

Table of Contents

Preface to the Second Edition	V
Preface	VI
Abbreviations	XIII

Part 1

Data Protection in Germany

A. The Concept of Data Privacy and Protection in Germany	1
I. Key Legislation: The Structure and Function of the Federal Data Protection Act	1
1. The Short History of Data Protection Law	1
a) First Development of a German Data Protection Legislation	1
b) Data Protection Law on International Level	2
c) Constitutional Background	2
d) The European Data Protection Directive	3
e) The E-Privacy Directive	4
f) Reform of the BDSG in 2009	4
g) Recent Developments	5
2. The European General Data Protection Regulation – The Future of Data Protection	5
3. The Legal Structure of German Data Protection Law	6
II. The underlying Principles of the German Data Protection Concept	8
1. General Principles	8
a) Personal Data	8
b) Scope of the BDSG: Automated and Non-Automated Collection, Processing and Use of Personal Data	9
aa) Automated Processing	9
bb) Non-Automated Filing System	9
c) Collection, Processing and Use of Personal Data	10
d) Legal Permission	11
e) Consent	11
aa) Free Decision of the Data Subject	11
bb) Informing the Data Subject	12
cc) Consent for Sensitive Data	13
dd) Formal Requirements	13
ee) Revocation of the Consent	14
f) Further Requirements of Lawful Data Processing	15
aa) Collection from Data Subject	15
bb) Principle of Data Reduction and Data Economy	16
g) The Controller	17

2. When does German Data Protection Law apply?	17
III. Rights of the Data Subject and Legal Consequences of a Breach of Law	19
1. Rights of the Data Subject	19
2. Further Legal Consequences	20
B. The Regulatory Framework: Supervisory Authorities and Compliance	21
I. The Role and Position of the Supervisory Authorities	21
1. The Federal and State Structure of the Supervisory Authorities	21
2. The Separation between Public and Private Entity Supervision	21
3. Scrutiny of the Supervisory Authorities' Roles and Dependencies	22
4. Changes to the Judicial Review Process	22
5. Headcount Ramp-up in the Supervisory Authorities	22
6. The Role of the Dusseldorf Circle	23
II. Notification Duties – Not Necessary in Germany!	24
1. Obligation to Notify	24
2. Exceptions from the Notification Duty	25
III. The Data Protection Officer and how to integrate him into your Compliance Organisation	26
1. Obligation to appoint a Data Protection Officer	26
2. The German DPO – a unique Function in the EU	27
3. Dispensing with Notification Requirements	29
4. The Duties of the DPO in General	29
5. Does the DPO need to be a Lawyer?	30
6. Beware of the “Placeholder” DPO	30
7. The DPO and its Interface to the Supervisory Authority	30
8. Avoiding Conflicts of Interest	30
9. The External DPO as an Alternative	31
10. The DPO on an EU Level	31
C. Customer and Supplier Data Protection	31
I. General Requirements	31
II. Use of Customer Data for “Own Commercial Purpose” (Sec.28 para.1 BDSG)	32
III. Use of Customer Data for “Marketing Purposes” (Sec.28 para.3 BDSG)	33
1. The Use of Personal Data for Marketing Purposes without Consent	34
a) Use of Personal Data for Advertising Purposes	34
b) Transferring Data for Advertising Purposes and Address Trading	36
aa) Sec.28 para.3 BDSG	36
bb) Sec.29 BDSG	37
2. The Use of personal Data for Marketing Purposes with Consent	37
a) Formal Requirements	37
b) Use of Standard Consent Forms	38
c) Consent under the TMG	38

3. Restrictions of Unfair Competition Law (UWG)	39
a) Distinction between Marketing Measures	39
b) Declaration of Consent (Double Opt-In)	40
4. Commercial Data Collection and Recording for the Purpose of Market or Opinion Research	40
IV. Data Protection in Regard to Website Publishers	42
1. Privacy Policy	42
2. Online Marketing and corresponding Consent	43
3. Use of Cookies, Tracking and Analytic Tools	45
a) Use of Cookies	45
b) Use of Web Tracking and Analytic Tools	45
V. Video Surveillance	47
D. Employee Data Protection – Using Employee Data in Globally Operating Organisations	48
I. Data Processing for Employment-related Purposes	48
II. Centralised Functions and the Use of Personal Data	50
1. General Concepts of centralised Functions	50
2. The Legal Employer and its Key Position	50
3. The Absence of “Group Regulations” and its Effects	50
4. The Position of the Dusseldorf Circle	51
5. The “need to know” Principle	51
6. Self-Generated and perceived Needs to Know	52
7. The Issue of Consent in Employee Relationships	52
III. The Role of the German Works Council – Codetermination and Information Obligations	53
1. Works Council and Works Agreement	53
2. Matching Works Councils and DPOs	54
a) Limits to the Works Council Codetermination Rights	54
b) The DPO as Expert for the Works Council	54
c) Supervision of Works Councils by the DPO	54
d) Cases of Conflict between Works Council and DPO	55
IV. Social Media and Social Networks	55
1. Use of Social Media and Social Networks as Sources of Infor- mation	55
2. Use of Social Media and Social Networks as Means of Publi- cation	56
V. Compliance Requirements vs. Data Protection Requirements	56
VI. Mergers & Acquisitions and Personal Data in Due Diligence Procedures	57
E. International Transfer of Personal Data	58
I. Legal Requirements according to Sec. 4b BDSG	58
1. International Data Transfer within the EU or EEA Area	59
2. International Data Transfer to Countries outside of the EU or EEA	59
II. Safeguarding Data Transfers to the U.S.	60
1. Safe Harbor invalidated	60
2. EU-U.S. Privacy Shield	60
III. Derogations according to Sec. 4c para. 1 BDSG	61
IV. Derogations according to Sec. 4c para. 2 BDSG	62

1. Standard Contractual Clauses	63
2. Binding Corporate Rules	63
a) Misconceptions as to the BCR	63
b) Drawbacks of the Implementation	64
c) Future Development of BCR	64
F. Commissioned Data Processing inside and outside of the EU/EEA ..	65
I. Legal Requirements for Commissioned Data Processing	65
1. Commissioned Data Processing in Germany, within the EU and the EEA	65
a) General Principles	65
b) Agreement on Commissioned Data Processing	67
2. No privilege for Commissioned Data Processing outside the Area of the European Union and the EEA.	69
a) Is Sec. 11 BDSG applicable to Commissioned Data Pro- cessing outside of the EU or EEA?	70
b) Deviation from European Regulations	70
II. Data Protection in the Cloud	72
G. Useful Toolkit for Companies for Compliance with Data Protection Law	73

Part 2

Relevant Statutory Material

Bundesdatenschutzgesetz (BDSG)	75
Federal Data Protection Act (BDSG)	75