table of contents

Foreword 5
Bibliography 23

§ 1 From Directive to Regulation – European Data Protection Law de lege lata 35

A. Preliminary Remarks 35
B. General Data Protection Law of the European Union 36
I. Starting Point 36
II. Charter of Fundamental Rights 37
III. The data protection principle as a general principle of EU law 43
IV. Special Protection Against the Action of the European Union 45
1. Scope of Protection 45
2. Impairments and Justification 46
C. Directive 95/46/EC 46
D. Deficits of the Policy Concept 49
E. The Directive Goes, the Regulation Comes 50
I. Legal Nature of a Regulation at EU Level 50
II. Objectives of the GDPR 50
III. Structure of the GDPR 53

§ 2 Key Terms 55

A. Preliminary Note 55
B. The Protagonists of Data Protection Law 55
I. Controller 55
II. Data Subjects 57
III. Third Party 60
IV. Recipient 61
V. Processor 61
VI. Representatives 62
VII. Company and Group of Undertakings 62
VIII. Supervisory Authority 63
C. Subject Matter of Data Protection Law 63
I. Personal Data 63
II. Special categories of Personal Data – "Sensitive Data" 68
1. General Provisions 68
2. Genetic Data 70
3. Biometric Data 70
4. Health Data 70
D. Handling of Data 71
I. Processing 71
1. Collection 72
2. Recording 73
3. Organization 73
4. Structuring 74

5. Storage 75
6. Adaptation 75
7. Alteration 76
8. Retrieval 76
9. Consultation 76
10. Use 76
11. Disclosure [by Transmission & Processing] 77
12. Alignment or Combination 78
13. Restriction 78
14. Erasure or Destruction 79
15. Pseudonymization 79
16. Anonymization 81
II. Automated Processing 81
III. Processing Other Than by Automated Means 82
E. Further legal definitions 82

§ 3 General Principles of Processing 83

A. Preliminary Note 83
B. Lawfulness, Fairness and Transparency 83
I. Lawfulness of Data Processing 83
II. Processing in Accordance with Fairness 84
III. Transparency 86
C. Principle on Purpose Limitation 88
I. Specified Purpose 89
II. Explicit and Clear Purpose 89
III. Legitimate Purpose 90
IV. Further Processing 90
D. Data Minimization 92
E. Accuracy 93
F. Storage Limitation 94
G. Integrity and Confidentiality 94
H. Accountability 95

§ 4 Legal Basis of Processing 99

A. Data Processing Based on a Consent, Art. 6 (1) (a) GDPR 99
I. Content Requirements for the Consent of the Data Subject 99
1. Free Decision 100
a) Free Decision in Employment Relationship 100
b) Free Decision When Awarding Financial Incentives 102
c) Free Decision within Negotiation Imbalance 105
d) Forced Consent 105
2. Concrete Purpose Limitation "for the Special Case" 106
3. Informed 106
4. Unambiguous 108
II. Formal Requirements , "Clear Affirmative Action" 108
III. Pre-formulated Declarations 109

IV. Conditions Applicable to Child's Consent, Art. 8 GDPR 110
1. Information Society Services 110
2. Consent and Information Society Services 110
a) At Least 13, at the Most 16 Years 111
b) Direct Offer to Children 111
c) Necessity of Consent by the Holder of Parental Responsibility 113
aa) Holder of Parental Responsibility – One Parent Sufficient? 113
bb) Demonstration of Parental Consent 116
cc) No Impact on Contract Law 117
3. Requirements Outside the Services of the Information Society 117
V. Consent to the Processing of Special Categories of Personal Data 118
VI. Facilitation of the Granting of Consent in Research and Science 119
VII. Consent for Cookies, Web Bugs and Co. 119
1. Cookies 119
a) Conceptuality and Function 119
b) Legal Assessment 120
aa) Consent Based on the Browser Settings of the Respective User 121
bb) No Application of the Provisions in §§ 14, 15 German Telemedia Act (TMG) 121
cc) Session Cookies 122
dd) Permanent Cookies 122
ee) Flash Cookies 122
2. Web Bugs 123
3. Use of So-Called Web Logs 123
4. Behavioral Targeting and Online Advertising 124
5. Control Considerations from Directive 2002/58/EC 125
6. Requirements for Consent 127
7. Future Revision – the ePrivacy Regulation 127
VIII. The Consent's Period of Validity 128
IX. Revocation of Consent 129
X. No Representation 129
XI. Special Issue: Consent Despite Other Existent Allowance 129
XII. Continuation of Old Consents 129
B. Data Processing as a Contractual Obligation, Art. 6 (1) (b) GDPR 130
I. Contract 130
II. Implementation/Fulfillment 132
III. Necessity of the Processing 133
C. Data Processing in Compliance With a Legal Obligation, Art. 6 (1) (c) GDPR 136
D. Data Processing for Protection of Vital Interests, Art. 6 (1) (d) GDPR 138
E. Data Processing for the Performance of a Task Carried Out in the Public Interest, Art. 6 (1) (e) GDPR 138
F. Data Processing Necessary for the Purposes of the Legitimate Interests Pursued by the Controller or by a Third Party, Art. 6 (1) (f) GDPR 139
I. General Details and Background 139
II. The Concept of the "Legitimate Interest" 144
III. Interests of the Data Subject 146
IV. Balancing of Interests 146
1. General Requirements 146

2. Criteria to Be Considered in the Balancing Process 147
a) Importance, Nature and Source of the Legitimate Interest 147
aa) Asserting One's Own Fundamental Right Positions or Fundamental Freedoms 148
bb) Public Interests 148
(1) Information Transmission by Consumer Centers 149
(2) Press Information by Competitors 149
(3) Identifying Press Releases 150
(4) Political Dispute 151
cc) Processing Within a Group of Undertakings (Group Data Processing) . 151
dd) Further Specifications 152
b) Importance, Nature and Source of the Data Subject's Interest 153
aa) Children 153
bb) Sick and Otherwise "Vulnerable" Persons 153
cc) Public Function and Reputation of the Data Subject 154
dd) Social Sphere vs. Privacy 154
c) Data Affected by Processing – Categorization and Default Privacy Model . 155
aa) Normal Protection Requirements 155
bb) High Protection Requirements 155
cc) Very High Protection Requirements 156
dd) "Public Data" 157
d) Form of Intended Processing 159
e) Established Precautionary Measures – Safeguards 159
f) Possible Consequences of Processing for the Data Subject 159
g) Instructions by the Article 29 Data Protection Working Party 160
h) Scoring Outside of a Concrete Decision-Making Process 160
i) Rights to Information Within an Association 161
G. Schematic Illustration of Processing 164
H. Purpose-Changing Further Processing 165
I. Art. 6 (4) GDPR 165
II. Further Processing Powers in the BDSG-new 165
1. Further Processing by Public Authorities, § 23 BDSG-new 166
a) Obviously "Presumed" Consent to Further Processing, § 23 (1) (1) BDSG-new 166
b) Verification of the Data Subject's Data, § 23 (1) (2) BDSG-new 166
c) Protection Against Considerable Disadvantages for the Common Good or Danger to Public Safety, § 23 (1) (3) BDSG-new 167
d) Prosecution of Criminal Offenses, Misdemeanors, Enforcement or Execution of Sentences, § 23 (1) (4) BDSG-new 167
e) Averting Serious Impairment of the Rights of Another Person 167
f) Exercise of Supervisory and Control Powers, etc., § 23 (1) (6) 167
g) Special Requirements for Further Processing of Special Categories of Personal Data, § 23 (2) BDSG-new 167
2. § 24 BDSG-new 168
a) Further Processing to Avert Threats to State or Public Security or for the Prosecution of Criminal Offenses, § 24 (1) (1) BDSG-new 168
b) Assertion, Exercise or Defense of Civil Law Claims, § 24 (1) (2) BDSG-new 169

c) Special Requirement for Further Processing of Special Categories of Personal Data, § 24 (2) BDSG-new 169
I. Processing of Special Categories of Personal Data, Art. 9 GDPR 169
I. Processing on the Basis of Consent 170
II. Processing Related to Labor Law, Social Security Law and Social Protection 170
III. Processing for the Protection of Vital Interests of the Data Subject or Another Natural Person 171
IV. Processing by a Political, Ideological, Religious or Union-Oriented Foundation, Association or Other Organization 171
V. Processing of Data Obviously Made Public by the Data Subject 171
VI. Processing for the Assertion, Exercise or Defense of Legal Claims or for Acts of the Courts 172
VII. Processing Based on a Significant Public Interest 172
VIII. Processing in the Field of Health Care and Occupational Medicine 173
IX. Processing for Public Health Purposes or to Avert Serious Health Risks 174
X. Processing for Archival Purposes of Public Interest, for Scientific or Historical Research Purposes or Statistical Purposes 175
XI. Processing Powers in § 22 BDSG-new 175
1. General Provisions 175
2. Exceptions in Favor of Public and Non-Public Bodies, § 22 (1) (1) BDSG-new 176
a) Exercise of Rights and Fulfillment of Obligations in Connection with Social Security and Social Protection, § 22 (1) (1) (a) BDSG-new 176
b) Health Care, Assessment of Work Ability, Medical Diagnosis and Treatment, § 22 (1) (1) (b) BDSG-new 176
c) Processing for Reasons of Public Interest in the Area of Public Health, § 22 (1) (1) (c) BDSG-new 177
3. Exceptions in Favor of Public Authorities, § 22 (1) (2) BDSG-new 177
4. Special Safeguards in the Context of the Processing of Special Categories of Personal Data, § 22 (2) BDSG-new 177
J. Processing of Personal Data Relating to Criminal Convictions and Offenses, Art. 10 GDPR 180
K. Profiling and Automated Individual Decision-Making 181
I. Profiling 181
1. Legal Definition, Art. 4 (4) GDPR, and Scope of Application 181
2. Application Examples 182
a) Big Data, Data Mining 182
b) Scoring 183
c) User Profiles on the Internet 184
II. Automated Individual Decision-Making 185
III. Exceptions to the Prohibition of Profiling and Automated Individual Decision-Making 186
1. Conclusion or Fulfillment of a Contract 186
2. Explicit Consent of the Data Subject 186
3. Admissibility in the Context of Providing Services Pursuant to an Insurance Contract, § 37 BDSG-new 186
a) Fully Sustaining Decision on a Claim for Benefits by the Data Subject, § 37 (1) (1) BDSG-new 187

b) Decision-Making Based on Binding Rules of Remuneration for Therapeutic Treatment ... 187
c) No Restriction to Certain Data Categories ... 188
4. Limitation of Processing Powers in Relation to Scoring and Credit Reports, § 31 BDSG-new ... 188
a) Subject Matter and Regulatory Authority ... 188
b) Use of Probability Values for the Purpose of Deciding on the Creation, Execution or Termination of a Contractual Relationship, § 31 (1) BDSG-new ... 190
c) Use of a Probability Value Calculated by Credit Reporting Agencies to Determine a Natural Person's Ability and Willingness to Pay ... 191
IV. Safeguarding the Data Subject's Interests, Art. 22 (3) GDPR ... 192

§ 5 Information and Notification Obligations of the Controller ... 193

A. Structure ... 193
B. Nature of the New Information Obligations When Collecting Data – Why and How? ... 193
I. Objective and Purpose – Why? ... 193
II. Formal Requirements of the Obligation to Inform – How? ... 194
1. Concise, Transparent, Easy to Understand and Easily Accessible ... 194
a) General Requirements ... 194
b) Icons ... 197
c) Increased Requirements for Information Towards Children ... 198
2. Formal Requirements ... 198
3. Costs ... 199
C. Information To Be Provided Where Personal Data Are Collected From The Data Subject (Direct Survey) ... 199
I. Structure of the Standard ... 199
1. Relationship Between Information Referred to in Paragraph 1 and Paragraph 2 ... 200
2. Information Only at the Time of First Collection or at Each Collection ... 201
II. Information Obligations Pursuant to Art. 13 (1) GDPR ... 202
1. Name and Contact Details ... 202
2. Contact Details of the Data Protection Officer ... 203
3. Purposes and Legal Basis of Processing ... 203
4. Legitimate Interests ... 203
5. Recipients or Categories of Recipients ... 204
6. Transmission to Third Countries or to International Organizations ... 204
III. Obligation to Provide Information pursuant to Art. 13 (2) GDPR ("Information for Retrieval") ... 204
1. Duration of Storage or Criteria for Determining the Storage Duration ... 204
2. Rights of the Data Subject ... 205
a) Right of Access ... 205
b) Right to Rectification ... 205
c) Right to Erasure ... 205
d) Right to Restriction of Processing ... 206
e) Right to Object ... 206
f) Right to Data Portability ... 206

g) Right to Withdraw His or Her Consent 206
h) Right to Lodge a Complaint 206
3. Obligation to Making Available of Data 206
a) Provision of Information due to Legal Obligation 207
b) Provision of Information due to Contractual Obligations 209
c) Provision of Information Required for the Conclusion of a Contract 209
d) Obligation of the Data Subject to Provide Information and Consequences of Non-Provision 210
4. Automated Decision-Making including Profiling 211
IV. Obligation to Provide Information When Further Processing Data 212
V. Inapplicability of the Obligation to Provide Information 212
1. Knowledge of the Data Subject, Art. 13 (4) GDPR 212
2. Exception When Further Processing in the Form of Disclosure or Transmission to Persons Subject to a Legal Obligation of Professional Secrecy, § 29 (2) BDSG-new 213
3. Further Exceptions to the Obligation to Provide Information When Further Processing, § 32 Abs. 1 BDSG-new 214
a) Disproportionate Effort in Further Processing of "Analog Stored Data", § 32 (1) No. 1 BDSG-new 214
aa) Data Stored in Analog Form 214
bb) Further Processing is Aimed Directly at the Data Subject 215
cc) Further Processing is Compatible with the Original Purpose of The Data Collection 215
dd) No Digital Communication 215
ee) Low Interest of the Data Subject in Information 215
ff) Case Study 215
b) Endangerment of the Proper Performance of Tasks as Referred to in Art. 23 (1) (a) to (e) GDPR, pursuant to § 32 (1) (2) BDSG-new 216
c) Endangerment of Public Security or Order, § 32 (1) No. 3 BDSG-new 216
d) Interference with the Establishment, Exercise or Defense of Legal Claims, § 32 (1) (4) BDSG-new 217
e) Endangerment of Confidential Transfer of Data to Public Bodies, § 32 (1) (5) BDSG-new 217
4. Measures to Protect the Legitimate Interests of the Data Subject When Information is Not Provided, § 32 (2) and (3) BDSG-new 218
a) Setting Down in Writing the Reasons for the Non-Provision of Information to the Data Subject, § 32 (3) p. 3 BDSG-new 218
b) Special Precautionary Measures for Cases acc. § 32 (1) (1–3) BDSG-new . 218
c) Providing Information within an Appropriate Period after a Temporary Obstacle, § 32 (3) BDSG-new 219
D. Obligation to Provide Information in the Context of Data Collection from Third Parties (Data Collection with Third Parties) 219
I. Structure of the Standard 219
1. Relationship Between Information Referred to in Paragraph 1 and Paragraph 2 219
2. Information Only at the Time of First Collection or at Each Collection 220
II. Time of the Arising of the Information Obligations pursuant to Art. 14 (1) and (2) GDPR, Art. 14 (3) GDPR 220
1. Within One Month after Obtaining the Personal Data, Art. 14 (3) (a) GDPR .. 220

2. Time of First Notification to the Data Subject, Art. 14 (3) (b) GDPR 221
3. At the Time of the Disclosure, Art. 14 (3) (c) GDPR 221
III. Information Obligations Pursuant to Art. 14 (1) GDPR 222
1. Identity and Contact Details, Art. 14 (1) (a) GDPR 222
2. Data Protection Officer, Art. 14 (1) (b) GDPR 222
3. Purposes and Legal Basis, Art. 14 (1) (c) GDPR 222
4. Data Categories, Art. 14 (1) (d) GDPR 222
5. Recipients or Categories of Recipients, Art. 14 (1) (e) GDPR 223
6. Transmission to Third Countries, Art. 14 (1) (f) GDPR 223
IV. Information Obligations Pursuant to Art. 14 (2) GDPR 223
1. Period of Storage, Art. 14 (2) (a) GDPR 223
2. Legitimate Interests, Art. 14 (2) (b) GDPR 224
3. Rights of the Data Subject 224
a) Right of Access 224
b) Right to Rectification 224
c) Right to Erasure 224
d) Right to Restriction of Processing 224
e) Right to Object 224
f) Right to Data Portability 225
g) Right to Withdraw His or Her Consent 225
h) Right to Lodge a Complaint 225
4. Origin of Data – Data Source, Art. 14 (2) (f) GDPR 225
5. Information on the Data Origin 225
6. Automated Decision-Making, including Profiling, Art. 14 (2) (g) GDPR 226
V. Obligation to Provide Information when Further Processing Data, Art. 14 (4) GDPR 226
VI. General Non-Applicability of the Obligation to Provide Information 226
1. Knowledge of the Data Subject, Art. 14 (5) (a) GDPR 226
2. Impossibility or Disproportionate Effort, Art. 14 (5) (b) GDPR 226
a) The provision of information proves impossible 226
b) The provision of information involves a disproportionate effort 228
c) Protective Measures Provided for by the Controller 229
3. Obtaining or Disclosure Expressly Laid Down by Union or Member State Law, Art. 14 (5) (c) GDPR 229
4. Professional Secrecy, Art. 14 (5) (d) GDPR 230
5. Legitimate Secrecy Interests of a Third Party, § 29 (1) p. 1 BDSG-new 230
VII. Exemptions pursuant to § 33 BDSG-new 231
1. Non-Applicability of Information Obligations When Further Processing in the Case of a Public Body, § 33 (1) (1) BDSG-new 231
a) Endangerment of the Proper Performance of Tasks, § 33 (1) (1a) BDSG-new 231
b) Threat of the Public Security or Order or Otherwise Detrimental Circumstance to the Federation or a Land, § 33 (1) (1b) BDSG-new 231
2. Non-Applicability of Information Obligations When Further Processing in the Case of a Non-Public (Private) Body, § 33 (1) (2) BDSG-new 232
a) Interference with the Establishment, Exercise or Defense of Legal Claims under Private Law, § 33 (1) (2a) BDSG-new 232
b) Endangerment of a Confidential Transmission of Data to a Public Body, § 33 (1) (2b) BDSG-new 232

3. Special Safeguards, § 33 (2) and (3) BDSG-new 233
VIII. Relationship between Art. 13 and Art. 14 GDPR 233
E. Special Obligations to Provide Information in Connection with Processing acc. Art. 6 (1) (e) or (f) GDPR and Direct Marketing, Art. 21 (4) GDPR 233
F. Communication Of a Personal Data Breach to the Data Subject, Art. 34 GDPR 234
I. Prerequisite – Potentially High Risk 235
II. Consequences, Form and Content 236
III. Exceptions to the Obligation to Notify 237
1. Appropriate Technical and Organizational Protection Measures, Art. 34 (3) (a) GDPR 237
2. Subsequent Measures by the Controller, Art. 34 (3) (b) GDPR 238
3. Disproportionate Effort, Art. 34 (3) (c) GDPR 238
4. Secrecy Interests, § 29 (1) S. 3 BDSG-new 238
IV. Prohibition of Use in Criminal Proceedings, § 42 (4) BDSG-new 239
G. Notification of a Personal Data Breach to the Supervisory Authority, Art. 33 GDPR 239
I. Prerequisite – Expected Risk 239
II. Content of the Information to Be Transmitted 239
1. Nature of the Personal Data Breach 239
2. Categories and Approximate Number of Data Subjects Concerned 240
3. Name and Contact Details of the Data Protection Officer or Other Contact Point where More Information Can Be Obtained 240
4. Description of the Probable Consequences of the Personal Data Breach 240
5. Measures Taken or Proposed to Be Taken by the Controller to Address the Personal Data Breach 240
III. Form and Deadline of the Communication 240
IV. Prohibition of Use in Criminal Proceedings, § 42 (4) BDSG-new 241

§ 6 Rights of the Data Subject 243

A. Preliminary Note 243
B. Right of Access, Art. 15 GDPR 243
I. Investigation Claim – Is Data About Me Processed at All? 243
II. Right of Access – What Data is Processed by Whom, for Whom, and What Can I Do About It? 244
1. General Part of the Claim for Access 244
a) Purposes of the Processing 245
b) Categories of Personal Data Being Processed 245
c) Recipients or Categories of Recipient 245
d) Envisaged Period For Which The Personal Data Will Be Stored Or The Criteria Used To Determine That Period 246
e) Rights of the Data Subject 246
aa) Right to Rectification 247
bb) Right to Erasure 247
cc) Right to Restriction of Processing 247
dd) Right to Object 247
ee) Right to Lodge a Complaint 247
f) All Available Information about the Origin of the Data 247
g) Automated Decision-Making including Profiling 248
h) Transmission to Third Countries 248

2. Special Part of the Claim for Access 248
a) All Processed Personal Data 248
b) Right to Free Copy of the Data 248
aa) Scale – What does "copy of personal data" mean? 248
bb) In General Free of Charge 249
cc) Special Problem: Information about the Content of Patient Files 251
3. Formal Requirements concerning the Provision of Information 252
a) In a Concise, Transparent, Intelligible and Easily Accessible Form 252
b) Without Undue Delay 252
c) In Paper Form, on Request Also Electronically 253
d) Provision to the Correct Data Subject 253
III. Limitations on the Right of Access 253
1. Limitations Necessary for the Fulfillment of the Research or Statistical Purposes, § 27 (2) BDSG-new 254
2. Restriction in Favor of Public Interest Archives, § 28 (2) BDSG-new 254
3. Interest in Maintaining Confidentiality/Secrecy, § 29 (1) S. 2 BDSG-new 254
4. Restrictions under § 34 BDSG-new 254
a) No Obligation to Provide Information under § 33 BDSG-new, § 34 (1) No. 1 BDSG-new 254
b) Data Only Available due to Storage Obligations, § 34 (1) No. 2a) BDSG-new 255
c) Data Only Serve Purposes of Monitoring Data Protection or Safeguarding Data, § 34 (1) (2)(b) BDSG-new 256
d) Special Documentation Obligations and Purpose Limitation, § 34 (2) BDSG-new 256
e) Special Regulations in the Event of Refusal of Information by Public Authorities, § 34 (3) and (4) BDSG-new 256
IV. Right of Access towards Credit Bureaus in the Context of Consumer Loans, § 30 BDSG-new 257
C. Right to Rectification 257
I. Art. 16 GDPR 257
II. Restriction of Processing for Archiving Purposes in the Public Interest, § 28 (3) BDSG-new 258
III. Notification Obligation of the Controller towards Recipients, Art. 19 GDPR 258
D. Right to Erasure ("Right to be Forgotten"), Art. 17 GDPR 259
I. Grounds for Erasure 259
1. Frustration of Purpose, Art. 17 (1) (a) GDPR 259
2. Consent Revocation, Art. 17 (1) (b) GDPR 262
3. Objection to the Processing, Art. 17 (1) (c) GDPR 262
a) Objection to Processing in the Context of Performing a Task in the Public Interest or Legitimate Interests of the Controller 262
b) Objection to Processing for Direct Marketing Purposes 263
4. Unlawful Processing 264
5. Erasure is Required to Fulfill a Legal Obligation 264
6. Data Collected in Relation to Information Society Services Offered Pursuant to Art. 8 (1) GDPR, Art. 17 (1) (f) GDPR 264
II. Non-Applicability of the Right/Obligation to Erasure 265
1. Exercise of the Right to Freedom of Expression and Information, Art. 17 (3) (a) GDPR 265

2. Fulfillment of a Legal Obligation, Art. 17 (3) (b) (1) GDPR-old 267
3. Performance of a Task Carried Out in the Public Interest, Art. 17 (3) (b) (2) GDPR - old 267
4. Processing Carried Out in the Exercise of Official Authority, Art. 17 (3) (b) – old (3) GDPR 267
5. Reasons of Public Interest in the Area of Public Health, Art. 17 (3) (c) GDPR . 268
6. Archiving Purposes in the Public Interest, Scientific or Historical Research Purposes or Statistical Purposes, Art. 17 (3) (d) GDPR 268
7. Establishment, Exercise or Defense of Legal Claims, Art. 17 (3) (e) GDPR ... 269
8. Restrictions under § 35 BDSG-new 269
a) Regulatory Power? 269
b) Disproportionate Effort in the Case of Non-Automated Data Processing, § 35 (1) BDSG-new 269
c) Obligation to Restrict Processing and Obligation to Inform the Data Subject, § 35 (2) BDSG-new 270
d) Conflict with Retention Periods set by Statute or Contract, § 35 (3) BDSG-new 271
III. Special Obligations for Making Data Publicly Accessible, Art. 17 (2) GDPR 272
IV. Notification Obligation of the Controller towards Recipients, Art. 19 GDPR 272
E. Right to Restriction of Processing, Art. 18 GDPR 273
I. Accuracy of the Personal Data is Contested, Art. 18 (1) (a) GDPR 273
II. Unlawful Processing, Art. 18 (1) (b) GDPR 273
III. Frustration of Purpose by the Controller 274
IV. Objection to Processing in Accordance with Art. 21 (1) GDPR 275
V. Legal Consequences of Processing, Art. 18 (2) GDPR 275
VI. Restriction of Rights under § 28 (4) BDSG-new 275
F. Right to Data Portability, Art. 20 GDPR 275
I. Affected Data 276
1. Provided 276
2. Personal Data Concerning the Data Subject 277
3. Processing due to Consent or Contract 277
4. Automated Processing 278
II. Scope of the Right to Data Portability 278
1. Structured, Common and Machine-Readable 278
2. Transmission to the Data Subject 279
3. Direct Transmission to a New Controller 279
III. Restrictions 280
IV. Obligations of the "New" Controller 280
G. Right to Object, Art. 21 GDPR 281
I. Overview of the Basic Content of the Right to Object 281
II. Objection under Art. 21 (1) GDPR 281
1. Subject Matter 281
2. Content Requirements 282
3. Formal Requirements/Time Limit 283
4. Legal Consequences 283
III. Objection to Processing with Marketing Purposes, Art. 21 (2) GDPR 284
1. Subject Matter, Content and Formal Requirements 284
2. Legal Consequences 286

IV. Objection to the Use of Data for Scientific or Historical Research Purposes or for Statistical Purposes, Art. 21 (5) GDPR 286
V. No Right to Object to Public Authorities, § 36 BDSG-new 286
VI. Restrictions for Archival and Research Purposes, § 27 (2) BDSG-new and § 28 (4) BDSG-new 287

§ 7 Safeguards for Ensuring Compliance with the GDPR 289

A. Preliminary Notes 289
B. Principles 289
C. Implementation of Technical and Organizational Measures, Art. 32 GDPR 293
I. Pseudonymization 294
1. Medical Research and Diagnostics 294
2. Video Surveillance 295
3. Test, Demonstration or Training Systems 295
4. Implementation Options for Pseudonymization 296
II. Encryption 296
III. Ensuring the Confidentiality, Integrity, Availability and Resilience of Systems and Services 297
1. Confidentiality 297
2. Integrity 297
3. Availability 298
4. Resilience 298
IV. Recoverability 298
V. Organizational Measures 299
VI. Regular Review, Assessment and Evaluation of the Effectiveness of Technical and Organizational Measures 299
D. Data Protection by Design and by Default, Art. 25 GDPR 300
I. Central Concepts and Their Foundations 300
1. Data Protection by (Technology) Design 300
a) Historical Development 300
b) Conclusions for the Content Determination of PbD 303
2. Data Protection by Privacy-Friendly Default Settings – Data Protection by Default 303
II. The Controller's Obligation to Implement 305
E. Documentation of Processing Activities 305
I. Records of Processing Activities of the Controller, Art. 30 GDPR 305
1. Deviations from the Previous Law 305
2. Formal and Content Requirements 306
3. Exceptions to the Obligation to Maintain Records of Processing Activities 307
II. Records of Processing Activities of the Controller 308
III. Documentation Obligations Derived from other Provisions 308
F. Data Protection Impact Assessment (DPIA) 310
I. Subject Matter and Scope of Application 310
1. Subject Matter – Target of Evaluation (ToE) 310
2. Potentially High Risk to the Rights and Freedoms of Natural Persons 313
a) High Risk 313
b) Likelihood and Time of Prediction of the High Risk 317

II. Specifications of Implementation ... 318
1. Consultation of the Data Protection Officer (DPO) ... 318
2. Form and Minimum Content ... 318
a) Systematic Description of Processing Operations and Purposes ... 319
b) Assessment of the Necessity and Proportionality of the Processing Operations concerning the Purpose ... 320
c) Assessment of the Risks to the Rights and Freedoms of the Data Subject(s) 320
d) Presentation of Corrective Measures ... 320
e) Grouped Description ... 321
f) Reference to Existing Certification Processes and Guidelines ... 322
3. Understanding the Point of View of the Data Subject ... 323
4. Review Process ... 323
5. Group or Branch Impact Assessment? ... 323
III. Special Consultation Obligations ... 323
G. Data Protection Officer (DPO) ... 324
I. Obligation to Designate a Data Protection Officer (DPO) ... 324
1. Provisions within the GDPR, Art. 37 (1) ... 324
a) Processing Carried Out by a Public Authority or Body ... 325
b) The Core Activities Consist of Processing Operations which Require Regular and Systematic Monitoring of Data Subjects on a Large Scale ... 325
c) The Core Activities Consist of Processing on a Large Scale of Special Categories of Data pursuant to Art. 9 GDPR or of Personal Data relating to Criminal Convictions and Offenses ... 326
2. Further Obligations in §§ 5–7 and 38 BDSG-new ... 326
II. Requirements for Being a Data Protection Officer (DPO) ... 327
1. Professional Qualities ... 327
2. Independence ... 328
3. Obligation of Confidentiality ... 329
4. Internal or External Company Data Protection Officer (DPO) ... 329
III. Tasks of the Data Protection Officer (DPO) ... 330
IV. Special Obligations of the Controller or the Processor ... 331
H. Certification ... 331
I. Code of Conduct ... 332
I. General Provisions ... 332
II. Requirements for Codes of Conduct ... 333
1. Authorization to Create a Code of Conduct ... 333
2. Admissible Content ... 333
3. Monitoring ... 334
III. Approval Procedure ... 334
IV. Legal Consequences ... 334

§ 8 Processing ... 335

A. General Provisions ... 335
B. Concept and Legal Basis of Processing ... 335
I. Position of the Processor – Differentiation from the Controller ... 335
II. Differentiation from Joint Responsibility pursuant to Art. 26 GDPR ... 337
1. Necessity of Differentiation / Liability Aspects ... 337
2. When is there a Case of Joint Responsibility? ... 338

3. Content Requirements for Joint Responsibility 340
a) Definition of the Respective Actual Functions and Relationships in an Agreement 340
b) Provision of Information to the Data Subject 342
III. Essence of the Order Processing – Privilege Function 342
C. Content Requirements for Processing 343
I. Justification by Contract or another Legal Instrument 343
II. Content Requirements for Contracts 344
1. General Requirements 344
2. Special Requirements 345
a) Action in Accordance with Documented Instructions 345
b) Confidentiality Obligation or Statutory Obligation of Secrecy 346
c) Taking Technical-Organizational Measures Pursuant to Art. 32 GDPR 346
d) Conditions for Utilising Sub-Processors 347
e) Assistance Related to the Fulfillment of Rights of Data Subjects 347
f) Assistance in Fulfilling Obligations Placed on the Controller in Art. 32 to 35 GDPR 348
g) Obligations to Erase and to Return 348
h) Supervision and Entry and Information Rights of the Controller and Accountability and Information Obligations of the Processor 349
3. Useful Contractual Supplements 349
D. Other Obligations of the Processor 349
I. Obligation to Designate a Representative, Art. 27 GDPR 349
II. Maintaining a Record of Processing Activities, Art. 30 (2) GDPR 350
III. Cooperation with the Supervisory Authority, Art. 31 GDPR 351
IV. Obligation to Designate a Data Protection Officer, Art. 37 GDPR 351
V. Addressee of Powers of the Supervisory Authorities, Art. 58 GDPR 351
E. Obligations of the Client 351

§ 9 Employment Data Protection Law in the BDSG-new 353

A. Introduction 353
B. Legal Basis 354
I. Current Regulations on Employees Data Protection in the BDSG 354
II. Structure of § 26 BDSG-new 355
C. Data Protection in the Application Procedure 358
I. Introduction 358
II. Applicant Profile Creation with the Aid of Publicly Accessible Sources 359
III. Data Collection in Job Interviews 363
1. Limitation of the Right to Ask Questions 363
2. Behavioral Analyses, Personality Tests, Medical Examinations 363
IV. Unsuccessful Applicants 364
D. Data Protection within the Framework of Existing Employment Relationships 365
I. Introduction 365
II. Internet, Email, Telephone and Mobile Telephone Use in the Workplace 365
III. Employee Data in the Enterprise's Internet Presence 366
1. Requirement to Obtain Consent 366
2. Images of Former Employees on the Internet 367
3. Admissible Content of Information on the Internet 367

IV. Establishing Electronic Information Databases 368
V. Maintaining so-called Skills Databases 368
E. Data Protection after Termination of the Employment Relationship 369

§ 10 Exporting Data to Third Countries 371

A. Preliminary Note 371
B. Adequacy Decision, Art. 45 GDPR 371
C. Provision of Appropriate Safeguards, Art. 46 GDPR 372
I. Binding Corporate Rules 372
1. Previous Legal Status 372
2. New Legal Situation 374
II. Standard Data Protection Clauses 375
III. Authorized Codes of Conduct and Certification 376
D. Other Derogations 376

§ 11 Remedies, Liability, Administrative Fines and Penalties 377

A. Supervisory Powers and Measures 377
I. Supervisory Authorities 377
1. Independence Requirements 377
2. Determination of Local Competence 378
II. Tasks of the Supervisory Authority 379
III. Powers of the Supervisory Authorities 379
IV. Legal Remedies of the Controller and the Processor 380
B. Legal Position of the Data Subject 381
I. Right to Lodge a Complaint 381
1. Content 381
2. Legal Remedies 381
II. Right to Compensation 381
1. Content 381
2. Legal Remedies 382
C. Administrative Fines 382
I. Basis of Calculation 382
II. Administrative Fine Structure 383
III. Legal Remedies 383
IV. Addressees – Liability of Executive Bodies? 384
D. Provisions on Penalties 385

§ 12 Austria 387

A. Preliminary Note 387
B. Structure of the DSG 2018 387
C. Regulations In Detail 387
I. Rectification and Erasure of Personal Data, § 4 (2) DSG 2018 387
II. Processing of Data about Judicial or Administrative Offenses, § 4 (3) DSG 2018 . 388
III. Specification in relation to Art. 8 GDPR 389
IV. Data Protection Officer (DPO), § 5 DSG 2018 389
V. Data Confidentiality, § 6 DSG 2018 389

VI. Transmission of Address Data for the Purpose of Notification and Questioning, § 8 DSG 2018 390
VII. Media Privilege, § 9 DSG 2018 391
VIII. Image Processing and Video Surveillance for Private Purposes, §§ 12, 13 DSG 2018 391
IX. Data Protection Supervisory, §§ 14 – 23 DSG 2018 392
X. Further Details on Legal Remedies, Liability and Sanctions, §§ 24 30 DSG 2018. 392
1. Right to Lodge a Complaint, § 24 DSG 2018 392
2. Compensatory Damages – Administrative Responsibility 393
3. Administrative Fines 393
Index 395