

Contents

Preface	V
Abbreviations	XIII
Legend	XV
Bibliography	XVII
List of Figures	XXI
A. Introductory remarks	1
I. Why Big Data?	1
II. Why must a party not established in the EU comply with GDPR with respect to Big Data applications?	1
1. General principles	1
2. Companies established in the EU (Art. 3 (1) GDPR)	2
3. Companies not established in the EU (Art. 3 (2) GDPR)	2
4. Offering of goods or services to data subjects in the EU	2
5. Monitoring the behaviour of subjects in the EU	4
6. Data processing facilities in a place where Member State law applies (Art. 3 (3) GDPR)	4
7. Limits of the scope of application – opening clauses	4
8. Most relevant opening clauses in the GDPR	5
a) Data processing in employment contexts (Art. 88 GDPR)	5
b) Designation of a data protection officer in cases other than Art. 37 (1) GDPR	6
c) Processing carried out in the public interest or in compliance with a legal obligation	6
9. Summary	6
III. Which data are affected?	7
IV. What are the differences between the data types?	8
V. Which verification steps need to be considered for a Big Data application?	11
B. Types of data	15
I. Personal data	16
1. Definition of “personal data” pursuant to Art. 4 (1) GDPR	16
2. Identifiability of personal data (Examples)	18
a) Dynamic IP addresses	18
b) Personnel or customer numbers	18
c) VIN/Vehicle registration numbers	19
d) Special categories of personal data	19
e) Location, traffic and usage data	20
f) Characteristics of specific data sources	21
aa) Social Media	21
bb) Open Data	23
cc) Data acquisition through Apps	23
II. Non-personal data	24
III. Databases and collections	25
1. Collections of works, data or other independent elements, § 4 German Copyright Act	26
2. Database protection rights	27
3. Protection of individual elements of a database or a collection	29
a) Database model	29
b) Data format	30
c) Interface	31
IV. Protection as business or trade secret	31
V. Householder’s right with regard to the collection of factual data	32
VI. Virtual householder’s right	33
VII. Factual data linked to IP addresses or other identifying characteristics	34
VIII. No data ownership	35

C. The controller	37
I. Processor	38
1. Controller-to-processor agreement (C2P)	39
2. Obligation to separate the databases	40
3. Other obligations of the processor	41
4. Securing instruments for compliance with data protection obligations of a controller of Big Data Applications with regard to the processor	41
a) Selection and prior checking	42
b) C2P agreement	42
II. Joint controllers, Art. 26 GDPR	43
1. Internal relationship between the joint controllers	44
2. Provision of the internal agreement	45
3. External Relationship Between the Joint Controllers and the Data Subject	45
III. Dynamic matrix structures	45
1. Participation in projects of multiple responsible entities	45
2. Employee secondment/supply of temporary staff	46
3. Joint controllers within the meaning of Art. 26 GDPR with regard to project participations	47
IV. Cloud computing	47
1. Storing in your own cloud	47
2. Use of third-Party cloud storage	48
D. Specific requirements and tasks of the data protection officer with regard to Big Data applications	49
I. Specialist knowledge	49
II. Organizational and operational involvement of the data protection officer	49
III. Communication with data subjects	50
IV. Information and monitoring obligations	50
V. Cooperation and control obligations	51
VI. Internal procedure in the event of a data protection violation	51
E. Lawful ground for data processing (collection, acquisition, transmission, evaluation and commercialization)	53
I. Statutory lawful grounds for personal data	54
1. Performance of a contract	57
2. Balance of interests	58
3. Works council agreements	59
4. Consent	60
a) Declaration of consent	62
b) Formal requirements	62
c) Free Will	63
d) Indication of the purpose of the collection and processing	64
e) Transmission to third parties, in particular to countries outside the EU	64
f) Right to withdraw consent	66
g) <i>Opt-in</i> and <i>opt-out</i> solutions	67
II. Processing of non-personal factual data	68
1. Processing of factual data	68
2. Obtaining data from data collections/databases	68
3. Obtaining data from Open Data projects	69
4. Data from publicly available sources	69
F. Data processing and data cycle (level of data purpose)	71
I. Data processing	71
II. Life cycle of data	71
III. Collection of personal data for purposes other than their use in Big Data applications – a change of purpose	73
1. The purpose of data collection and processing	73
2. The “purpose” of contracts for the supply and use of data	74
3. The problem of dynamic purpose changes in Big Data applications	74
a) The link between the original and new purpose	76

Contents

b) The context of data collection.....	76
c) The type of personal data.....	76
d) Possible consequences of the intended subsequent processing for the data subjects.....	76
e) The existence of appropriate guarantees.....	77
G. Third country transfer/Applicable law (Level of applicable law).....	79
H. Development of a Big Data application.....	83
I. Collection of data.....	84
II. Obtaining and acquiring data from data service providers.....	84
1. Legality of the collecting data provided by a data supplier.....	84
2. Legitimacy of data acquisition from third parties.....	85
3. Rectifying deficiencies.....	85
III. Combination of data.....	86
1. Lawfulness of combining different data categories at the level of data retrieval.....	88
2. Combining personal data from different data sources.....	88
3. Combining personal data with factual data or anonymous data.....	89
4. Combination of personal data from different countries of origin.....	90
5. Combining different personal data collected for different purposes.....	90
6. Rectifying deficiencies.....	93
IV. Extending the range: anonymization/pseudonymization of data stored in a Big Data database.....	95
1. Pseudonymization (Art. 4 No. 5 GDPR).....	95
2. Anonymization.....	98
3. Encryption and secrecy.....	100
4. De-anonymization for large amounts of data that allow re-identification.....	101
5. Data Trustee.....	102
a) Requirements for a data trustee.....	103
b) Contractual penalty for breach of duties or for overcoming joint management controls.....	103
V. Transmission of data from several controllers to a central Big Data application.....	103
VI. Evaluation and analysis of data.....	104
1. Lawful grounds for the evaluation and analysis of personal data.....	104
2. Big Data applications for the analysis of data with reference to employees or applicants.....	105
a) Applicant analysis.....	105
aa) Collection and Processing of Employee Data in Developing Algorithms for People Analytics Applications.....	106
bb) Analysis of applicant data in people analytics applications.....	107
b) Employee analysis.....	108
aa) Analyses for the purpose of employee retention.....	108
bb) People analytics application with reference to data from social networks.....	108
cc) People analytics application with reference to other publicly accessible data.....	108
dd) Limit of people analytics applications.....	109
c) Stress and mood analyses.....	109
d) Databases for project analysis.....	109
e) Prohibition of completely automatically generated individual decisions.....	110
3. Collective agreements.....	110
4. Rights of the works council to participate (in Germany § 87 (1) No. 6 BetrVG).....	111
5. Special cases.....	112
a) Scoring.....	112
b) User profile.....	113
VII. Continuation of personal reference even after evaluation and analysis of data.....	113
1. Analysis of personal data records insofar as personal references still exist or can be restored.....	113
2. Evaluation of pseudonymized data records.....	114
3. Evaluation of non-personal data, factual data or anonymized data.....	114
VIII. Use of personal data or person-related evaluation/analysis results.....	114

Contents

I. Erasure obligations	117
I. Development of an erasure concept	119
II. Implementation of a data erasure concept	120
III. Necessary elements of a data erasure concept?	121
1. Description of retention and erasure obligations	121
2. What is the relevant law for determining retention and erasure obligations?	121
3. Legal retention obligations	121
4. Erasure periods for archiving data on the basis of consent	122
5. Determining erasure periods from the purpose of use, the applicable statutory provisions and the business process reference of the processed data	122
6. Types of data for which the intended use provides the basis for determining the retention period	123
a) Determining a purpose and associated lawful ground for personal data	123
b) Purpose and retention of non-personal data	123
IV. Start times of retention and erasure obligations	123
V. Assignment of data types to erasure classes	124
VI. Resolution of conflicts when using one data type in different databases	124
VII. What does “erasure” of data mean in contrast to its “blocking”, “masking”, “pseudonymization” or “anonymization”?	125
VIII. Obligation to erase personal data regarding a data subject	127
1. Reasons	127
a) Personal data	127
b) Non-personal data	128
2. Date	128
3. Reasons for exclusion	129
4. Right to be forgotten	129
5. Right to limitation of processing	130
IX. Erasure obligations towards licensors, data suppliers etc. independent of the data content	130
X. Uniform erasure period for all documents and data	131
XI. Erasure obligations for cross-border data processing	132
XII. Storage locations and erasure obligations	133
J. Relevant rights of data subjects in Big Data applications according to the GDPR	135
I. Information obligations according to Art. 13, 14 GDPR	135
II. Rights of data subjects pursuant to Art. 15 <i>et seq.</i> GDPR	137
1. Right to access	137
2. Right to rectification	137
3. Right to erasure and to be forgotten	138
4. Right to restriction of processing	138
5. Right to data portability	138
6. Right to lodge a complaint	139
III. Records of processing activities according to Art. 30 GDPR	139
IV. Implementation of technical and organizational measures to protect personal data from unauthorized access	140
1. Access control	141
2. (Virtual) Access control	141
3. Admission control	142
4. Data medium control	142
5. Access and user control	142
6. Control of disclosure, transmission and transport	143
7. Input and storage control	143
8. Contract control	143
9. Availability control	144
10. Separation control	144
11. Recoverability	144
12. Reliability	145
13. Data integrity	145
14. Sanction for non-existent or inadequate technical and organizational measures	145

V. General principles for the processing of personal data in Art. 5 GDPR.....	145
1. General principles for the processing of personal data.....	145
2. Principle of accountability (Art. 5 (2) GDPR).....	146
3. Sanctioning a breach of these principles.....	146
K. Data protection impact assessment.....	147
L. System data protection when operating Big Data applications	149
I. System data protection for personal data	149
1. Fundamental right to informational self-determination	149
2. The fundamental right to ensure the integrity and confidentiality of information technology systems.....	150
3. Indirect effect of fundamental rights between private individuals; Interpretation of guidelines.....	150
4. Ensuring confidentiality through technical and organizational measures.....	151
II. System data protection for non-personal data only in a Big Data Application	153
M. Protection of Big Data applications.....	155
I. Technical and organizational measures	155
II. Protection of the algorithms underlying the Big Data application.....	155
III. Compliance management system	156
IV. Aspects of copyright contract law in the database management system	157
N. Legal consequences of non-compliance with the legal requirements set out in this guide	159
I. Sanctions in case of violation of data protection regulations	160
1. Administrative fines.....	160
2. Material and non-material damages supplemented by power to bring collective actions	162
3. Misdemeanours.....	162
4. Entry in central trade register (loss of entitlement to participate in public tenders).....	162
5. Penalties according to the BDSG.....	162
6. Supervisory intervention rights of the data protection supervisory authorities	163
II. Legal consequences of infringement of copyrights in collective works or database protection rights	164
1. Injunctive relief.....	164
2. Damages claim	164
3. Enforcement of copyright claims.....	164
4. Destruction claim	165
5. Liability of the controller.....	165
6. Right to information.....	165
7. Criminal offences	165
III. Violation of virtual householder's rights	166
1. Injunctive relief.....	166
2. Damage claims	166
3. Subordinate claims.....	166
4. Relevance under criminal law	166
IV. Sanctions for infringing business or trade secrets pursuant to the German Trade Secrets Act.....	167
1. Criminal offences	167
2. Civil law Claims under the German Trade Secrets Act.....	167
V. Contractual claims	168
O. Big Data Applications as a service	169
P. Recommended Actions.....	175
Index of keywords	177