectification or erasure of personal data or restriction of processing
20	Right to data portability

21	Right to object
22	Automated individual decision-making, including profiling
23	Restrictions
24	Responsibility of the controller
25	Data protection by design and by default
26	Joint controllers
27	Representatives of controllers or processors not established in the Union
28	Processor
29	Processing under the authority of the controller or processor
30	Records of processing activities
32	Security of processing
33	Notification of a personal data breach to the supervisory authority
34	Communication of a personal data breach to the data subject
35	Data protection impact assessment
36	Prior consultation
37	Designation of the data protection officer
38	Position of the data protection officer
39	Tasks of the data protection officer
44	General principle for transfers
45	Transfers on the basis of an adequacy decision
46	Transfers subject to appropriate safeguards
47	Binding corporate rules
48	Transfers or disclosures not authorised by Union law
49	Derogations for specific situations

89	Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes
91	Existing data protection rules of churches and religious associations

ANNEX 6 - ETHICS REVIEW APPLICATION FORM

To be used for School or University level review

Please append all relevant and supporting documentation to this project application form when submitting for School level (SREC) or University (UREC) review. Text boxes will expand as required and all language used to explain or justify the application should be comprehensible to a lay person.

Application form and all associated documents should be submitted electronically.

Submission deadline dates for UREC can be found on the [UREC webpage](#).

Section 1: APPLICATION DETAILS

1.1 PROJECT AND DATES				
Title	Putting Privacy by Design and by Default in Practice: Unveiling the internal inconsistencies of the General Data Protection Regulation (GDPR) and propounding solutions			
Date of submission	06/04/2021			
Start date	01/04/2021			
End date	End of doctoral thesis			
1.2 APPLICANT DETAILS				
Chief Investigator	Prof. Stavroula Karapapa			
Please note that an undergraduate or postgraduate student cannot be a named Chief Investigator for research ethics purposes. The supervisor must be declared as Chief Investigator.				
Is the project being carried out in whole or in part to support a student degree?				
<input checked="" type="checkbox"/> Yes <input type="checkbox"/> Undergraduate <input type="checkbox"/> Masters <input checked="" type="checkbox"/> PhD				
<input type="checkbox"/> No				
School	Law			
Department	N/A			
Email	s.karapapa@essex.ac.uk			
Telephone				
All other Applicants	Name:	School	Position	Email
	Virgilio Emanuel Lobato Cervantes	Law	Ph.D. Student	v.lobatocervantes@pgr.reading.ac.uk
	Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.

1.3 WHAT REVIEW IS NEEDED?

Please tick the appropriate box below to confirm which review your ethics application requires.

Please tick all that apply.

School Level Review (SREC)

External (for example, HRA)

University Research Ethics Committee Review (UREC)

Projects expected to require review by the University Research Ethics Committee (for example; research involving NHS patients, research involving potential for distress to participants) must be reviewed by the Chair of the School Ethics Committee or the Head of School before submission to UREC. For further information see Section 16 of the [UREC Guidance](#).

1.4 EXTERNAL RESEARCH ETHICS COMMITTEES

Please provide details of other external research ethics committees from whom a favourable ethics opinion will be required (for example; HRA REC)

Name of Committee	Date of submission / approval	Reference	Status
Click here to enter text.	Click here to enter a date.	Click here to enter text.	Click here to enter text.

1.5 PROJECT SUBMISSION DECLARATION

On behalf of my co-applicants and myself,

- I confirm that to the best of my knowledge I have made known all information relevant to the appropriate Research Ethics Committee and I undertake to inform the Committee(s) of any such information which subsequently becomes available whether before or after the research has begun
- I understand that it is a legal requirement that both staff and students undergo Disclosure and Barring Service checks when in a position of trust (for example, when working with children or vulnerable adults)
- I confirm that if this project is an intervention study, a list of names and contact details of the participants in this project will be compiled and that this, together with a copy of the Consent Form, will be retained within the School for as long as necessary.
- I confirm that I have given due consideration to equality and diversity in the management, design and conduct of the research project.
- (For Chemistry, Food & Pharmacy (CFP) only) I confirm the Internal Review has been undertaken by Click here to enter text. and I have made the changes requested.

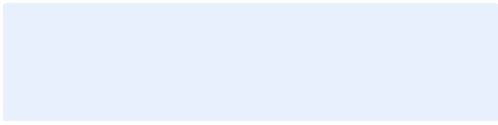
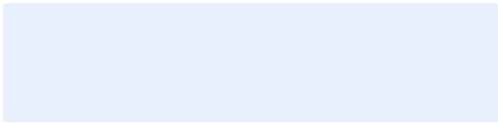
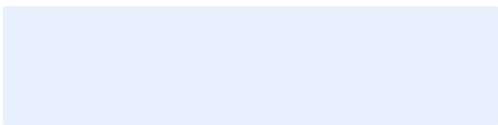
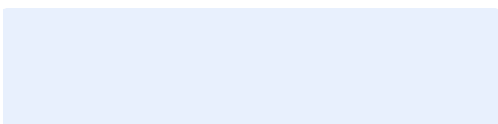
SIGNED, CHIEF INVESTIGATOR

06/04/2021

Where required by the School's Research Ethics Procedures, this ethics application should be signed off by the appropriate person to confirm the School Body are content for this application to be reviewed by UREC.

Chemistry, Food & Pharmacy – will require sign off from: Chair of SREC, Head of Department and School Ethics Administrator – insert rows below as required.

SIGNED, AUTHORISING SIGNATORY

Signature:	Position:	Date:
	Choose an item.	Click here to enter a date.
	Choose an item.	Click here to enter a date.
	Choose an item.	Click here to enter a date.
	Choose an item.	Click here to enter a date.

Section 2: PROJECT DETAILS

2.1 LAY SUMMARY

Please provide a summary of the project in plain English that can be understood by a non-specialist audience, which includes a description of the background of the study (existing knowledge), the questions the project will address, the methods to be used and the key ethical issues.

Please note the lay summary should not contain references and be no more than 500 words.

My Thesis investigates GDPR's internal inconsistencies and external constraints, towards the realization of Privacy by Design and Privacy by Default (PbDD). It also looks at how the rights to privacy and data protection have been accosted by the emerging of new data processing paradigms such as big-data analytics, digital marketing targeting and profiling, and "new to the world" technologies. The 'operationalisation' of the law – bridging and incorporating legal requirements into information systems and contemporary business operations – as mandated by Article 25 GDPR, has been flagged by many scholars, practitioners, and organisations as one task of very difficult accomplishment. I investigate whether the contemporary technical and organisational practicalities involving the electronic processing of personal data, which not always seem to be compatible with the PbDD measures prescribed by the Regulation, are aspects that impede, de facto, organisations from achieving compliance. I also investigate whether some aspects of the law have become unduly complex, resulting in the occasional impossibility of its practical application. **The question the project will address is:** 'On the basis of the provisions of the GDPR, it is feasible to incorporate PbDD into the contemporary business systems and operations? 'If so, which is the appropriate model (or conceptual framework) to effectively protect personal data at the standard required by the GDPR?.

The methodology of my work is mainly doctrinal, build upon the study of legislation and case law, and informed by literature focusing on the theories of privacy and data protection law.

Empirical methods: Correlational research: The correlation coefficient indicates the correlation between two variables, a value measured between -1 and +1. When the correlation coefficient is close to +1, there is a positive correlation between the two variables. If the value is close to -1, there is a negative correlation between the two variables. When the value is close to zero, then there is no relationship between the two variables.

The aim of integrating correlational analysis in this study is to find out whether there is either a positive correlation - when the number of fines increases, issues related with the application of PbDD also increases (both variables change in the same direction), a negative correlation - when the number of fines increases, issues related with the application of PbDD decreases (the variables change in opposite directions), or a zero correlation – when the number of fines issued by EU supervisory authorities is not correlated with the application of PbDD.

This quantitative statistical analyse of data solely intends to find out if there is a relationship between two variables, it will not find a causal relationship between them.

Hypothesis included in the scientific research method:

H1= An ineffective application of PbDD makes unviable businesses' compliance with the GDPR.

H2= The operationalisation of PbDD is not feasible in the context of the current GDPR accountability (risk-based) approach.

H3= The operationalisation of PbDD is possible if integrated in a more stringent DPPA framework.

2.2 PRIMARY RESEARCH QUESTION

Please detail the primary research question this project will answer.

On the basis of the provisions of the GDPR, it is feasible to incorporate Privacy by Design and by Default into the contemporary business systems and operations? If so, which is the appropriate model (or conceptual framework) to effectively protect personal data at the standard required by the GDPR?

2.3 SECONDARY RESEARCH QUESTION(S)

Please detail any secondary research question(s) this project will answer.

By sampling and analysing research data, based on qualitative interpretations, the researcher intends to identify the main issues beyond the practical application of PbDD – and more generally, beyond the practical application of GDPR - by asking: What are the most current GDPR violations leading to the application of a fine by a SA? Are those violations related to an unsuccessful application of the GDPR requirements into the business operations, namely, PbDD? If so, it is possible to determine with scientific rigour, what are the technical and organisational faults, or weaknesses, leading to the application of such fines? What are the sectors of economic activity attracting a higher number of fines? It is possible to track down the type of transgression over a set period of time and identify non-compliance trends? Are most violations related to the online processing of personal data, linked to the use of new technologies, arising from poor data processing practices (including information security), or lack of understanding of the Regulation? Perhaps, such faults emerge from the impossibility, or impracticability, of application of the data protection principles and GDPR requirements into the businesses systems, processes, and operations?

2.4 DESIGN AND PROCEDURE

Please describe concisely what the study will involve, how many times and in what order, for your participants and the procedures and methodology to be used.

Note: Any questionnaires or interview scripts should be appended to this application.

Apart from literature review and documentary research, the study will involve the collection and analysis of aggregated data sets (fines issued by EU supervisory authorities under the GDPR) obtained directly from the European Data Protection Board (EDPB) and/or EU supervisory authorities. This is publicly available data:

Methodology	Methods applied	Population	Sampling approach	Sampling dimension
Quantitative method	Self-completion spreadsheets and	EU supervisory authorities (SA's)	Targeted sampling	[pre-determined number (>500)] of fines and

	relational databases (correlational research)	European Data Protection Board (EDPB)		penalties which data protection authorities within the EU have imposed under the GDPR
--	---	---------------------------------------	--	---

2.5 LOCATION

Please describe where the research will take place.

United Kingdom

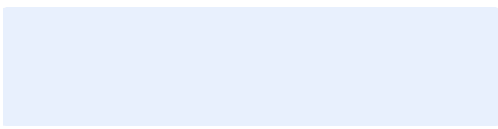
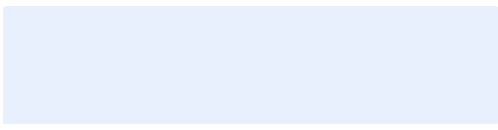
Please state whether an appropriate risk assessment/ local review has been undertaken.

- Yes
 No
 Not required

Note:

- Ensure specific risk assessments have been undertaken for non-University locations (for example; schools or participant homes). Please consult either your School Ethics Contact or UREC for guidance.

If the project is to take place in Hugh Sinclair Unit of Human Nutrition, it must be reviewed by the Research Nurses and the Hugh Sinclair Manager also informed that the ethics application is being submitted for the study.' Signatures are required below.

	Hugh Sinclair Manager	Click here to enter a date.
	Research Nurse <i>Click here to enter text.</i>	Click here to enter a date.

2.6 FUNDING

Is the research supported by funding from a research council or other external source (for example; charities, businesses)?

- Yes
 No

If "yes", please,

- (a) Give details of the funding body;

[Click here to enter text.](#)

(b) Confirm if the funder specifically stipulates review by the University Research Ethics Committee.

Yes

No

2.7 ETHICAL ISSUES

Please summarise the main ethical issues, including harms and risks, arising from your study and explain how you have addressed them.

The main ethical issue for the research would be unintentional 'plagiarism', where the researcher shall be very cautious on, namely by resorting to an automated referencing system called "Zotero". Regarding the empirical research, the main ethical issue would be the processing of personal data, where GDPR fines are issued to individuals (i.e. sole traders), here, the researcher will proceed to the anonymization of any personal data included in the data sets received from the EDPB/SA's. The researcher will address all information with automated credit/citation from the textbooks and legal sources (Zotero) and data sets received from the EDPB/SA's shall remain confidential and anonymous and shall be used only for the research purposes.

2.8 DECEPTION

Will the research involve any element of intentional deception (for example; providing false or misleading information about the study)?

Yes

No

If "yes", please justify and append a description of the debriefing procedure.

Click here to enter text.

2.9 PAYMENT

Will research participants receive any payments, reimbursement of expenses or any other benefits or incentives for taking part in this research?

Yes

No

If "yes", please specify and justify the amount.

2.10 DATA PROTECTION

This section is required for applications reviewed at School (SREC) level only.

For applications reviewed at UREC level, do not complete this section. Move onto section 2.11.

What steps will be taken to ensure appropriate secure handling of personal data? Give comprehensive details on the collection, retention, sharing and disposal of participant personal data.

Personal data means any data relating to a participant who could potentially be identified. It includes pseudonymised data capable of being linked to a participant through a unique code number.

For guidance on data protection please, see the [Data Protection for Researchers Guidance](#) document.

Data collected from the EDBP and supervisory authorities is anonymised data. The storage of research data is in the Office 365 platform (OneDrive) provided by the University of Reading to their students.

The UK GDPR does not apply to personal data that has been anonymised. Recital 26 explains that:

“...The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.”

2.11 DATA MANAGEMENT PLAN

Requirement for applications to be submitted to UREC, only.

Applications submitted to UREC must be accompanied by a [Data Management Plan](#) (document available via link).

Please append the Data Management Plan.

- N/A, application not to be submitted to UREC
 Yes, appended*

*Please note; as the Data Management Plan is appended there is **no** requirement to complete section 2.10 Data Protection.

2.12 DATA PROTECTION IMPACT ASSESSMENT (DPIA)

Will the research involve any activity that requires a [Data Protection Impact Assessment](#) (DPIA)?

- Yes
 No

If “yes”, please append the “[Pre-Screening Questionnaire for Data Protection Impact Assessment](#)”.

Please note; the Pre-Screening Questionnaire for a DPIA is only accessible with staff credentials and the Chief Investigator is responsible for its completion.

2.13 INFORMED CONSENT

a. Will you obtain informed consent from, or on behalf of, research participants?

- Yes (go to question b)
 No (go to question c)

b. If “yes”, please describe the process by which they will be informed about the nature of the study and the process by which you will obtain consent.

c. If “no”, you are not obtaining consent, please explain why (for example; ‘opt-out’ methodology without the acquisition of consent)?

Please append all relevant participant facing information documentation for participants, parents or guardians. Please note, age-appropriate information sheets must be supplied for all participants wherever possible, including children. Assent should be obtained from children, under 16 years, in addition to the consent required from parents, guardians or carers.

N/A. - Data processed is only publicly available data - details of fines and penalties which data protection authorities within the EU have imposed under the EU General Data Protection Regulation.

2.14 GENOTYPING

Are you intending to genotype the participants?

- Yes
 No

If "yes", which genotypes will be determined?

Click here to enter text.

Section 3: PARTICIPANT DETAILS

3.1 PARTICIPANT NUMBER

How many participants do you plan to recruit?

Please briefly explain why the number is appropriate to answer the study's research question(s).

My principal concern is that secondary data (data that has already been collected through primary sources and made readily available for researchers to use for their own research) used in my research remained up to date, rigorous and sufficient flexible for application into different analysis approaches throughout my study. As such, I could not think of a better source than an independent body, which contributes to the consistent application of data protection rules throughout the European Union - the European Data Protection Board (EDPB) - as the provider of the data sets used to validate my research findings. The EDPB is formed by a representative of the supervisory authority of each Member States together with a representative of the European Data Protection Supervisor (EDPS), as such has privileged access to crucial raw data, as well as the data transformation means to provide such information in a suitable format. The UK has left the EU on the 31 December 2020. However, the EU GDPR was integrated into domestic law (UK GDPR, aside the Data Protection Act 2018). As such, UK data is directly sourced from the Information Commissioner's Office (ICO).

The following SA's may be also contacted for the purposes of this research:

Austria

*Österreichische Datenschutzbehörde
Hohenstaufengasse 3
1010 Wien
Tel. +43 1 531 15 202525
Fax +43 1 531 15 202690
dsb@dsb.gv.at
<http://www.dsb.gv.at/>*

Belgium

*Commission de la protection de la vie privée
Commissie voor de bescherming van de persoonlijke levenssfeer
Rue de la Presse 35 / Drukpersstraat 35
1000 Bruxelles / 1000 Brussel
Tel. +32 2 274 48 00
Fax +32 2 274 48 35
commission@privacycommission.be
<http://www.privacycommission.be/>*

Bulgaria

*Commission for Personal Data Protection
2, Prof. Tsvetan Lazarov blvd.
Sofia 1592
Tel. +359 2 915 3580
Fax +359 2 915 3525
kzld@cpdp.bg
<http://www.cdpd.bg/>*

Croatia
Croatian Personal Data Protection Agency
Martićeva 14
10000 Zagreb
Tel. +385 1 4609 000
Fax +385 1 4609 099
azop@azop.hr or info@azop.hr
<http://www.azop.hr/>

Cyprus
Commissioner for Personal Data Protection
1 Iasonos Street,
1082 Nicosia
P.O. Box 23378, CY-1682 Nicosia
Tel. +357 22 818 456
Fax +357 22 304 565
commissioner@dataprotection.gov.cy
<http://www.dataprotection.gov.cy/>

Czech Republic
The Office for Personal Data Protection
Urad pro ochranu osobnich udaju
Pplk. Sochora 27
170 00 Prague 7
Tel. +420 234 665 111
Fax +420 234 665 444
posta@uouu.cz
<http://www.uouu.cz/>

Denmark
Datatilsynet
Borgergade 28, 5
1300 Copenhagen K
Tel. +45 33 1932 00
Fax +45 33 19 32 18
dt@datatilsynet.dk
<http://www.datatilsynet.dk/>

Estonia
Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon)
Väike-Ameerika 19
10129 Tallinn
Tel. +372 6274 135
Fax +372 6274 137
info@aki.ee
<http://www.aki.ee/en>

Finland
Office of the Data Protection Ombudsman
P.O. Box 315
FIN-00181 Helsinki
Tel. +358 10 3666 700
Fax +358 10 3666 735
tietosuoja@om.fi
<http://www.tietosuoja.fi/en/>

France
Commission Nationale de l'Informatique et des Libertés – CNIL
8 rue Vivienne, CS 30223
F-75002 Paris, Cedex 02
Tel. +33 1 53 73 22 22
Fax +33 1 53 73 22 00
<http://www.cnil.fr/>

Germany
Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Husarenstraße 30
53117 Bonn
Tel. +49 228 997799 0; +49 228 81995 0
Fax +49 228 997799 550; +49 228 81995 550
poststelle@bfdi.bund.de
<http://www.bfdi.bund.de/>

Greece
Hellenic Data Protection Authority
Kifisias Av. 1-3, PC 11523
Ampelokipi Athens
Tel. +30 210 6475 600
Fax +30 210 6475 628
contact@dpa.gr
<http://www.dpa.gr/>

Hungary
National Authority for Data Protection and Freedom of Information
Szilágyi Erzsébet fasor 22/C
H-1125 Budapest
Tel. +36 1 3911 400
peterfalvi.attila@naih.hu
<http://www.naih.hu/>

Ireland
Data Protection Commissioner
Canal House
Station Road
Portllington
Co. Laois
Lo-Call: 1890 25 22 31
Tel. +353 57 868 4800
Fax +353 57 868 4757
info@dataprotection.ie
<http://www.dataprotection.ie/>

Italy
Garante per la protezione dei dati personali
Piazza di Monte Citorio, 121
00186 Roma
Tel. +39 06 69677 1
Fax +39 06 69677 785
garante@garanteprivacy.it
<http://www.garanteprivacy.it/>

Latvia
Data State Inspectorate
Director: Ms Daiga Avdejanova
Blaumana str. 11/13-15
1011 Riga
Tel. +371 6722 3131
Fax +371 6722 3556
info@dvi.gov.lv
<http://www.dvi.gov.lv/>

Lithuania
State Data Protection
Žygimantų str. 11-6a
011042 Vilnius
Tel. +370 5 279 14 45
Fax +370 5 261 94 94
ada@ada.lt
<http://www.ada.lt/>

Luxembourg
Commission Nationale pour la Protection des Données
1, avenue du Rock'n'Roll
L-4361 Esch-sur-Alzette
Tel. +352 2610 60 1
Fax +352 2610 60 29
info@cnpd.lu
<http://www.cnpd.lu/>

Malta
Office of the Data Protection Commissioner
Data Protection Commissioner: Mr Joseph Ebejer
2, Airways House
High Street, Sliema SLM 1549
Tel. +356 2328 7100
Fax +356 2328 7198
commissioner.dataprotection@gov.mt
<http://www.dataprotection.gov.mt/>

Netherlands
Autoriteit Persoonsgegevens
Prins Clauslaan 60
P.O. Box 93374
2509 AJ Den Haag/The Hague
Tel. +31 70 888 8500
Fax +31 70 888 8501
info@autoriteitpersoonsgegevens.nl
<https://autoriteitpersoonsgegevens.nl/nl>

Poland
The Bureau of the Inspector General for the Protection of Personal Data – GIODO
ul. Stawki 2
00-193 Warsaw
Tel. +48 22 53 10 440
Fax +48 22 53 10 441
kancelaria@giodo.gov.pl; desiwm@giodo.gov.pl
<http://www.giodo.gov.pl/>

Portugal
Comissão Nacional de Protecção de Dados – CNPD
R. de São. Bento, 148-3º
1200-821 Lisboa
Tel. +351 21 392 84 00
Fax +351 21 397 68 32
geral@cnpd.pt
<http://www.cnpd.pt/>

Romania
The National supervisory authority for Personal Data Processing
President: Mrs Ancuța Gianina Opre
B-dul Magheru 28-30
Sector 1, BUCUREȘTI
Tel. +40 21 252 5599
Fax +40 21 252 5757
anspdcp@dataprotection.ro
<http://www.dataprotection.ro/>

Slovakia
Office for Personal Data Protection of the Slovak Republic
Hraničná 12
820 07 Bratislava 27
Tel.: + 421 2 32 31 32 14
Fax: + 421 2 32 31 32 34

statny.dozor@pdp.gov.sk
<http://www.dataprotection.gov.sk/>

Slovenia
Information Commissioner
Ms Mojca Prelesnik
Zaloška 59
1000 Ljubljana
Tel. +386 1 230 9730
Fax +386 1 230 9778
gp.ip@ip-rs.si
<https://www.ip-rs.si/>

Spain
Agencia de Protección de Datos
C/Jorge Juan, 6
28001 Madrid
Tel. +34 91399 6200
Fax +34 91455 5699
internacional@agpd.es
<https://www.agpd.es/>

Sweden
Datainspektionen
Drottninggatan 29
5th Floor
Box 8114
104 20 Stockholm
Tel. +46 8 657 6100
Fax +46 8 652 8652
datainspektionen@datainspektionen.se
<http://www.datainspektionen.se/>

United Kingdom
The Information Commissioner's Office
Water Lane, Wycliffe House
Wilmslow – Cheshire SK9 5AF
Tel. +44 1625 545 745
international.team@ico.org.uk
<https://ico.org.uk>

EUROPEAN FREE TRADE AREA (EFTA)

Iceland
Icelandic Data Protection Agency
Rauðarárstíg 10
105 Reykjavík
Tel. +354 510 9600; Fax +354 510 9606
postur@personuvernd.is

Liechtenstein
Data Protection Office
Kirchstrasse 8, P.O. Box 684
9490 Vaduz
Principality of Liechtenstein
Tel. +423 236 6090
info.dss@llv.li

Norway
Datatilsynet
The Data Inspectorate
P.O. Box 8177 Dep
0034 Oslo
Tel. +47 22 39 69 00; Fax +47 22 42 23 50
postkasse@datatilsynet.no

Switzerland
Data Protection and Information Commissioner of Switzerland
Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
Mr Adrian Lobsiger
Feldeggweg 1
3003 Bern
Tel. +41 58 462 43 95; Fax +41 58 462 99 96
contact20@edoeb.admin.ch

3.2 PARTICIPANT CHARACTERISATION

What age-range of participants will you recruit?

N/A

Please list the principal inclusion and exclusion criteria.

N/A

N/A

3.3 RECRUITMENT

Please describe the recruitment process and append any advertising if used.

Direct contact via email, fax, telephone or social media (i.e. LinkedIn)

3.4 NHS AND SOCIAL SERVICES INVOLVEMENT

Will participants be recruited because of their status as NHS patients or Social Services clients, or identified through those services' records?

- Yes
 No

If "yes", please give details of current status of the HRA REC review.

Click here to enter text.

Will the study involve adult participants unable to consent for themselves as defined by the Mental Capacity Act 2005 or other vulnerable adults?

- Yes
 No

If "yes", please detail the associated procedures as set out in the HRA REC application.

Click here to enter text.

CHECKLIST

1. The Application form has the appropriate signatories		Choose an item.
2. The Participant Information Sheet includes a statement to the effect that the project has been reviewed by the appropriate Research Ethics Committee and has been given a favourable ethical opinion for conduct.		Yes
3. The Participant Information Sheet contains the relevant Data Protection information.		Yes
4. Where minors (under 18) are involved in the study/research, please confirm that all investigators have obtained a full enhanced DBS (Disclosure and Barring Service check). Please select 'Not applicable' if this does not apply to your research.		Not Applicable
5. EITHER	a) The proposed research will not generate any information about the health of participants;	<input checked="" type="checkbox"/>
OR	b) If the research could reveal adverse information regarding the health of participants, their consent to pass information on to their GP will be included in the consent form and in this circumstance I will inform the participant and their GP, providing a copy of the relevant details to each and identifying by date of birth.	<input type="checkbox"/>
OR	c) I have explained within the application why (b) above is not appropriate.	<input type="checkbox"/>
6. EITHER	a) The proposed research does not involve children under the age of 5;	<input checked="" type="checkbox"/>
OR	b) My Head of School (or authorised responsible person) has given details of the proposed research to the <u>University's insurance officer</u> .	<input type="checkbox"/>
7. EITHER	a) The proposed research does not involve the taking of blood samples:	<input checked="" type="checkbox"/>
OR	b) For anyone whose proximity to the blood samples brings a risk of Hepatitis B, documentary evidence of immunity prior to the risk of exposure will be retained by the Head of School or authorised responsible person.	<input type="checkbox"/>
8. EITHER	a) The proposed research does not involve the storage of human tissue, as defined by the <u>Human Tissue Act 2004</u> ;	<input checked="" type="checkbox"/>
OR	b) I have explained within the application how the requirements of the Human Tissue Act 2004 will be met.	<input type="checkbox"/>
9. EITHER	a) The proposed research does not involve the use of ionising radiation;	<input checked="" type="checkbox"/>
OR	b) I am aware the proposed research will require <u>HRA REC review</u> .	<input type="checkbox"/>

VERSION CONTROL

VERSION	KEEPER	REVIEWED	APPROVED BY	APPROVAL DATE
1.4	UREC	Annually	UREC	September 2020

APPROVAL

Re: ETHICS REVIEW APPLICATION FORM

Dear Gil,

With apologies for the delay, I can confirm that I am happy to sign this off at school level.

With all good wishes,

Charlotte

Dr Charlotte L. Smith
Associate Professor in Law
School of Law, Foxhill House
University of Reading
Shinfield Road
Reading
RG6 6EP

Tel. 0118 378 5410
Fax. 0118 378 4543

Please note that I work part-time and that my working days are Tuesday, Wednesday and Friday 09:00 - 16:00.

Due to my flexible work/life balance, you may get emails from me outside normal working hours. I respect your working pattern and do not expect you to respond outside of your agreed working hours.