

Table of contents

About this second edition, contributors and the author	x
Key terms	xii
How to use this Field Guide	1
1. Key concepts	4
1.1 The field: data protection, privacy and security	4
1.1.1 Data protection	4
1.1.2 Data privacy	5
1.1.3 Data security	6
1.1.4 Data privacy as an umbrella term	6
1.2 The territory: Europe, United States and ROW	6
1.3 The species: personal data, PII and sensitive data	7
1.3.1 Personal data	8
1.3.2 Personally identifiable information (PII)	9
1.3.3 Sensitive data	9
1.4 Activities encountered: transfers and other forms of processing	10
1.5 The observed: data controllers, processors	12
1.6 The game wardens: data protection authorities, officers	13
2. Starting a compliance program	14
2.1 Taking charge	14
2.2 Working with internal stakeholders and outside advisors	16
2.2.1 Internal stakeholders	16
2.2.2 Outside advisors	16
2.3 Appointing a privacy officer	17
2.3.1 Requirement to appoint a data protection officer under German law	18
2.3.2 Mandatory or beneficial appointments in other jurisdictions	21
2.4 Preparing a task list	23
2.4.1 Take inventory of your data	26

2.4.2	Define your objective and priorities	26
2.4.3	Find the best approach for your company	27
2.4.4	Identify legal and other requirements	29
2.4.5	Data privacy by region – an overview for orientation purposes	31
2.4.6	What other laws and requirements have to be considered?	34
2.4.7	Identify applicable substantive compliance requirements	34
2.4.8	Identify applicable formal compliance requirements	37
2.5	Executing tasks	38
3.	International data transfers	40
3.1	Three hurdles	42
3.2	Compliance mechanisms compared	48
3.2.1	Consent and contracts can offer flexibilities	48
3.2.2	Geographical and topical coverage of data and transfers	49
3.2.3	Implementation costs and timing	50
3.2.4	Ongoing administration	51
3.2.5	Onward transfers	52
3.2.6	Submission to European law and jurisdiction	54
3.2.7	Customer and public relations benefits	55
3.3	Implementation	58
3.3.1	Statutory, contractual transfer obligations	58
3.3.2	Consent	61
3.3.3	Data transfers based on standard contractual clauses	61
3.3.4	Safe Harbor Certification	63
3.3.5	Binding Corporate Rules	65
3.4	Data transfers from countries outside the EEA	66
4.	Drafting documentation	68
4.1	Why are you creating the document?	68
4.1.1	Legal purposes	69
4.1.2	Marketing purposes	70
4.1.3	Organizational purposes	71
4.2	Who is your audience?	71
4.3	Categories and examples of documentation	73
4.3.1	Other labels, e.g., policies	74

4.4	Notices	75
4.4.1	To whom do you have to issue notices?	78
4.4.2	Who should issue notices – service provider or customer?	78
4.4.3	Which topics do you typically have to address in privacy notices?	79
4.4.4	Form and delivery requirements	84
4.5	Consent	85
4.6	How to obtain valid consent	88
4.7	Opt-in, out and in between	90
4.7.1	Examples of consent mechanisms	90
4.7.2	Minimum requirements	92
4.7.3	Selecting implementation options	92
4.7.4	Silence as consent	92
4.7.5	Affirmative, express consent	93
4.8	Above and beyond opt-in consent	94
4.9	Other considerations for consent drafting	95
4.9.1	Incorporation of notices into consent declarations	95
4.9.2	Expressing focused consent	96
4.9.3	Placement of consent mechanism and declaration	97
4.9.4	Who should obtain consent – data controller or processor?	97
4.10	Agreements	98
4.10.1	Agreements with data subjects vs. consent from data subjects	98
4.10.2	Asking for an express acceptance of website privacy statements or general privacy notices	98
4.10.3	Agreements instead of consent	100
4.10.4	Commercial agreements between companies	100
4.10.5	Terms for data processing services agreements	102
4.11	Protocols	104
4.12	Questionnaires and data submission forms	105
4.13	Documenting decisions and compliance efforts	106
4.14	Government notifications, approvals	107
5.	Maintaining and auditing data privacy compliance programs	110
5.1	The maintenance challenge	110

5.2	Documentation	110
5.3	Taking over or auditing an existing compliance program	110
5.4	Due diligence in M&A scenarios	112
5.4.1	Due diligence on service providers and vendors	113
6.	Data privacy A–Z	115
	Advertising	116
	Big data, data brokers and the Internet of everything	118
	Cloud computing	120
	Data retention	134
	Employee data and monitoring	138
	Financial information	150
	Government investigations, information requests	151
	Health information	154
	Information processing fairness – FIPs	156
	Jurisdiction	158
	K – Contracts	161
	Location data	162
	Minors	163
	Notification of data security breaches and other notices and notifications	164
	Ownership	169
	Privacy by design	170
	Questionnaires	171
	Rights, remedies, enforcement	172
	Social media	177
	Tracking	179
	Unsolicited communications (spam email, cold calls, etc.)	184
	Vendor management	190
	Wiretapping	192
	X-rays, genes, fingerprints, faces – biometric data	193
	Y – Why protect data privacy?	195
	Zip codes, IP addresses and other numbers	198
	Checklist	201
	Resources	205
	Abbreviations	207
	Index	211