



THE ULTIMATE
GDPR
PRACTITIONER
GUIDE

Stephen Massey MSc CISSP

THE ULTIMATE GDPR PRACTITIONER GUIDE: DEMYSTIFYING PRIVACY & DATA PROTECTION

STEPHEN MASSEY MSc FIP CISSP



Fox Red Risk Publishing is an Imprint of Fox Red Risk Solutions Ltd (9997987)
27 Old Gloucester Street, LONDON, WC1N 3AX, UNITED KINGDOM



#ultimateGDPRguide

Copyright © 2017 Stephen Massey. Published by Fox Red Risk Publishing.

All rights reserved.

Please direct enquiries to info@foxredrisk.com

This publication contains information licensed under the Open Government Licence v3.0 (<http://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/>).

This publication contain information authorised for commercial and non-commercial reuse. <http://eur-lex.europa.eu>, © European Union, 1998-2017

This publication contains information licenced under Creative Commons up to and including Attribution-ShareAlike Licence v4.0 (<https://creativecommons.org/licenses/by-sa/4.0/legalcode>).

Although the author and publisher have made every effort to ensure that the information in this book was correct at press time, the author and publisher do not assume and hereby disclaim any liability to any party for any loss, damage, or disruption caused by errors or omissions, whether such errors or omissions result from negligence, accident, or any other cause.

The information and opinions provided in this book do not address individual requirements and are for informational purposes only. They do not constitute any form of legal advice and should not be relied on or treated as a substitute for specific advice relevant to particular circumstances and is not intended to be relied upon when making (or refraining from making) any specific decisions.

All terms mentioned in this book that are known to be or are suspected of being trademarks or service marks have been appropriately capitalised. The author and publisher cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark of service mark.

ISBN-13: 978-1999827205 (Print)

ISBN-13: 978-1-9998272-1-2 (Kindle)

ISBN-13: 978-1-9998272-2-9 (ePUB)

DEDICATION

I dedicate this book to the two most inspirational people in my life:

My late wife Kate and, my best boy Cooper

CONTENTS

PART I: THE ULTIMATE PRACTITIONER - (THE BASICS)	1
1. INTRODUCTION	1
Welcome Practitioner!	1
Why Should I Care about Privacy?	1
I am not even in the EU, so I definitely shouldn't care...should I?	2
Using this Book	2
Key Terms	3
2. WHAT IS THE GENERAL DATA PROTECTION REGULATION (GDPR)?	5
History of Privacy & Data Protection	5
What is GDPR?	8
Key Changes	8
Structure of GDPR	9
What is Personal Data?	11
What is Sensitive Data?	11
Comparison with US Privacy Legislation	12
Establishing Lawful Grounds for Processing	13
Consent	13
Consent and Children	13
The Controller & the Processor	13
The Supervisory Authority	15
Consequences of Non-Compliance	16
3. QUICK START CHECKLIST	19
Appoint a Data Protection Officer (DPO)	19
A Project Approach	20
No (Wo)man is an Island	20
Management Systems & Standards	21
Data is King!	21
The 12 (initial) Steps to Compliance	22
4. GDPR PRINCIPLES & DATA SUBJECTS' RIGHTS	25
The Six Principles	25
The Eight Rights	29

5. THE DATA PROTECTION OFFICER (DPO)	35
What is the DPO?	35
Do I need a DPO?	36
Tasks of the DPO?	36
Qualities of a DPO?	37
Relationship with the Supervisory Authority	38
A Protected Species	39
Data Protection Officer as a Service (DPOaaS)	40
PART I: THE ULTIMATE PRACTITIONER (IMPLEMENTATION)	41
6. AWARENESS	43
Stakeholder Analysis	43
Communications Planning	47
Communications Plan Template	51
Awareness through Learning	53
Lesson Plan Template	59
7. DATA PROTECTION POLICIES AND PRIVACY NOTICES	61
Standardised Terminology	61
Policy Framework	62
Policy Life-Cycle	65
Drafting Policy	70
Procedures, Guidelines, Standards, Methodologies & Templates	73
Policy Enforcement	75
The Data Protection / Privacy Notice	76
Example General Data Protection Policy	81
Example Privacy Notice	89
8. INFORMATION AUDITS & PROCESS MAPPING	97
The Information Audit	97
Record Keeping	99
Process Mapping	100
9. DATA PROTECTION IMPACT ASSESSMENT	103
What are the minimum requirements for a DPIA?	103
When is a DPIA Required?	104
Exceptions	104
Consultation	105

Codes of Conduct	105
Standalone or Integrated?	105
The DPIA Process	106
Example Data Protection Impact Assessment (DPIA) – Initial and Full Reports	110
Example Initial DPIA	110
Example Full DPIA	113
10. INFORMATION SECURITY	125
What is Information Security?	125
Know your Environment	126
The CIRAN Paradigm	128
Information Risk Management (IRM)	130
Information Security Management Systems(ISMS)	130
Defence Detect Manage (DDM)	131
Security Assessment	133
Security Metrics	135
11. DATA PROTECTION BY DESIGN & BY DEFAULT	137
Information Life-Cycle & Records Management	137
Information Classification	139
Systems Development Life Cycle (SDLC)	142
End User Computing Applications (EUCA)	144
Consent Mechanisms	145
Data Minimisation	147
Privacy Dashboards	147
Just-in-time Privacy Notices	148
Pseudonymisation	149
Encryption & other Cryptographic Techniques	151
Identity and Access Management (IAM)	156
Data Protection and APIs	159
OWASP Top 10	161
Data Protection and Database Design	164
Artificial Intelligence / Big Data / Analytics	166
Computer Vision & CCTV	167
Data Protection Design Specification Template	169
12. INCIDENT MANAGEMENT & BREACH NOTIFICATION	171
What is a Data Breach?	172
The Incident Response Life-Cycle	173
Calculating Data Breach Severity	179
Notification to the Supervisory Authority	186
Notification to Data Subjects	188

13. DATA SUBJECT ACCESS REQUESTS (DSAR)	189
What is a Data Subject Access Request (DSAR)?	189
Key changes to Data Subject Access Requests	190
FOI or DSAR?	190
Exemptions	191
Common concerns raised by Data Subjects	191
The Subject Access Request Process	192
14. THIRD PARTIES & OUTSOURCING	197
The Controller-Processor relationship	198
Data Protection through the Procurement and Supply Life-Cycle	199
Example Data Protection Detailed Specification	205
15. THIRD COUNTRIES AND ORGANISATIONS OUTSIDE THE EU	207
Adequacy	208
Safeguards	209
Derogations	210
Designating a Representative	211
PART II: THE EU GENERAL DATA PROTECTION REGULATION	213
I: GENERAL PROVISIONS	215
Article 1: Subject-matter and objectives	215
Article 2: Material scope	215
Article 3: Territorial scope	216
Article 4: Definitions	216
II: PRINCIPLES	219
Article 5: Principles relating to processing of personal data	219
Article 6: Lawfulness of processing	219
Article 7: Conditions for consent	220
Article 8: Conditions applicable to child's consent in relation to information society services	221
Article. 9: Processing of special categories of personal data	221
Article. 10: Processing of personal data relating to criminal convictions and offences	222
Article 11: Processing which does not require identification	222

III: RIGHTS OF THE DATA SUBJECT	223
Article 12: Transparent information, communication and modalities for the exercise of the rights of the Data Subject	223
Article 13: Information to be provided where personal data are collected from the Data Subject	224
Article 14: Information to be provided where personal data have not been obtained from the Data Subject	225
Article 15: Right of access by the Data Subject	226
Article 16: Right to rectification	227
Article 17: Right to erasure ('right to be forgotten')	227
Article 18: Right to restriction of processing	227
Article 19: Notification obligation regarding rectification or erasure of personal data or restriction of processing	228
Article 20: Right to data portability	228
Article 21: Right to object	229
Article 22: Automated individual decision-making, including profiling	229
Article 23: Restrictions	230
IV: CONTROLLER AND PROCESSOR	231
Article 24: Responsibility of the Controller	231
Article 25: Data protection by design and by default	231
Article 26: Joint Controllers	231
Article 27: Representatives of Controllers or Processors not established in the Union	232
Article 28: Processor	232
Article 29: Processing under the authority of the Controller or Processor	233
Article 30: Records of processing activities	234
Article 31: Cooperation with the Supervisory Authority	234
Article 32: Security of processing	235
Article 33: Notification of a personal data breach to the Supervisory Authority	235
Article 34: Communication of a personal data breach to the Data Subject	236
Article 35: Data protection impact assessment	236
Article 36: Prior consultation	237
Article 37: Designation of the data protection officer	238
Article 38: Position of the data protection officer	239
Article 39: Tasks of the data protection officer	239
Article 40: Codes of conduct	240
Article 41: Monitoring of approved codes of conduct	241
Article 42: Certification	242
Article 43: Certification bodies	242
V: TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS	245
Article 44: General principle for transfers	245
Article 45: Transfers on the basis of an adequacy decision	245
Article 46: Transfers subject to appropriate safeguards	246
Article 47: Binding corporate rules	247
Article 48: Transfers or disclosures not authorised by Union law	248
Article 49: Derogations for specific situations	248

Article 50: International cooperation for the protection of personal data	249
VI: INDEPENDENT SUPERVISORY AUTHORITIES	251
Article 51: Supervisory Authority	251
Article 52: Independence	251
Article 53: General conditions for members of Supervisory Authority	251
Article 54: Rules on the establishment of the Supervisory Authority	252
Article 56: Competence of the lead Supervisory Authority	253
Article 57: Tasks	253
Article 58: Powers	254
Article 59: Activity reports	256
VII: COOPERATION AND CONSISTENCY	257
Article 60: Cooperation between the lead Supervisory Authority and the other supervisory authorities concerned	257
Article 61: Mutual assistance	258
Article 62: Joint operations of supervisory authorities	259
Article 63: Consistency mechanism	260
Article 64: Opinion of the Board	260
Article 65: Dispute resolution by the Board	261
Article 66: Urgency procedure	262
Article 67: Exchange of information	262
Article 68: European Data Protection Board	262
Article 69: Independence	263
Article 70: Tasks of the Board	263
Article 71: Reports	265
Article 72: Procedure	265
Article 73: Chair	265
Article 74: Tasks of the Chair	265
Article 75: Secretariat	265
Article 76: Confidentiality	266
VIII: REMEDIES, LIABILITY AND PENALTIES	267
Article 77: Right to lodge a complaint with a Supervisory Authority	267
Article 78: Right to an effective judicial remedy against a Supervisory Authority	267
Article 79: Right to an effective judicial remedy against a Controller or Processor	267
Article 80: Representation of Data Subjects	267
Article 81: Suspension of proceedings	268
Article 82: Right to compensation and liability	268
Article 83: General conditions for imposing administrative fines	269
Article 84: Penalties	270

IX: PROVISIONS RELATING TO SPECIFIC PROCESSING SITUATIONS	271
Article 85: Processing and freedom of expression and information	271
Article 86: Processing and public access to official documents	271
Article 87: Processing of the national identification number	271
Article 88: Processing in the context of employment	271
Article 89: Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes	272
Article 90: Obligations of secrecy	272
Article 91: Existing data protection rules of churches and religious associations	272
X: DELEGATED ACTS AND IMPLEMENTING ACTS	273
Article 92: Exercise of the delegation	273
Article 93: Committee procedure	273
XI: FINAL PROVISIONS	275
Article 94: Repeal of Directive 95/46/EC	275
Article 95: Relationship with Directive 2002/58/EC	275
Article 96: Relationship with previously concluded Agreements	275
Article 97: Commission reports	275
Article 98: Review of other Union legal acts on data protection	275
Article 99: Entry into force and application	276
PART III: THE RECITALS	277
THE RECITALS	279
1:37 - General Provisions	279
38:57 - Principles (38:57)	285
58:73 - Rights of the Data Subject	291
74:100 - Controller and Processor	295
101:116 - Transfers to Third Countries or International Organisations	301
117:131 - Independent Supervisory Authorities	305
131:140 - Cooperation and Consistency	309
141:152 - Remedies, Liabilities and Penalties	311
153:165 - Processing Relating to Specific Processing Situations	315
166:170 - Delegated Acts and Implementing Acts	319
171:173 - Final Provisions	321
LIST OF EUROPEAN UNION DATA PROTECTION AUTHORITIES	323
ABOUT THE AUTHOR	325

***“We’re all going to have to change
how we think about data protection.”***
Elizabeth Denham, UK Information Commissioner

Biblioteka Główna
Akademii Sztuki Wojennej

26678/III (CB)



03-026678-000-0

The Ultimate GDPR Practitioner Guide provides those tasked with implementing Data Protection processes, useful information on how to achieve compliance with GDPR. The book is crammed with advice, guidance and templates and also includes a copy of the full regulation text and the supporting recitals. Topics include:

- The Data Protection Officer
- Data Protection Policies
- Data Protection Notices
- Data Protection Impact Assessments
- Outsourcing
- Subject Access Requests
- And Much Much More!

When Elizabeth Denham, the UK Information Commissioner, delivered the above quote at a lecture for the Institute of Chartered Accountants in England and Wales in London on 17 January 2017, she was highlighting the requirement for organisations to be accountable for the Personal Data they hold and process. Under the EU General Data Protection Regulation (GDPR) we all need to up our game!

GDPR is a transformative piece of regulation that applies from 25 May 2018. GDPR enhances current rights and freedoms afforded to EU citizens under the 1995 EU Data Protection Directive (95/46/EC). GDPR gives Supervisory Authorities strengthened powers to take enforcement action on those organisations who fail in their duty to uphold those rights and freedoms. GDPR is a game-changer!



ISBN 978-1-9998272-0-5

9 781999 827205