

Table of Contents

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
2. The European General Data Protection Regulation – The Future of Data Protection?	5
3. The legal structure of German Data Protection Law	5
II. The underlying principles of the German Data Protection Concept	7
1. General Principles	7
a. Personal data	7
b. Scope of the BDSG: automated and non-automated collection, processing and use of personal data	8
c. Collection, processing and use of personal data	9
d. Legal permission	9
e. Consent	9
aa. Free decision of the data subject	10
bb. Informing the data subject	11
cc. Consent for sensitive data	11
dd. Formal requirements	12
ee. Revocation of the consent	12
f. Further requirements of lawful data processing	12
aa. Collection from data subject	12
bb. Principle of data reduction and data economy	13
g. The controller	14
2. When does German data protection law apply?	14
III. Rights of the Data Subject and Legal Consequences of Breach of Law	15
B. The Regulatory Framework: Supervisory Authorities and Compliance	17
I. The Role and Position of the Supervisory Authorities	17
1. The Federal and State Structure of the Supervisory Authorities	17
2. The Separation between Public and Private entity Supervision	17
3. Scrutiny of the Supervisory Authorities' Roles and Dependencies	17
4. Changes to the Judicial Review Process	18
5. Headcount Ramp-up in the Supervisory Authorities	18
6. The Role of the Düsseldorf Circle	18
II. Notification Duties – Not necessary in Germany!	19
1. Obligation to notify	20
2. Exceptions from the notification duty	20

III. The Data Protection Officer and how to integrate him into your Compliance Organisation.....	21
1. Obligation to appoint a Data Protection Officer	21
2. The German DPO – a unique Function in the EU	22
3. Dispensing with Notification Requirements	23
4. The Duties of the DPO in General	23
5. Does the DPO need to be a Lawyer?	23
6. Beware of the "Placeholder" DPO	24
7. The DPO and its Interface to the Supervisory Authority	24
8. Avoiding Conflicts of Interest	24
9. The external DPO as an alternative	25
10. The Future of the DPO on an EU Level.....	25
C. Customer and Supplier Data Protection – Proving a Web Trust to your Partners.....	27
I. General requirements	27
II. Use of customer data for "own commercial purpose" (Sec. 28 para. 1 BDSG).....	27
III. Use of customer data for "marketing purposes" (Sec. 28 para. 3 BDSG).....	28
1. The use of personal data for marketing purposes without consent	29
a. Use of personal data for advertising purposes	29
b. Transferring for advertising purposes and address trading	30
2. The use of personal data for marketing purposes with consent	32
a. Formal requirements	32
b. Using of standard consent forms.....	32
c. Consent under the TMG	33
3. Restrictions of unfair competition law (UWG).....	33
a. Distinction between marketing measures	33
b. Declaration of consent (Double Opt-In)	34
4. Commercial data collection and recording for the purpose of market or opinion research	35
IV. Data protection in regard to website publishers.....	35
1. Privacy Policy	35
2. Online marketing and corresponding consent.....	36
3. Use of cookies, tracking and analytic tools	37
a. Use of cookies	37
b. Use of web tracking and analytic tools.....	38
V. Video surveillance & Street View	39
1. Video surveillance	39
2. Google Street View	40
VI. Disclosure of Data – Consequences of breaching applicable data protection rules	40
VII. Annex: Useful Toolkit for companies for compliance with data protection law.....	41

D. Employee Data Protection – Using Employee Data in Globally Operating Organisations	43
I. Centralised Functions and the Use of Personal Data	43
1. General Concepts of Centralised Functions	43
2. The Legal Employer and its Key Position	43
3. The Absence of "Group Regulations" and its Effects	43
4. The Position of the Düsseldorf Circle	44
5. Practical Implementation of Düsseldorf Circle Guidance	44
6. The "N+x" Approach	44
7. Self-Generated and Perceived Needs to Know	45
8. The Issue of Consent in Employee Relationships	45
9. Anticipated Development on the EU Level	45
II. The Role of the German Works Council – Co-Determination and Information Obligations	46
1. Works Council and Works Agreement	46
2. Matching Works Councils and DPOs	47
a. Limits to the Works Council Codetermination Rights	47
b. The DPO as Expert for the Works Council	47
c. Supervision of Works Councils by the DPO	47
d. Cases of Conflict between Works Council and DPO	48
III. Social Media and Social Networks	48
1. Use of Social Media and Social Networks as Sources of Information	48
2. Use of Social Media and Social Networks as Means of Publication	49
IV. Compliance Requirements vs. Data Protection Requirements	50
V. Mergers & Acquisitions and personal data in due diligence procedures	51
E. International Transfer of Personal Data	53
I. Legal requirements according to Sec. 4b BDSG	53
1. International data transfer within the EU or EEA area	53
2. International data transfer to countries outside of the EU or EEA area	54
II. Safeguarding data transfers to the US – Safe Harbor Principles	54
III. Derogations according to Sec. 4c para. 1 BDSG	55
IV. Derogations according to Sec. 4c para. 2 BDSG	56
1. Standard Contractual Clauses	56
2. Binding Corporate Rules	56
a. Misconceptions as to the BCR	57
b. Drawbacks in the implementation	57
c. Future Development of BCR	57
d. BCR – Still the method of choice?	58
F. Commissioned Data Processing in- and outside of the EU/EEA	59
I. System and legal requirements for commissioned data processing	59

1. Commissioned data processing in Germany, within the EU and the area of the EEA	59
a. General Principles	59
b. Agreement on commissioned data processing	60
2. No privilege for commissioned data processing outside the area of the European Union and the EEA	62
a. Is Sec. 11 BDSG applicable to commissioned data processing outside of the EU or EEA?	62
b. Deviation from European regulations	63
II. Central Processing and End-to-End Transfer of Personal Data within Groups of Companies	64
1. A Viable Model	64
2. Use of Central Platform Resources by the Controllers	65
3. End-to-End Transfer of Personal Data between Controllers	65
III. Data Protection in the Cloud	66
Annex Federal Data Protection Act (bi-lingual German-English)	69
Index	159