
The EU General Data Protection Regulation (GDPR)

Paul Voigt • Axel von dem Bussche

The EU General Data Protection Regulation (GDPR)

A Practical Guide



Springer

Paul Voigt
Taylor Wessing
Berlin, Germany

Axel von dem Bussche
Taylor Wessing
Hamburg, Germany

ISBN 978-3-319-57958-0 ISBN 978-3-319-57959-7 (eBook)
DOI 10.1007/978-3-319-57959-7

Library of Congress Control Number: 2017942999

© Springer International Publishing AG 2017

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Contents

1	Introduction and ‘Checklist’	1
1.1	Legislative Purpose and Previous Legal Provisions	1
1.1.1	The Data Protection Directive	1
1.1.2	The General Data Protection Regulation	2
1.2	Checklist: Most Important Data Protection Obligations	3
1.2.1	Organisational Requirements	3
1.2.2	Lawfulness of the Processing Activities	5
	References	7
2	Scope of Application of the GDPR	9
2.1	In Which Case Does the Regulation Apply?	9
2.1.1	‘Processing’	9
2.1.2	‘Personal Data’	11
2.1.3	Exemptions from the Scope of Application	16
2.2	To Whom Does the Regulation Apply?	17
2.2.1	‘Controller’	17
2.2.2	‘Processor’	20
2.2.3	Beneficiaries of Protection Under the GDPR	20
2.3	Where Does the Regulation Apply?	21
2.3.1	Data Processing in the Context of the Activities of an EU Establishment	22
2.3.2	Processing of Personal Data of Data Subjects in the EU	26
	References	29
3	Organisational Requirements	31
3.1	Accountability	31
3.2	General Obligations	33
3.2.1	Responsibility, Liability and General Obligations of the Controller	33
3.2.2	The Allocation of Responsibility Between Joint Controllers	34
3.2.3	Cooperation with Supervisory Authorities	37
3.3	Technical and Organisational Measures	38
3.3.1	Appropriate Data Protection Level	38

3.3.2	Minimum Requirements	39
3.3.3	Risk-Based Approach Towards Data Security	40
3.3.4	The NIS Directive	42
3.4	Records of Processing Activities	44
3.4.1	Content and Purpose of the Records	44
3.4.2	Exemption from the Obligation to Maintain Records	45
3.5	Data Protection Impact Assessment	47
3.5.1	Affected Types of Data Processing	47
3.5.2	Scope of the Assessment	49
3.6	Data Protection Officer	53
3.6.1	Designation Obligation	53
3.6.2	Aspects Regarding the Designation of the Data Protection Officer	56
3.6.3	Position	58
3.6.4	Responsibilities	60
3.7	Privacy by Design and Privacy by Default	62
3.8	Personal Data Breaches	65
3.8.1	Personal Data Breach	65
3.8.2	Notification to the Supervisory Authority	65
3.8.3	Communication to the Data Subjects	69
3.9	Codes of Conduct, Certifications, Seals, Etc.	71
3.9.1	Relationship Between Codes of Conduct and Certifications	71
3.9.2	Codes of Conduct	72
3.9.3	Certifications, Seals, Marks	77
3.10	Data Processors	80
3.10.1	Privileged Position of the Processor	80
3.10.2	Obligation of the Controller When Choosing a Processor	81
3.10.3	Obligations of the Processor	83
3.10.4	Designation of a Sub-Processor	84
	References	84
4	Material Requirements	87
4.1	Basic Principles	87
4.1.1	Lawfulness, Fairness and Transparency	88
4.1.2	Purpose Limitation	88
4.1.3	Data Minimisation	90
4.1.4	Accuracy	91
4.1.5	Storage Limitation	92
4.1.6	Integrity and Confidentiality	92
4.2	Legal Justifications for Data Processing	92
4.2.1	Processing Based on Consent	93
4.2.2	Processing Based on a Legal Permission	100
4.2.3	Processing of Special Categories of Personal Data	110

4.3	Data Transfers to Third Countries	116
4.3.1	Safe Third Countries	117
4.3.2	Consent	118
4.3.3	Standard Contractual Clauses	119
4.3.4	EU–U.S. Privacy Shield	122
4.3.5	Binding Corporate Rules	125
4.3.6	Codes of Conduct, Certifications, Etc.	129
4.3.7	Derogations for Specific Situations	130
4.3.8	Appointment of a Representative by Non-EU Entities	133
4.4	Limited Privilege for Intra-Group Processing Activities	135
4.4.1	Separate Data Protection Responsibility of Each Group Member	136
4.4.2	Facilitations Regarding Material Requirements	137
4.4.3	Facilitation Regarding Organisational Requirements	138
	References	138
5	Rights of Data Subjects	141
5.1	Transparency and Modalities	141
5.1.1	The Manner of Communicating with the Data Subject	142
5.1.2	The Form of Communication	143
5.2	Information Obligation of the Controller Prior to Processing	143
5.2.1	Time of Information	144
5.2.2	Collection of the Data from the Data Subject	144
5.2.3	Obtainment of the Data from Another Source	146
5.2.4	Practical Implications	147
5.3	Response to Data Subjects' Requests	147
5.3.1	Manner of Response	147
5.3.2	Time of Response	149
5.3.3	Information in Case of Inaction	149
5.3.4	Verification of the Data Subject's Identity	150
5.4	Right to Access	150
5.4.1	Scope of the Right to Access	150
5.4.2	Provision of Access to the Personal Data	152
5.4.3	Practical Implications	153
5.5	Rights to Erasure, Rectification and Restriction	154
5.5.1	Right to Rectification	154
5.5.2	Right to Erasure	156
5.5.3	Right to Restriction of Processing	164
5.5.4	Notification of Third Parties Regarding the Rights to Erasure, Rectification and Restriction, Art. 19	167
5.6	Right to Data Portability	168
5.6.1	Scope and Exercise of the Right to Data Portability	169
5.6.2	Technical Specifications	174
5.6.3	Transmission of the Data	174

5.6.4	Relation to the Right to Erasure	175
5.6.5	Exclusion of the Right to Data Portability	175
5.7	Right to Object	176
5.7.1	Grounds for an Objection to Processing	177
5.7.2	Exercise of the Right and Legal Consequences	179
5.7.3	Information Obligation	180
5.8	Automated Decision-Making	180
5.8.1	Scope of Application of the Prohibition	181
5.8.2	Exceptions from the Prohibition	183
5.8.3	Appropriate Safeguards	184
5.9	Restrictions of the Data Subjects' Rights	184
	References	185
6	Interaction with the Supervisory Authorities	189
6.1	Determination of the Competent Supervisory Authority	189
6.2	One-Stop-Shop Mechanism	191
6.3	Determination of the Competent Lead Supervisory Authority	192
6.3.1	Determination Based on an Entity's Main Establishment	192
6.3.2	Determination in the Absence of an EU Establishment	195
6.3.3	Exception: Local Competences	195
6.4	Cooperation and Consistency Mechanism	197
6.4.1	European Data Protection Board	197
6.4.2	Cooperation Mechanism	198
6.4.3	Consistency Mechanism	198
	References	199
7	Enforcement and Fines Under the GDPR	201
7.1	Tasks and Investigative Powers of the Supervisory Authorities	201
7.1.1	Greater Consistency of Investigative Powers Throughout the EU	202
7.1.2	Scope of Investigative Powers	202
7.1.3	Exercise of the Powers	204
7.2	Civil Liability	204
7.2.1	Right to Claim Compensation	205
7.2.2	Liable Parties	207
7.2.3	Exemption from Liability	208
7.3	Administrative Sanctions and Fines	208
7.3.1	Corrective Powers of the Supervisory Authorities	209
7.3.2	Grounds for and Amounts of Administrative Fines	210
7.3.3	Imposition of Fines, Including Mitigating Factors	211
7.3.4	Sanctioning of Groups of Undertakings	212
7.3.5	Practical Implications	213

7.4	Judicial Remedies	214
7.4.1	Remedies Available to Data Processing Entities	214
7.4.2	Remedies Available to Data Subjects	215
	References	216
8	National Peculiarities	219
8.1	Various Opening Clauses	219
8.1.1	Opening Clauses Included in General Provisions of the GDPR	219
8.1.2	EU Member State Competence for Specific Processing Situations	223
8.2	Employee Data Protection	224
8.2.1	Opening Clause	225
8.2.2	Co-determination Bodies Provided for in Selected EU Member States	226
8.3	Telemedia Data Protection	230
	References	232
9	Special Data Processing Activities	235
9.1	Big Data	235
9.1.1	Applicability of the GDPR	236
9.1.2	Accountability	237
9.1.3	Safeguarding the Basic Principles of Lawful Processing	237
9.2	Cloud Computing	238
9.2.1	Allocation of Responsibilities	239
9.2.2	Choosing a Suitable Cloud Service Provider	239
9.2.3	Third-Country Cloud Service Providers	240
9.3	Internet of Things	240
9.3.1	Legal Basis for Processing in the IoT	241
9.3.2	Privacy by Design and Privacy by Default	242
	References	242
10	Practical Implementation of the Requirements Under the GDPR	245
10.1	Step 1: ‘Gap’ Analysis	246
10.2	Step 2: Risk Analysis	246
10.3	Step 3: Project Steering and Resource/Budget Planning	247
10.4	Step 4: Implementation	247
10.5	Step 5: National Add-On Requirements	249
	References	249
	Annex I: Juxtaposition of the Provisions and Respective Recitals of the GDPR	251
	Index	381