

GDPR Articles
With
Commentary & EU Case Laws

Author

Adv. Prashant Mali

[M.Sc.(Computer Science), CCFP, CISSA,LLM, Ph.D(Pursu.)]

About Author:

Author is International Cyber Law & Privacy Expert and a practicing High Court Lawyer based out of Mumbai in India. He is Masters in Computer Science and Masters in Law with Certification in Computer Forensics & Information Systems Security Auditing and prior working experience in the field of Software, Networking & IT Security. He is Chevening (UK) Cyber Security Fellow & IVLP (USA). He is the founder president of a law firm named Cyber Law Consulting. He was awarded as Cyber Security Lawyer of the year (Asia Pacific) in 2016 and Cyber Security Lawyer of the Year by Financial Monthly Magazine of UK. He has been a sought after speaker on National and International forums and is interviewed by BBC World, Bloomberg, Zee News, NDTV, CNBC, Al Jazeera etc. His articles are published in various magazines across the world and he is been quoted by leading daily newspapers. He has conducted various workshops on GDPR in various countries and has unique way of explaining GDPR with examples and by comparing it to existing laws of the country.

Note:

Every effort has been made to avoid errors or omissions in this, errors may creep in any mistake, error or discrepancy noted may be brought to our notice which shall be taken care of in the next edition. It is notified that neither the publisher or the author or seller will be responsible for any damages or loss of action to any one, of any kind, in the manner, there from. It is suggested that to avoid any doubt the reader should cross-check all the facts, law and contents of the publication with original Government publication or notification.

All rights reserved. No part of this work may be copied, reproduced, adapted, abridged or translated. Stored in any retrieval system, computer system, photographic or other system or transmitted in any form by any means whether electronic, mechanical, digital, optical photographic or otherwise without the prior written permission of cyber Infomedia. Any breach will entail legal action and prosecution without further notice.

INDEX

Articles	Particular	Page No.
	CHAPTER 1 : GENERAL PROVISIONS	
1	GDPR Subject-matter and objectives	01
2	GDPR Material scope	03
3	GDPR Territorial scope	04
4	GDPR Definitions	10
	CHAPTER 2 : PRINCIPLES	14
5	GDPR Principles relating to processing of personal data	14
6	GDPR Lawfulness of processing	17
7	GDPR Conditions for consent	20
8	GDPR Conditions applicable to child's consent in relation to information society services	23
9	GDPR Processing of special categories of personal data	24
10	GDPR Processing of personal data relating to criminal convictions and offences	28
11	GDPR Processing which does not require identification	29
	CHAPTER 3 : RIGHTS OF THE DATA SUBJECT	30
	Section 1 : Transparency and modalities	
12	GDPR Transparent information, communication and modalities for the exercise of the rights of the data subject	30
	Section 2 : Information and access to personal data	32
13	GDPR Information to be provided where personal data are collected from the data subject	32
14	GDPR Information to be provided where personal data have not been obtained from the data subject	34

15	GDPR Right of access by the data subject	37
	Section 3 : Rectification and erasure	38
16	GDPR Right to rectification	38
17	GDPR Right to erasure ('right to be forgotten')	39
18	GDPR Right to restriction of processing	41
19	GDPR Notification obligation regarding rectification or erasure of personal data or restriction of processing	42
20	GDPR Right to data portability	43
	Section 4 : Right to object and automated individual decision-making	44
21	GDPR Right to object	44
22	GDPR Automated individual decision-making, including profiling	46
	Section 5 : Restrictions	47
23	GDPR Restrictions	47
	CHAPTER 4 : CONTROLLER AND PROCESSOR	49
	Section 1 : General obligations	
24	GDPR Responsibility of the controller	49
25	GDPR Data protection by design and by default	52
26	GDPR Joint controllers	55
27	GDPR Representatives of controllers or processors not established in the Union	58
28	GDPR Processor	60
29	GDPR Processing under the authority of the controller or processor	64
30	GDPR Records of processing activities	64
31	GDPR Cooperation with the supervisory authority	67
	Section 2 : Security of personal data	68

32	GDPR Security of processing	68
33	GDPR Notification of a personal data breach to the supervisory authority	72
34	GDPR Communication of a personal data breach to the data subject	74
	Section 3 : Data protection impact assessment and prior consultation	77
35	GDPR Data protection impact assessment	77
36	GDPR Prior consultation	82
	Section 4 : Data protection officer	84
37	GDPR Designation of the data protection officer	84
38	GDPR Position of the data protection officer	86
39	GDPR Tasks of the data protection officer	88
	Section 5 : Codes of conduct and certification	93
40	GDPR Codes of conduct	93
41	GDPR Monitoring of approved codes of conduct	96
42	GDPR Certification	99
43	GDPR Certification bodies	100
	CHAPTER 5 : TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS	104
44	GDPR General principle for transfers	104
45	GDPR Transfers on the basis of an adequacy decision	106
46	GDPR Transfers subject to appropriate safeguards	109
47	GDPR Binding corporate rules	112
48	GDPR Transfers or disclosures not authorised by Union law	116
49	GDPR Derogations for specific situations	117

50	GDPR International cooperation for the protection of personal data	121
	CHAPTER 6 : INDEPENDENT SUPERVISORY AUTHORITIES	123
	Section 1 : Independent status	
51	GDPR Supervisory authority	123
52	GDPR Independence	124
53	GDPR General conditions for the members of the supervisory authority	126
54	GDPR Rules on the establishment of the supervisory authority	127
	Section 2 : Competence, tasks and powers	128
55	GDPR Competence	128
56	GDPR Competence of the lead supervisory authority	129
57	GDPR Tasks	131
58	GDPR Powers	134
59	GDPR Activity reports	137
	CHAPTER 7 : COOPERATION AND CONSISTENCY	138
	Section 1 : Cooperation	
60	GDPR Cooperation between the lead supervisory authority and the other supervisory authorities concerned	138
61	GDPR Mutual assistance	140
62	GDPR Joint operations of supervisory authorities	142
	Section 2 : Consistency	144
63	GDPR Consistency mechanism	144
64	GDPR Opinion of the Board	144
65	GDPR Dispute resolution by the Board	146

66	GDPR Urgency procedure	148
67	GDPR Exchange of information	149
	Section 3 : European data protection board	149
68	GDPR European Data Protection Board	149
69	GDPR Independence	150
70	GDPR Tasks of the Board	150
71	GDPR Reports	154
72	GDPR Procedure	154
73	GDPR Chair	154
74	GDPR Tasks of the Chair	155
75	GDPR Secretariat	155
76	GDPR Confidentiality	157
	CHAPTER 8 : REMEDIES, LIABILITY AND PENALTIES	158
77	GDPR Right to lodge a complaint with a supervisory authority	158
78	GDPR Right to an effective judicial remedy against a supervisory authority	158
79	GDPR Right to an effective judicial remedy against a controller or processor	160
80	GDPR Representation of data subjects	161
81	GDPR Suspension of proceedings	162
82	GDPR Right to compensation and liability	163
83	GDPR General conditions for imposing administrative fines	163
84	GDPR Penalties	170
	CHAPTER 9 : PROVISIONS RELATING TO SPECIFIC PROCESSING SITUATIONS	171

85	GDPR Processing and freedom of expression and information	171
86	GDPR Processing and public access to official documents	171
87	GDPR Processing of the national identification number	171
88	GDPR Processing in the context of employment	172
89	GDPR Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes	173
90	GDPR Obligations of secrecy	175
91	GDPR Existing data protection rules of churches and religious associations	176
	CHAPTER 10 : DELEGATED ACTS AND IMPLEMENTING ACTS	178
92	GDPR Exercise of the delegation	178
93	GDPR Committee procedure	179
	CHAPTER 11 : FINAL PROVISIONS	181
94	GDPR Repeal of Directive 95/46/EC	181
95	GDPR Relationship with Directive 2002/58/EC	181
96	GDPR Relationship with previously concluded Agreements	182
97	GDPR Commission reports	182
98	GDPR Review of other Union legal acts on data protection	183
99	GDPR Entry into force and application	183
	CASE LAWS	185
	I. SUMMARY OF EU COURT DECISIONS RELATING TO DATA PROTECTION (IN NUMERICAL ORDER OF CASE NUMBER)	186

1	COURT OF JUSTICE DECISIONS	
1.1	C-450/00, COMMISSION V. LUXEMBOURG, 4.10.2001 (“LUXEMBOURG”)	186
1.2	C-465/00 AND C-138/01, RECHNUNGSHOF V. OSTERREICHISCHER RUNDFUNK, 20.5.2003 (“RECHNUNGSHOF”)	186
1.3	C-101/01, LINDQUIST, 6.11.2003 (“LINDQUIST”)	187
1.4	C-317 AND 318/04, PARLIAMENT V. COUNCIL (PNR), 30.5.2006 (“PNR”)	189
1.5	C-275/06, PROMUSICAE, 29.1.2008 (“PROMUSICAE”)	189
1.6	C-301/06, IRELAND V. PARLIAMENT AND COUNCIL, 10.2.2009 (“IRELAND”)	190
1.7	C-524/06, HUBER V. GERMANY, 16.12.2008 (“HUBER”)	191
1.8	C-73/07, TIETOSUOJAVALTUUTETTU [FINNISH DATA PROTECTION OMBUDSMAN] V. SATAKUNNAN MARKKINAPORSSI OY AND SATAMEDIA OY, 16.12.2008 (“TIETOSUOJAVALTUUTETTU”)	192
1.9	C-518/07, COMMISSION V. GERMANY, 9.3.2010 (“GERMANY”)	193
1.10	C-553/07, COLLEGE VAN BURGEMEESTER EN WETHOUDERS VAN ROTTERDAM V. RIJKEBOER, 7.5.2009 (“RIJKEBOER”)	194
1.11	C-557/07, LSG-GESELLSCHAFT ZUR WAHRNEHMUNG VON LEISTUNGSSCHUTZRECHTEN GMBH V. TELE2 TELECOMMUNICATION GMBH, 19.2.2009 (“LSG”)	194
1.12	C-28/08, COMMISSION V. BAVARIAN LAGER CO., 29.6.2010 (“BAVARIAN LAGER”)	195
1.13	C-92/09 VOLKER UND MARKUS SCHECKE GBR V. LAND HESSEN, AND C-93/09, EIFERT V. LAND HESSEN AND BUNDESANSTALT FUR LANDWIRTSCHAFT UND ERNAHRUNG, 9.11.2010 (“SCHECKE”)	198

1.14	CASE C-70/10, SCARLET EXTENDED SA V. SOCIETE BELGE DES AUTEURS, COMPOSITEURS ET EDITEURS SCRL (SABAM), 24.11.2011 (“SCARLET”)	200
1.15	CASE C-461/10, BONNIER AUDIO AB ET AL. V. PERFECT COMMUNICATION SWEDEN, 19.4.2012 (“BONNIER”)	201
1.16	JOINED CASES C-468/10 AND C-469/10, ASOCIACION NACIONAL DE ESTABLECIMIENTOS FINANCIEROS DE CREDITO (ASNEF) AND FEDERACION DE COMERCIO ELECTRONICO Y MARKETING DIRECTO (FECEMD) V. ADMINISTRACION DEL ESTADO, 24.11.2011 (“ASNEF”)	202
1.17	C-614/10, COMMISSION V. AUSTRIA, 16.10.2012 (“AUSTRIA”)	203
1.18	C-614/10, COMMISSION V. AUSTRIA, 16.10.2012 (“AUSTRIA”)	204
1.19	C-131/12, GOOGLE SPAIN SL V. AEPD (THE DPA) & MARIO COSTEJA GONZALEZ, 13.5.2014 (“GOOGLE”)	205
1.20	C-141/12 AND C-372/12, MINISTER VOOR IMMIGRATIE V. M, 17.7.2014 (“M”)	209
1.21	C-288/12, COMMISSION V. HUNGARY, 8.4.2014 (“HUNGARY”)	210
1.22	C-291/12, SCHWARZ V. BOCHUM, 17.10.2014 (“SCHWARZ”)	210
1.23	C-293/12 AND C-594-12, DIGITAL RIGHTS IRELAND LTD V. IRELAND, 8.4.2014 (“DRI”)	211
1.24	C-342-12, WORTEN-EQUIPAMENTOS PARA O LAR SA V. ACT (AUTHORITY FOR WORKING CONDITIONS), 30.5.2013 (“WORTEN”)	214
1.25	C-473/12, IPI V. ENGLEBERT (“ENGLEBERT”)	215
1.26	C-486/12, X, 12.12.2013 (“X”)	216
1.27	C-212/13, RYNES V. ÚŘAD PRO OCHRANU OSOBNICH ÚDAJŮ, 11.12.2014 (“RYNES”)	216
1.28	C-615/13 P, CLIENT EARTH ET AL. V. EFSA, 16.7.2015 (“CLIENT EARTH”)	217

1.29	C-201/14, SMARANDA BARA ET AL. V. PRESEDINTELE CASEI NATIONALE DE ASIGURARI DE SANATATE (CNAS) ET AL., 1.10.2015 (“BARA”)	219
1.30	C-230/14, WELTIMMO S.R.O. V. NEMZETI ADATVEDELMI ES INFORMACIOSZABADSAG HATOSAG (HUNGARIAN DPA), 1.10.15 (“WELTIMMO”)	220
1.31	C-362/14, SCHREMS V. DATA PROTECTION COMMISSIONER, 6.10.2015 (“SCHREMS”)	222
2	GENERAL COURT DECISIONS	224
2.1	T-320/02, ESCH-LEONHARDT AND OTHERS V EUROPEAN CENTRAL BANK, 18.2.2004 (“ESCH-LEONHARDT”)	224
2.2	T-198/03, BANK AUSTRIA CREDITANSTALT AG V COMMISSION OF THE EUROPEAN COMMUNITIES, 30.5.2006 (“BANK AUSTRIA”)	225
2.3	T-259/03, NIKOLAOU V. COMMISSION, 12.9.2007 (“NIKOLAOU”)	225
2.4	T-161/04, JORDANA V. COMMISSION, 7.7.2011 (“JORDANA”)	227
2.5	T-82/09, DENNEKAMP V. EUROPEAN PARLIAMENT, 23.11.2011 (“DENNEKAMP I”)	227
2.6	T-190/10, EGAN & HACKETT V. EUROPEAN PARLAMENT, 28.3.2012 (“EGAN & HACKETT”)	228
2.7	T-115/13, DENNEKAMP V. EUROPEAN PARLIAMENT (15.7.2015) (“DENNEKAMP II”)	229
2.8	T-496/13, MCCULLOUGH V. CEDEFOP (11.6.2015)(“MCCULLOUGH”)	231
3	CIVIL SERVICE TRIBUNAL DECISIONS	232
3.1	F-30/08, NANOPOULOS V. COMMISSION, 11.5.2010 (“NANOPOULOS”) (ON APPEAL, CASE T-308/10)	232
3.2	F-46/09, V & EDPS V. EUROPEAN PARLAMENT, 5.7.2011 (“V”)	232
4	POST GDPR IMPLEMENTATION CASE LAWS	234
4.1	GOOGLE CASE	234

4.2	GERMAN COURTS - WHETHER AN INFRINGEMENT OF THE GDPR ALSO QUALIFIES AS UNFAIR-COMPETITIVE BEHAVIOR	235
4.3	GOOGLE IN LANDMARK NORDIC LEGAL CASE ON THE "RIGHT TO BE FORGOTTEN."	236
4.4	GDPR FINE –BARREIRO MONTIJO HOSPITAL CENTER IN PORTUGAL CASE	237
4.5	FACEBOOK BREACH IN GDPR TEST CASE.	238
	II. SUMMARY OF EU COURT DECISIONS RELATING TO DATA PROTECTION (ORGANISED BY TOPIC)	239
1	GENERAL	239
1.1	DEFINITION OF PERSONAL DATA	239
1.2	DEFINITION OF PROCESSING	240
1.3	DEFINITION OF CONTROLLER	241
1.4	LEGAL PERSONS	242
1.5	SENSITIVE PERSONAL DATA	242
1.6	CONSENT	243
1.7	NECESSITY/PROPORTIONALITY	243
1.8	SECURITY	245
1.9	DEROGATIONS	245
1.10	NON-CONTRACTUAL LIABILITY	246
2	DATA SUBJECT RIGHTS	246
2.1	INFORMATION	246
2.2	ACCESS	247
2.3	ERASURE	248
3	BALANCING FUNDAMENTAL RIGHTS	248
3.1	PROTECTION OF PROPERTY AND AN EFFECTIVE REMEDY	248

3.2	FREEDOM OF EXPRESSION	249
3.2	ACCESS TO DOCUMENTS	249
4	TRANSFERS	252
4.1	APPROPRIATE LEGAL BASIS	254
4.2	ADEQUATE LEVEL OF PROTECTION	254
4.3	SAFE HARBOUR	255
5	REGULATION 45/2001	256
5.1	SCOPE	256
5.2	LAWFULNESS	256
6	DIRECTIVE 95/46	256
6.1	SCOPE	256
6.2	LAWFULNESS	257
6.3	ESTABLISHMENT OF THE CONTROLLER	257
6.4	INDEPENDENCE OF DPA	259
6.5	DPA POWERS	261
6.6	PROCESSING FOR SOLELY JOURNALISTIC PURPOSES	262
6.7	PROCESSING FOR PURELY PERSONAL OR HOUSEHOLD ACTIVITY	262
6.8	TRANSPOSITION/HARMONISATION	263
6.9	DIRECT APPLICABILITY	263
7	DIRECTIVE 2002/58	264
7.1	SCOPE	264
7.2	TRAFFIC DATA	264
8	DIRECTIVE 2006/24	265

8.1	APPROPRIATE LEGAL BASIS	265
8.2	SCOPE	266
8.3	LAWFULNESS	266
9	ARTICLES 7, 8 CFR	267
10	ARTICLE 8 ECHR	269
	APPENDIX 1: RECITALS [1 to 173]	271
	APPENDIX 2: EU/EEA NATIONAL SUPERVISORY AUTHORITIES	328
	APPENDIX 3: LOOPHOLES IN GDPR	330
	APPENDIX 4: FLOW CHART - COMPOSITION OF EUROPEAN DATA PROTECTION BOARD	342

PREFACE

I was the early starter to get awakened towards GDPR due to my practice in cyber and privacy law. When I first started the firm EUGDPR Institute, I was sure about writing a book on GDPR but never knew the connotations it would have. I was involved in training participants from many large IT Companies like Tech Mahindra, TCS, Oracle, IBM, Cognizant etc. and obviously partners from large law firms then I decided to pen this book as the legal language and its interpretation was always a challenge to these technology or GRC migrants. Being author of published and famous books on cyber law made the structure of this book clear in my mind. Articles of GDPR do have a typical international law kinda language and often raises more than one questions or doubts in the avid reader of the topic.

This book is a series of articles and interpretations. It deals with questions of applicability of GDPR articles in various scenarios; at its core, GDPR is a new set of rules designed to give EU citizens more control over their personal data. It aims to simplify the regulatory environment for business so both citizens and businesses in the European Union can fully benefit from the digital economy.

Fundamentally, almost every aspect of our lives revolves around data. From social media companies, to banks, retailers, and governments -- almost every service we use involves the collection and analysis of our personal data. Your name, address, credit card number and more all collected, analysed and, perhaps most importantly, stored by organisations

In this busy age, when we are all bombarded with information, it is helpful, I think, to be offered a chance to take a breath and do things simply. There is something meditative about reading the GDPR articles one by one and again going through it next time. There is something therapeutic in watching people's faces light up when they find they are compliant to particular article of GDPR. There is something healing in the simple task of being aware about applicability of GDPR to the organisation. GDPR applies to any organisation operating within the EU, as well as any organisations outside of the EU, which offer goods or services to customers or businesses in the EU. That ultimately means that almost every major corporation and practitioner in the world will need this book to understand, implement, comply and re-comply with GDPR.

Whether you are a DPO, a auditor, a lawyer, a student, a GRC professional, a privacy devotee, a lonely heart nostalgic for GDPR trainings — I hope you find something of value in these pages. This book might inspire you to read your GDPR compliance report again, or it might just offer you an imaginative escape from the incessant hurry of modern day compliance requirements. Maybe it will prompt you to call your legal and compliance team. Regardless of how you use this book, I hope it helps you in some small way to build a data protection and privacy regime within your mind or in the organisation.

I Sincerely want to put on record my deep appreciation and salute to the team working on this book with special reference to Lawyer Tejal Patel, she has gone extra length to research and formalize the contents of this book.

Author

Prashant Mali [M.Sc. (Computer Science), LL.M]

Chevening Cyber Security Fellow (UK) & IVLP (USA)

Email: cyberlawconsulting@gmail.com

CHAPTER 1: GENERAL PROVISIONS

Art. 1 GDPR Subject-matter and objectives

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.
2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.
3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

Suitable Recitals

(1) Data protection as a fundamental right; (2) Respect of the fundamental rights and freedoms; (3) Directive 95/46/EC harmonization; (4) Data protection in balance with other fundamental rights; (5) Cooperation between Member States to exchange personal data; (6) Ensuring a high level of data protection despite the increased exchange of data; (7) The framework is based on control and certainty; (8) Adoption into national law; (9) Different standards of protection by the Directive 95/46/EC; (10) Harmonised level of data protection despite national scope; (11) Harmonisation of the powers and sanctions; (12) Authorization of the European Parliament and the Council.

COMMENTARY:

The European Union's (EU) view on data protection is closely linked to privacy issues, which does not appear to always be the right approach in dealing with data protection. The privacy concept as outlined in Art. 8 of the European Convention on Human Rights refers mainly to the right to private and family life, respect of private home and private correspondence. The data protection could include privacy issues but is not limited to them.

Data protection means the right of a person to know which data is gathered in regards to her person, how the data is used, aggregated, protected, and where the data is transmitted. Anyone has the right to have access to that data and to modify it. In all cases, the person has to give his/her consent for that data to be used by another person, government, or any other entity. Data protection values are not essentially privacy related ones. These values cannot be dealt with just through the privacy perspective. They are autonomous values, which grant fundamental rights: the right to data protection as recognised by Article 8 in the Charter of Fundamental Rights of the European Union: "Protection of personal data: Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified".

Thank You for previewing this eBook

You can read the full version of this eBook in different formats:

- HTML (Free /Available to everyone)
- PDF / TXT (Available to V.I.P. members. Free Standard members can access up to 5 PDF/TXT eBooks per month each month)
- Epub & Mobipocket (Exclusive to V.I.P. members)

To download this full book, simply select the format you desire below

