

Rücker / Kugler

# New European General Data Protection Regulation

A Practitioner's Guide

C.H.BECK · HART · NOMOS

Rücker / Kugler  
New European General Data Protection Regulation

# New European General Data Protection Regulation

A Practitioner's Guide

Ensuring Compliant Corporate Practice

edited by

Dr. Daniel Rücker, LL.M.

Tobias Kugler

2018

C.H.BECK · HART · NOMOS

*Published by*

Nomos Verlagsgesellschaft, Waldseestraße 3-5, 76530 Baden-Baden, Germany,  
email: [vertrieb@nomos.de](mailto:vertrieb@nomos.de)

*Co-published by*

Verlag C.H.BECK oHG, Wilhelmstraße 9, 80801 München, Germany,  
email: [bestellung@beck.de](mailto:bestellung@beck.de)

and

Hart Publishing, Kemp House, Chawley Park, Cumnor Hill, Oxford, OX2 9PH, United Kingdom,  
email: [orders@isbs.com](mailto:orders@isbs.com)

Published in North America (US and Canada) by Hart Publishing,  
c/o International Specialized Book Services,  
930 NE 58<sup>th</sup> Avenue, Suite 300, Portland, OR 97213-3786, USA,  
email: [orders@isbs.com](mailto:orders@isbs.com)

ISBN 978-3-8487-3262-3 (Nomos Print)

ISBN 978-3-8452-7609-0 (Nomos ePDF)

ISBN 978-3-406-69536-0 (C.H.BECK)

ISBN 978-1-5099-2060-0 (Hart Publishing)

First Edition 2018

© Nomos Verlagsgesellschaft, Baden-Baden 2018. Printed in Germany.

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically those of translation, reprinting, re-use of illustrations, broadcasting, reproduction by photocopying machine or similar means, and storage in data banks. Under § 54 of the German Copyright Law where copies are made for other than private use a fee is payable to »Verwertungsgesellschaft Wort«, Munich.

## Foreword

Digitalisation is advancing rapidly, and enterprises across Europe and the world are swiftly adapting their business processes and products to bring them into the new digital age. At the very heart of this business adaptation is the processing of personal data, which has increased significantly over recent decades and which has become one of the core assets of digital business.

Data protection law is still fragmented across Europe under the current data protection Directive 95/46/EC and its various national implementations. To unify data protection law in Europe and to improve the protection of fundamental rights, the new European General Data Protection Regulation (“GDPR”) introduces uniform data protection legislation that will apply directly in all European Member States from 25 May 2018. The GDPR will also serve as a binding legal framework for countless companies outside the EU that do business in the Union.

This handbook clearly and concisely addresses the legal pitfalls and compliance requirements resulting from the GDPR and explains in detail the new situation under the law. It was written to fully embrace the new European approach to data protection by focusing on the debate among legal professionals and on legal sources at European level. There is a wealth of expert legal commentary on national law, but the European debate, mandatory from 25 May 2018, still lacks comprehensive expert literature on the practical questions of data processing. Conceived as a guide for legal professionals in their day-to-day practice, this book is intended to help fill that gap using practical examples and scenarios to assist companies affected by the GDPR.

Giving comprehensive insight into the GDPR, this handbook starts with a chapter on the regulatory background (Development and importance of the data protection reform) and the essential material and personal scope of the GDPR (Scope of application of the GDPR). Subsequently, the consequences of a strictly European legal framework and rules for a consistent and uniform interpretation of the GDPR are presented in detail. Another key issue is the fundamental principles of lawful data processing under the GDPR for any company (Lawful processing of personal data in companies under the General Data Protection Regulation), including the newly introduced compatibility test. The chapter General conditions for data processing in companies under the GDPR deals with particular legal requirements to be implemented by companies. The legal assessment also addresses subjects such as the increased duties towards the data subjects and their rights, including the right to be forgotten, data portability as well as the question of group privileges and the issue of drastically increased administrative fines and damages. Finally, the chapter on Practical examples addresses inevitable aspects of data management such as cloud computing, outsourcing and data transfer to third countries outside the EU. This chapter also provides general guidance to any business for successfully exploring data as an asset.

## *Foreword*

This includes direct marketing as well as (user) profiling and compliance issues in app development.

We would like to thank everyone involved in bringing this book into existence. We owe our deepest gratitude to our co-authors as well as to Charlotte Fischer, Patricia Gola, Stefanie Schneider, Sarina Schwake, Victoria Copeland and Patricia Cress for their contribution to this handbook.

September 2017  
Munich/Frankfurt

Daniel Rücker  
Tobias Kugler

## Summary of Contents

Contributors .....	XXV
List of Abbreviations .....	XXVII
A. Development and Importance of the Data Protection Reform .....	1
I. Legislative procedure and legal basis of the GDPR .....	1
II. Importance of the GDPR for companies .....	8
B. Scope of application of the GDPR .....	9
I. Material scope of application .....	9
II. Personal scope of application of the GDPR .....	23
III. Territorial scope of application of the GDPR – Change from the principle of territoriality to effects doctrine .....	37
IV. Limits of the scope of application .....	41
C. Lawful processing of personal data in companies under the General Data Protection Regulation .....	49
I. Principles relating to processing of personal data from a business perspective .....	49
II. Key requirements for lawful processing of personal data from a business perspective .....	75
D. General conditions for data processing in companies under the GDPR	105
I. Data privacy in private companies .....	105
II. Codes of Conduct .....	120
III. Data protection certifications and privacy seals – relevance of these instruments for business entities .....	123
IV. Duties towards the data subjects and their rights .....	127
V. Cooperation between companies and the supervisory authorities .....	155
VI. Appointment and role of an internal or external data protection officer (“DPO”) .....	175
VII. Risks of Liability for breaches of data protection law .....	186

*Summary of Contents*

E. Practical examples .....	195
I. Transfer of personal data to third countries .....	195
II. Outsourcing .....	221
III. Processing of special categories of personal data .....	235
IV. Direct Marketing .....	243
V. Profiling .....	264
VI. Company Website .....	275
VII. Apps .....	279
Index .....	287

## Contents

Contributors .....	XXV
List of Abbreviations .....	XXVII
A. Development and Importance of the Data Protection Reform .....	1
I. Legislative procedure and legal basis of the GDPR .....	1
1. Key steps within the legislative procedure .....	1
2. Main objectives of the Data Protection Reform .....	1
a) Harmonisation of the level of protection .....	1
b) Adaption to the technical progress .....	3
c) Strengthening the rights of data subjects .....	3
d) Free movement of personal data .....	3
e) One-Stop-Shop-Principle .....	4
3. Legal basis of the GDPR and direct applicability .....	4
a) Legal basis .....	4
aa) Legislative power and legal basis for adopting the GDPR .....	4
bb) Fundamental rights in context with data protection .....	5
b) Direct Applicability .....	5
4. Rules for a consistent and uniform interpretation of the GDPR .....	6
a) Need for a uniform European interpretation .....	6
b) Guidelines for a uniform interpretation .....	6
aa) Interpretation Guidelines provided by the GDPR itself .....	6
(1) Actual wording of the GDPR .....	6
(2) Statements of supervisory authorities .....	7
(3) Statements issued by the European Data Protection Board and the Art. 29 Working Party .....	7
bb) Other suitable sources for interpreting the GDPR ..	8
II. Importance of the GDPR for companies .....	8

B. Scope of application of the GDPR .....	9
I. Material scope of application .....	9
1. “Processing” of personal data .....	9
a) Processing subject to the GDPR .....	9
aa) Definition of “Processing” .....	10
bb) Processing by manual means .....	10
b) Limits to the material scope of application of the GDPR .....	11
aa) Limits of applicability resulting from the technical way of processing .....	11
bb) Household exemption .....	12
2. Personal data .....	12
a) “Any information” suitable for potentially being personal data .....	14
b) Relationship required between the information and the data subject .....	15
c) Requirements for identifiability of the data subject .....	16
aa) Identified natural person .....	16
bb) Identifiability of a natural person – relevant criteria and threshold .....	17
(1) Direct or indirect identifiability .....	17
(2) Criteria for determining indirect identifiability .....	18
(3) Decision of the European Court of Justice on IP addresses .....	19
d) Anonymous and anonymised data .....	19
e) Pseudonymisation .....	20
f) Encrypted data .....	21
3. Data subjects – natural persons .....	21
a) Dead persons .....	21
b) Legal persons .....	22
aa) No protection under the GDPR .....	22
bb) Indirect protection and protection under national law .....	22
4. Consequences of inapplicability of the GDPR .....	23
II. Personal scope of application of the GDPR .....	23
1. Controller .....	24
a) Determination of the responsible body – natural person, legal person or any other body .....	25
b) Power to determine “purposes and means” of data processing – distinguishing controllers and processors .....	25
aa) Criteria for “determining” the relevant purposes and means .....	25
(1) Determination by law .....	26
(2) Determination by way of factual influence .....	26

bb) “Purposes and means” of data processing .....	27
cc) Determination of the “purposes”/“why” of processing .....	27
dd) Determination of the “means”/“how” of processing .....	27
c) Joint controllers – joint responsibility .....	28
aa) Requirements for joint control under the GDPR ....	28
bb) Consequences of a joint controllership .....	29
(1) No privilege for transferring personal data between joint controllers .....	29
(2) Transparent allocation of responsibilities .....	30
(3) Joint liability .....	30
2. Processor .....	30
a) Processing personal data “on behalf of a controller” .....	31
aa) No factual influence of the processor on determining the purposes and means of processing .....	31
bb) Processor subject to the instructions of the data controller .....	31
cc) Factual compliance with the instructions of the data controller .....	32
b) Requirements for engaging a processor .....	32
aa) Mandate of the processor .....	32
bb) Choice of the right processor – provision of sufficient guarantees by the processor .....	32
cc) Processing contract .....	33
dd) Necessary content of a processing contract .....	33
c) Further explicit obligations of processors .....	34
aa) Appropriate technical and organisational measures .....	34
bb) Data protection officer .....	35
cc) Records of processing activities .....	35
d) Lawfulness of a data transfer to a data processor .....	35
e) Consequence each of the contractual relationship for the processor .....	35
f) How to handle former mandates .....	36
3. Micro, small and medium-sized enterprises .....	36
III. Territorial scope of application of the GDPR – Change from the principle of territoriality to effects doctrine .....	37
1. Companies with an establishment in the EU (GDPR, art. 3, para 1) .....	37
2. Companies without any establishment in the EU (GDPR, art. 3, para 2) .....	38
a) Offering of goods or services to data subjects in the EU .....	38
b) Monitoring the behaviour of subjects in the EU .....	40

3. Application by virtue of public international law (GDPR, art. 3, para 3) .....	40
4. Summary assessment on changed scope of application .....	40
IV. Limits of the scope of application .....	41
1. Basic principle: direct application of the Regulation irrespective of many opening clauses .....	41
2. Remaining scope and amendments of national data protection laws and relevant examples for application of national data protection laws .....	41
a) Data processing in employment contexts, GDPR, art. 88	41
b) Designation of a data protection officer in cases other than GDPR, art. 37, para 1 .....	43
c) Processing carried out in the public interest or in compliance with a legal obligation .....	44
d) Automated decisions and profiling .....	45
e) Joint controllers .....	45
f) Further examples .....	45
3. Data protection for online and electronic communication services .....	46
4. Data protection at public bodies .....	47
 C. Lawful processing of personal data in companies under the General Data Protection Regulation .....	 49
I. Principles relating to processing of personal data from a business perspective .....	49
1. Principle of lawfulness, fairness and transparency .....	50
a) Notion of lawfulness .....	50
aa) General prohibition of processing personal data ....	51
bb) Legitimate basis for processing personal data as an exception .....	51
b) Notion of fairness .....	51
c) Notion of transparency .....	52
d) No principle of collecting personal data directly from the data subject .....	53
2. Principle of purpose limitation .....	53
a) Collection for specified, explicit and legitimate purposes .....	54
aa) “Specified” purpose .....	55
bb) “Explicit” purpose .....	56
cc) “Legitimate” purpose .....	56

b)	No further processing in a manner that is incompatible with the specified, explicit and legitimate purposes of the preceded collection .....	57
aa)	(In)compatibility test requirement .....	57
bb)	Notion of “further processing” and scope of compatibility test .....	58
cc)	Exceptions from the requirement of a compatibility test .....	59
(1)	Assumed compatibility of further use for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes .....	59
(2)	Explicit legal exceptions from compatibility test .....	60
dd)	Compatibility test .....	60
(1)	No change of purpose .....	60
(2)	Change of purpose .....	61
ee)	Key factors for the compatibility test .....	61
(1)	Link between the purposes .....	62
(2)	Context in which the personal data have been collected .....	62
(3)	Nature of the personal data .....	63
(4)	Possible consequences of the intended further processing .....	63
(5)	Existence of appropriate safeguards .....	63
ff)	Consequences of compatibility and incompatibility .....	64
(1)	Consequences of incompatibility .....	64
(2)	Consequences of compatibility .....	64
gg)	Documentation of compatibility test .....	65
3.	Data minimisation .....	65
a)	Notion of “necessity” .....	65
b)	Anonymisation and pseudonymisation .....	67
c)	Concept of data protection by design and by default .....	67
4.	Accuracy .....	67
a)	Notion of “accurate data” .....	68
b)	Updating of inaccurate data .....	68
c)	Erasure and rectification of inaccurate data .....	69
5.	Storage limitation .....	70
a)	Notion of “necessity” .....	70
b)	Exception for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes .....	70

c) Erasure, restriction and anonymisation of personal data no longer necessary .....	71
d) Processing which does not require identification .....	71
6. Integrity and confidentiality .....	72
7. Accountability .....	73
a) Notion of accountability .....	73
b) Possibilities to demonstrate compliance .....	74
II. Key requirements for lawful processing of personal data from a business perspective .....	75
1. Relevance and importance of the different legal grounds of the GDPR for processing of personal data from a business perspective .....	75
2. Legitimation of data processing by law .....	76
a) Contract or pre-contractual relations .....	77
aa) Performance of a contract to which the data subject is party .....	77
bb) Steps at the request of the data subject prior to entering into a contract .....	78
b) Legal obligation .....	79
aa) Sources for legal obligations .....	79
bb) Quality of legal basis and additional national provisions .....	79
c) Vital interests .....	80
d) Public interest or exercise of official authority .....	81
aa) Relevance for the private sector .....	81
bb) Legal basis for public interests or official authority .....	81
cc) Quality of legal basis and additional national provisions .....	82
e) Legitimate interests .....	82
aa) Legitimate interests pursued by the controller or by a third party .....	82
bb) Interests or fundamental rights and freedoms of the data subject .....	84
cc) Balancing test .....	84
(1) Assessment of nature and source of the legitimate interest .....	86
(2) Assessment of impact on data subjects .....	87
(3) Provisional balance .....	89
(4) Assessment of additional safeguards and final balance .....	89
(5) Documentation of balance test .....	90

3. Legitimation of data processing by consent .....	90
a) Notion of consent .....	90
aa) Indication of data subject's wishes signifying agreement .....	91
(1) Statement or clear affirmative action .....	91
(2) Written or oral consent .....	92
(3) Consent by electronic means .....	92
(4) Implied consent .....	92
(5) Limitation to processing of personal data of the data subject .....	93
bb) Freely given .....	93
(1) Clear imbalance between controller and data subject .....	93
(2) Horizontal and vertical restriction of interconnection .....	94
cc) Specific .....	95
dd) Informed .....	95
ee) Unambiguous .....	95
b) Consent in the context of a written declaration which also concerns other matters .....	96
c) Consent of data subjects lacking full legal capacity, in particular children .....	97
aa) Consent of children in relation to information society services .....	97
(1) Information society services .....	97
(2) Direct offer to a child .....	97
(3) Age thresholds .....	97
(4) Age and authorisation verification mechanisms .....	98
bb) Other consent of children and other data subjects lacking full legal capacity .....	99
d) Ability to demonstrate consent .....	99
e) Right to withdraw consent .....	100
f) Need for adaption and obtaining renewed consent .....	100
4. Processing of special categories of personal data .....	101
a) Additional requirement of a legal ground .....	101
b) Explicit consent .....	102
c) Statutory exceptions .....	102
d) Further conditions pursuant to Member State law .....	103
5. Processing of personal data relating to criminal convictions and offences .....	103

D. General conditions for data processing in companies under the GDPR	105
I. Data privacy in private companies	105
1. Company as controller	105
2. Concept of Joint Controllers (GDPR, art. 4, no. 7 and GDPR, art. 26)	105
a) Definition	105
b) Forms	106
c) Allocation of responsibilities between Joint Controllers	106
aa) Fulfilment of data subject's rights	107
bb) Fulfilment of obligations to inform pursuant to GDPR, art. 13 and 14	107
d) Formal requirements, GDPR, art. 26, para 2, sentence 2	108
e) Joint and several responsibility and liability vis-a-vis data subject	108
f) Administrative fine	108
3. Group Privilege?	108
a) Principle: no group privilege	108
b) Group privilege via concept of joint controllers	109
c) Affiliation as a reasonable interest within GDPR, art. 6, para 1, subpara f) and Recital 48	109
4. Responsibility for GDPR-compliance	109
5. Controllers/processors not established in the European Union, GDPR, art. 27	110
6. Records of processing activities, GDPR, art. 30	111
7. Data protection by design and default, GDPR, art. 25	111
a) Data protection by design	112
b) Data protection by default	112
c) Possible measures and scope	113
d) Administrative fine	113
8. Data security, GDPR, art. 32	114
a) Risk evaluation	114
b) Appropriate measures	114
c) Control of subordinate natural persons	114
d) Administrative fine	115
9. Data Protection Impact Assessment, GDPR, art. 35 and 36	115
a) In which cases Data Protection Impact Assessments are to be carried out?	116
b) Minimum content of Data Protection Impact Assessments	117
c) Prior Consultation, GDPR, art. 36	119
d) Administrative fines	119
II. Codes of Conduct	120
1. Drafting codes of conduct (GDPR, art. 40, para 2)	120

2. Approval procedure .....	121
3. Monitoring of approved codes of conduct .....	121
4. Relevance for business entities .....	122
III. Data protection certifications and privacy seals – relevance of these instruments for business entities .....	123
1. Purpose of certifications and seals (GDPR, art. 42, paras 1 and 4) .....	124
2. Voluntariness (GDPR, art. 42, para 3) .....	124
3. Certification bodies (GDPR, art. 42, para 5 and GDPR, art. 43) .....	124
4. Certification Proceeding, GDPR, art. 42, para 6 .....	125
5. Maximum term of certificate/seal, GDPR, art. 42, para 7 ...	126
6. Register for certifications, data protection seals and marks	126
7. Relevance of certifications or seals for companies .....	126
IV. Duties towards the data subjects and their rights .....	127
1. General Requirements related to the rights of data subjects, GDPR, art. 11 and 12 .....	127
a) Deadline for fulfilment of data subject’s rights: One month pursuant to GDPR, art. 12, para 3 .....	127
b) Form requirements .....	128
c) Right to determine identity of individual wishing to enforce their rights pursuant to GDPR, art. 12, para 6: Controller’s right to request a copy of the claimant’s passport .....	129
d) Processing which does not require identification, GDPR, art. 11, para 2 and no right to refuse (GDPR, recital 57) .....	130
e) Free of charge, GDPR, art. 12, para 5 .....	130
f) Information on legal remedies available, GDPR, art. 12, para 4 .....	130
g) Administrative fines .....	131
2. Information to be provided, GDPR, art. 13 and 14 .....	131
a) Information duties .....	131
b) Point in time .....	134
c) Exceptions of the information duties .....	135
d) Administrative fines .....	135
3. Right of access by the data subject, GDPR, Art. 15 .....	136
a) Obligation to provide information, GDPR, art. 15, para 1 .....	136
b) Right of access, GDPR, art. 15, para 3 .....	137
c) Exceptions, GDPR, art. 15, para 4 .....	137
d) Administrative fines .....	138

4. Rectification, GDPR, art. 16 .....	138
a) Correction .....	138
b) Completion .....	138
5. Right to Erasure/Right to be forgotten, GDPR, art. 17 .....	139
a) Prerequisites for right to erasure pursuant to GDPR, art. 17, para 1 .....	139
b) Exceptions, GDPR, art. 17, para 3 .....	140
c) Right to be forgotten, GDPR, art. 17, para 2 and GDPR, art. 19 .....	141
d) Administrative fines .....	142
6. Right to restriction of processing, GDPR, art. 18 .....	142
7. Data Portability, GDPR, art. 20 .....	144
a) Prerequisites .....	144
b) Performance of data portability .....	145
c) What means “portability”? .....	145
d) Receiving data controller .....	146
e) Exceptions, GDPR, art. 20, paras 3 and 4 .....	146
f) Administrative fines .....	146
8. Right to object, GDPR, art. 21 .....	147
a) Right to object to processing for direct marketing purposes .....	147
b) Obligation to inform the data subject about his right to object .....	148
c) Modalities to exercise the right to object .....	148
d) Deadline for the controller to respond to an objection ...	148
e) Right to object to processing personal data for scientific or historical research purposes or statistical purposes pursuant to GDPR, art. 89, para 1 .....	149
f) Administrative fines .....	149
9. Right not to be subject to automated individual decision- making, GDPR, art. 22 .....	149
a) Legal or similar significant effects .....	149
b) Exceptions and examples .....	150
c) Right to review .....	151
d) Special categories of personal data .....	151
e) Administrative fines .....	152
10. Data breach notification to data subject, GDPR, art. 34 .....	152
a) Obligation of the controller to notification .....	152
b) Minimum content and form .....	153
c) Exceptions .....	154
d) Administrative fines .....	155

V. Cooperation between companies and the supervisory authorities .....	155
1. Competent authority – one stop shop .....	155
a) Concept of lead and concerned authority .....	157
b) Cooperation between authorities .....	160
c) Consistency mechanism GDPR, art. 63 .....	161
2. Duty to cooperate (GDPR, art. 31) .....	163
3. Data breach notification to the supervisory authorities (GDPR, art. 33) .....	164
4. Tasks and enforcement powers of the supervisory authorities .....	167
a) Tasks of the supervisory authorities .....	167
b) Enforcement empowerments .....	169
c) Administrative fines, GDPR, art. 83 .....	172
VI. Appointment and role of an internal or external data protection officer (“DPO”) .....	175
1. Obligation to appoint a DPO, GDPR art. 37, para 1 .....	176
a) Risk based approach, GDPR, art. 37, para 1 .....	176
b) Criteria to appoint a DPO in GDPR, art. 37, para 1, subparas b) and c) .....	176
c) Processing on a large scale .....	177
d) Regular and systematic monitoring of the data subjects .....	177
e) Special categories of personal data .....	177
f) Data relating to criminal convictions and offences .....	178
2. Addresses of the obligation to appoint a DPO .....	178
a) Controllers .....	178
b) Processors .....	179
3. Infringement to appoint a DPO .....	179
4. Group privilege, GDPR, art. 37, para 2 .....	179
5. Internal/external, GDPR, art. 37, para 6 .....	180
6. Full or part time .....	180
7. Qualification, GDPR, art. 37, para 5 .....	181
8. Publication/communication contact details, GDPR, art. 37, para 7 .....	181
9. Role of the DPO, GDPR, art. 38 .....	182
a) Secrecy obligation .....	182
b) No instructions, privileged status .....	182
c) Information obligation .....	183
d) Necessary resources .....	183
e) Direct reporting line, GDPR, art. 38, para 3, third sentence .....	184
f) Contact for data subjects .....	184

10. Tasks of a DPO, GDPR, art. 39 .....	185
a) Inform .....	185
b) Monitor .....	185
c) Advice .....	185
d) Cooperate with authorities/contact point .....	185
VII. Risks of Liability for breaches of data protection law .....	186
1. Administrative fines under the GDPR .....	186
a) Levels of fines .....	186
aa) Level 1 infringements .....	186
bb) Level 2 infringements .....	187
cc) Concept of “undertaking” .....	187
dd) Further criteria .....	188
b) Enforcement .....	189
aa) Ex officio proceedings .....	189
bb) Administrative complaints (GDPR, art. 77 and 78) .....	189
cc) Proceedings against data controllers and data processors (GDPR, art. 79) .....	190
dd) Capacity to sue for non-profit bodies, organisations or associations mandated by the data subject (GDPR, art. 80) .....	190
2. Damages based on the GDPR .....	191
a) Concept of damage .....	191
b) Relevant infringements .....	192
c) Exemption .....	192
d) Joint processing .....	192
3. Liability based on national laws .....	193
E. Practical examples .....	195
I. Transfer of personal data to third countries .....	195
1. Adequate level of protection .....	196
a) Procedure of implementing an adequacy decision .....	196
b) Adequacy decisions under Directive 95/46 .....	197
c) Special case: United States (Safe Harbour/EU-U.S. Privacy Shield) .....	198
2. Appropriate safeguards .....	201
a) Binding Corporate Rules .....	202
aa) Binding Corporate Rules under Directive 95/46 .....	203
bb) Procedure to implement Binding Corporate Rules .....	205
b) Standard Data Protection Clauses .....	207
aa) Standard Contractual-Clauses under Directive 95/46 .....	207
bb) Implementation and use of Standard Data Protection Clauses .....	208

c) Codes of conduct .....	209
d) Certification .....	210
e) Individual authorisation of contractual clauses .....	211
3. Derogations for specific situations .....	212
a) Consent of the data subject .....	213
b) Performance of a contract .....	214
c) Interest of the data subject .....	215
d) Public interest .....	215
e) Legal claims .....	216
aa) Interpretation of derogation Directive 95/46, art. 26, para 1, subpara d) .....	216
bb) Uniform Interpretation and framework under the GDPR .....	218
cc) Transfers or disclosures not authorised by Union law .....	219
f) Vital interests .....	219
g) Public register .....	220
h) Special justification .....	220
II. Outsourcing .....	221
1. Controller or processor .....	222
2. Data processing .....	223
a) Selection of service provider and commissioning as processor .....	223
b) Processors in third countries .....	223
aa) Standard data protection clauses .....	223
bb) Binding Corporate Rules .....	225
cc) Approved codes of conduct and approved certifications .....	226
dd) Other measures .....	226
ee) Derogations .....	226
3. Sub-processing .....	227
a) General provisions applicable to sub-processing .....	227
aa) Prior authorisation .....	227
bb) Contract between processor and sub-processor .....	228
cc) Liability .....	229
b) Third country transfers .....	229
aa) Processor and sub-processor in third countries .....	229
bb) Processor in the EU and sub-processor in a third country .....	230
4. Example: Cloud computing .....	232
a) Cloud computing rollout and service models .....	232
b) Cloud computing and data protection .....	233
aa) Roles and responsibilities of parties involved .....	233

bb) Commissioning as data processing and sub-processing .....	234
cc) Documentation and information obligations .....	235
III. Processing of special categories of personal data .....	235
1. Special categories of personal data .....	236
a) Genetic data .....	236
b) Biometric data .....	236
c) Data concerning health .....	237
2. Specific prohibition with exceptions .....	237
a) Explicit Consent .....	237
b) Statutory exceptions .....	238
aa) Employment, social security and social protection law .....	239
bb) Vital interests .....	239
cc) Foundation, association or any other not-for-profit body .....	240
dd) Personal data manifestly made public .....	240
ee) Legal claims .....	240
ff) Substantial public interest .....	241
gg) Processing for medical purposes .....	241
hh) Public interest in the area of public health .....	242
ii) Archiving purposes in the public interest, scientific or historical research purposes or statistical purposes .....	242
jj) Limitations in Member State law .....	243
3. Additional protective measures .....	243
IV. Direct Marketing .....	243
1. Definition of direct marketing .....	244
2. Direct Marketing in Directive 95/46 and the GDPR .....	244
3. ePrivacy-Directive and Unfair Commercial Practices Directive .....	245
a) Directive 2002/58/EC (ePrivacy-Directive) .....	245
b) Directive 2005/29/EC (Unfair Commercial Practices Directive) .....	246
4. General requirements .....	247
a) Right to object .....	247
aa) GDPR .....	247
bb) Directive 2002/58/EC (ePrivacy-Directive) .....	248
b) Right to obtain erasure .....	249
c) Principle of transparency .....	250
d) Principle of purpose limitation .....	251

5. Legitimation of advertising by consent .....	252
a) Requirements for consent .....	252
aa) Freely given .....	253
bb) Pre-formulated declaration of consent .....	254
cc) Time limit .....	254
b) Right to withdraw consent .....	254
6. Legitimation of advertising by law .....	254
a) Contract or pre-contractual relations .....	255
b) Advertising based on legitimate interests .....	256
7. Use cases .....	257
a) Electronic mail .....	258
aa) Obligatory prior consent (opt-in) .....	258
bb) Exceptions .....	259
cc) Transparency and information .....	259
b) Telemarketing .....	260
aa) Automated calling .....	260
bb) Direct marketing voice-to-voice calls .....	261
cc) ePrivacy Regulation .....	261
c) Postal advertising .....	261
d) Sweepstake .....	262
e) Tell-a-friend .....	262
f) Address trading .....	263
V. Profiling .....	264
1. Definition of profiling .....	264
2. General requirements .....	265
a) Data protection impact assessment .....	265
b) Purpose limitation .....	265
c) Data minimisation .....	266
d) Obligation to inform .....	266
e) Right to object .....	266
f) Privacy by design and by default .....	267
3. Cookies (and similar technologies) .....	267
a) ePrivacy-Directive .....	268
b) Consent to the use of cookies .....	269
4. Use cases .....	271
a) Statistical and aggregate data .....	271
b) Online Behavioural Advertising .....	271
aa) Roles and responsibilities .....	272
bb) Legal basis .....	273
cc) Obligation to inform .....	273
dd) Further obligations .....	274
c) Customer Relationship Management .....	274

## Contents

VI. Company Website .....	275
1. Web analytics .....	275
2. Social media .....	276
a) Social media page .....	276
b) Social plugins .....	277
3. Privacy policy .....	278
4. Right to be forgotten .....	278
VII. Apps .....	279
1. Roles and Responsibilities .....	279
a) App developers .....	279
b) App store operators .....	280
c) OS and device manufactures .....	280
2. Legal basis .....	281
a) Consent .....	281
b) Processing necessary for performance of a contract .....	282
c) Legitimate interests .....	283
3. Geolocation .....	283
4. Privacy Policy .....	284
Index .....	287

## Contributors

### **Sebastian Dienst**

Lawyer at Noerr LLP, Munich, Germany

*Chapter C: Lawful processing of personal data in companies*

### **Tobias Kugler**

Lawyer/Associated Partner at Noerr LLP, Frankfurt am Main, Germany

*Foreword*

*Chapter E: Practical examples (1<sup>st</sup> Part)*

Dr. **Daniel Rücker**, LL.M. (University of New South Wales, Sydney)

Lawyer/Partner at Noerr LLP, Munich, Germany

*Foreword*

*Chapter A: Development and Importance of the Data Protection Reform*

*Chapter B: Scope of application (1<sup>st</sup> Part)*

### Professor Dr. **Joachim Schrey**

Lawyer and Expert Lawyer in IT-Law/Partner at Noerr LLP, Frankfurt am Main, Germany

Honorary professor at Goethe University Frankfurt am Main

*Chapter D: Data privacy in private companies (1<sup>st</sup> Part)*

### **Pascal Schumacher**,

Lawyer at Noerr LLP, Berlin, Germany

*Chapter B: Scope of application (2<sup>nd</sup> Part)*

*Chapter D: Data privacy in private companies (2<sup>nd</sup> Part)*

### **Eva Irene Wille**, LL.M. (UCLA)

Judge at the Local Court Frankfurt am Main, Germany

*Chapter E: Practical examples (2<sup>nd</sup> Part)*



## List of Abbreviations

AG	Advocate General
art.	Article
BCR	Binding Corporate Rules
cf.	see, compare
CFI	Court of First Instance
CJEU	Court of Justice of the European Union
DPIA	Data protection impact assessments
DPO	Data protection officer
EC	European Community
ECHR	European Court of Human Rights
ECLR	European Competition Law Review
ECR	European Court Reports
ed.	Editor
EEA	European Economic Area
EDPL	European Data Protection Law Review
EFTA	European Free Trade Association
EJIL	European Journal of International Law
EJRR	European Journal of Risk Regulation
EJSL	European Journal of Social Law
EJSS	European Journal of Social Security
ELJ	European Law Journal
E.L.Rev.	European Law Review
EP	European Parliament
ePrivacy-Directive	Directive 2002/58/EC
ESC	European Social Charter
et al.	and others
et seq.	following
EU	European Union
EuGRZ	Europäische Grundrechte-Zeitschrift
EULF	The European Legal Forum
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
GDPR	General Data Protection Regulation
laaS	Infrastructure as a Service
ibid.	cited in preceding footnote
ILO	International Labour Organization
infra	see below
IR	Implementing Regulation, Reg. No. 987/2009
JCMS	Journal of Common Market Studies
mn.	Margin Number (Randnummer)
NATO	North Atlantic Treaty Organization
NJW	Neue Juristische Wochenschrift
NZS	Neue Zeitschrift für Sozialrecht
OJ	Official Journal
OMC	Open Method of Coordination
p.	page/s

## *List of Abbreviations*

PaaS	Platform as a Service
para.	Paragraph
RAE	Revue des Affaires Européennes
RBSS	Revue Belge de sécurité sociale (The same articles are published in Dutch by BTSZ)
RDSS	Revue de droit sanitaire et social
REDS	Revue européenne du Droit Social
Reg.	Regulation
RISS	Revue international de sécurité sociale
RLM	Revue de l'Union Européenne (former Revue du marché commun)
RSV	Rechtspraak Sociale verzekeringen (Case-law in social security)
RTDE	Revue trimestrielle de droit européen
SaaS	Software as a Service
SEW	Tijdschrift voor Europees en economisch recht (Journal for European and economic law)
SGb	Die Sozialgerichtsbarkeit
supra	see above
SZS	Schweizerische Zeitschrift für Sozialversicherung und berufliche Vorsorge
TEU	Treaty on European Union
TFEU	Treaty on the functioning of the European Union
ZD	Zeitschrift für Datenschutz (Journal)