

Neues Datenschutzrecht

in der Reihe:

Bearbeitungs- und Prüfungsleitfaden

Prozesse prüfen * Risiken vermeiden * Fehler aufdecken
→ Handlungsempfehlungen ableiten



Bearbeitungs- und Prüfungsleitfaden

Neues Datenschutzrecht

Mike Bona-Stecki

Manager/Auditor Informationssicherheit
DekaBank
Frankfurt am Main

Dr. Martin Andreas Duncker (Hrsg.)

Dr. Martin Andreas Duncker Rechtsanwalt und Fachanwalt
für Bank- und Kapitalmarktrecht Zertifizierter Compliance-
Beauftragter (IHK & TÜV) Schlatter Rechtsanwälte
Steuerberater PartGmbH



Thomas Göhrig

Berater für Informationssicherheit und Datenschutz
FCH Compliance GmbH

Dr. Ulrich Hallermann (Hrsg.)

Dr. Ulrich Hallermann Rechtsanwalt und Fachanwalt für
Arbeitsrecht Datenschutzbeauftragter Investitions- und
Strukturbank Rheinland-Pfalz (ISB)

Dr. Markus Lang

Dr. Markus Lang Rechtsanwalt Externer
Datenschutzbeauftragter

Christian Maul (Hrsg.)

Spezialist Compliance
FCH Compliance GmbH
Heidelberg





Dr. Stephanie Müller
Referentin beim Bundesbeauftragten
für den Datenschutz und die Informationsfreiheit

Denise Primus
Rechtsanwältin
Schlatter Rechtsanwälte Steuerberater PartG mbB
Heidelberg

Jürgen Ranger
Projektleiter Strategische Projektportfoliosteuerung
Creditplus Bank AG
Stuttgart

Inhaltsübersicht

A. Vorwort (<i>Mauß</i>)	1
B. Aufsichtliche Würdigung (<i>Müller</i>)	5
C. Aufbau und Funktion der Datenschutzorganisation (<i>Ranger</i>)	15
D. Löschpflicht und Löschkonzepte (<i>Duncker/Primus</i>)	57
E. Kundendatenschutz (<i>Lang</i>)	107
F. Beschäftigtendatenschutz und Fraud Maßnahmen (<i>Hallermann</i>)	165
G. Technische und organisatorische Maßnahmen (<i>Bona-Stecki</i>)	213
H. Aktuelle Sonderthemen des Datenschutzes (<i>Mauß</i>)	271
I. Datenschutz bei Datenauswertungen & Big Data (<i>Göbrig</i>)	299



Inhaltsverzeichnis

A.	Vorwort	1
B.	Aufsichtliche Würdigung	5
I.	Inhalte und Bedeutung des Datenschutzmanagements	7
II.	Zuständigkeiten und Zusammenspiel der Behörden	8
1.	Bundesrepublik Deutschland	8
2.	EU	9
3.	Zusammenarbeit mit anderen Staaten	12
4.	Aufgaben und Befugnisse der Aufsichtsbehörden	13
III.	Datenschutzkontrollen und Zertifizierungen	14
C.	Aufbau und Funktion der Datenschutzorganisation	15
I.	Verhältnis von Compliance-Funktion, Risikomanagement und Datenschutz	17
II.	Grundsätze des Datenschutzes	21
1.	Zulässigkeit der Verarbeitung und Grundsatz der Zweckbindung	23
2.	Grundsatz der Datensparsamkeit und -Vermeidung/ Verhältnismäßigkeitsgrundsatz	24
III.	Datenschutzbeauftragter	28
1.	Benennung und Stellung des Datenschutzbeauftragten	28
2.	Aufgaben des Datenschutzbeauftragten	29
3.	Eignung durch Fachkunde und Zuverlässigkeit	32
IV.	Bestandteile des Datenschutzmanagements	33
1.	Verarbeitungsverzeichnis	33
2.	Datenschutz-Richtlinie	40
3.	Risikoanalysen und Datenschutzfolgenabschätzungen	43
4.	Technische und organisatorische Maßnahmen	48
5.	Vertragswesen der verantwortlichen Stelle mit Dritten	51

a)	Auftragsverarbeitungsverträge	51
b)	Verträge bei gemeinsamer Datenverantwortlichkeit	53
c)	Datenübermittlungen in Drittstaaten	53
D.	Löschpflicht und Löschkonzepte	57
I.	Datenschutzrechtliche Einordnung	59
1.	Zum Begriff »Löschen«	62
2.	Verarbeitungsverbot mit Erlaubnisvorbehalt	63
3.	Recht auf Löschung und Pflicht zur Löschung	63
a)	Löschgründe	64
b)	Einschränkung der Löschpflicht: Rückausnahmen	69
c)	Zusätzliche Maßnahmen bei erfolgter Veröffentlichung: Informationspflicht	76
4.	Löschpflicht nach Zweckerreichung?	79
5.	Rechtsfolge: »Unverzügliches« Löschen der personenbezogenen Daten	81
II.	Technische und organisatorische Umsetzung der Löschpflichten	82
1.	Löschkonzepte in ERP-Systemen	88
a)	Mögliche Vorgehensweisen	89
b)	Häufige Probleme/Risiken	90
c)	Praxishinweise	91
2.	Löschkonzepte in Laufwerkstrukturen/ Verzeichnisstrukturen	92
a)	Mögliche Vorgehensweisen	93
b)	Häufige Probleme/Risiken	94
c)	Praxishinweise	95
3.	Papierhafte Aufbewahrungsformen wie Ordnersysteme oder Archive	97
a)	Mögliche Vorgehensweisen	97
b)	Häufige Probleme/Risiken	98
c)	Praxishinweise	98
III.	Sperrung von Datensätzen als Alternative zur Löschung	99
1.	Rechtliche Einordnung	100

2. Technisch-organisatorische Umsetzung	101
3. Häufige Probleme/Risiken	102
4. Praxishinweise	102
IV. Zusammenfassung	103
V. Literaturverzeichnis	103
E. Kundendatenschutz	107
I. Ausgangspunkt	109
1. Datenschutz und Bankgeheimnis	109
2. Datenschutzrechtliche Zulässigkeit	110
II. Analyse von Kundendaten	111
1. Wesentliche Vorgaben	111
2. Checkliste	113
3. Praxishinweise	114
III. Scoring	114
1. Wesentliche Vorgaben	115
a) Erlaubnistatbestände	115
b) Weitere Vorgaben gem. § 31 BDSG	116
2. Checkliste	117
3. Praxishinweise	120
IV. Automatisierte Entscheidungen im Einzelfall	121
1. Wesentliche Vorgaben	121
a) Zulässigkeit	122
b) Profiling	122
2. Checkliste	123
3. Praxishinweise	125
V. Datenweitergabe an Auskunfteien	125
1. Wesentliche Vorgaben	125
2. Checkliste	128
3. Praxishinweise	128

VI.	Verarbeitung zu werblichen Zwecken und werbliche Ansprache	129
1.	Wesentliche Vorgaben	129
a)	Verarbeitung zu Zwecken der Werbung auf Basis von Art. 6 Abs. 1 lit. f DSGVO	130
b)	Verarbeitung zu Zwecken der Werbung auf Basis einer Einwilligung	132
c)	Werbung per Telefon, Fax, SMS und E-Mail	134
2.	Checkliste	136
3.	Praxishinweise	139
VII.	Kundenzufriedenheitsbefragungen	140
1.	Wesentliche Vorgaben	140
2.	Checkliste	141
3.	Praxishinweise	142
VIII.	Widerspruchsrecht	143
1.	Wesentliche Vorgaben	143
a)	Allgemeines Widerspruchsrecht	143
b)	Widerspruchsrecht bei Direktwerbung	144
2.	Checkliste	145
3.	Praxishinweise	146
IX.	Recht auf Auskunft	147
1.	Wesentlicher Inhalt	147
a)	Pflicht zur Auskunft	147
b)	Inhalt der Auskunft	147
c)	Verfahren und Form der Auskunft	149
d)	Ausnahmen von der Auskunftspflicht	150
e)	Verstoß gegen die Auskunftspflicht	151
2.	Checkliste	151
3.	Praxishinweise	153
X.	Weitere Rechte der Kunden (Berichtigung, Löschung und Einschränkung)	154
1.	Wesentliche Vorgaben	155
a)	Recht auf Berichtigung	156

b) Recht auf Löschung	156
c) Recht auf Einschränkung der Verarbeitung	157
d) Recht auf Datenübertragbarkeit	158
2. Checkliste	159
3. Praxishinweise	160
XI. Melde- und Benachrichtigungspflicht bei Verletzung des Datenschutzes nach Art. 33 und 34 DSGVO	160
1. Wesentliche Vorgaben	160
2. Checkliste	162
3. Praxishinweise	163
XII. Literaturverzeichnis	163
F. Beschäftigtendatenschutz und Fraud Maßnahmen	165
I. Grundlagen des Beschäftigtendatenschutzes	167
1. Die rechtliche Ausgangslage unter Berücksichtigung der Datenschutzgrundverordnung	167
a) Definition des Beschäftigten	167
b) Datenschutz des Beschäftigten	167
c) Checklisten	172
2. Datenschutz in der Bewerbungsphase	175
a) Erheben und Speichern in der Bewerbungsphase	175
b) Verarbeiten und Nutzen in der Bewerbungsphase	176
c) Problematik der AGG Klagen auch im Datenschutz?	177
d) Facebook, Fanpages und der Datenschutz	177
3. Datenschutz im Beschäftigtenverhältnis	179
a) Erheben und Speichern nach Einstellung	179
b) Verarbeiten und Nutzen im Beschäftigtenverhältnis	179
c) Auftragsverarbeitungen (Art. 28 DSGVO) und gemeinsame Verantwortung (Art. 26 DSGVO)	180
d) Datenschutzfolgenabschätzung	181
e) Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO)	181
f) Verpflichtung auf das Datengeheimnis nach der DSGVO	182

g)	Betriebsvereinbarungen	182
h)	Informationspflichten gegenüber Arbeitnehmern gem. Art. 13 DSGVO	183
4.	Checklisten	184
a)	Checkliste für den Fachbereich	184
b)	Zusammenfassende Checkliste für die Revision/Wirtschaftsprüfung	190
5.	Übermittlung personenbezogener Daten im Konzern	191
a)	Wesentliche Vorgaben	191
b)	Checkliste	192
II.	Datenschutz und Compliance	193
1.	Abgrenzung von Datenschutz und Compliance	193
2.	Ergebnis	194
3.	Checklisten	195
a)	Checkliste für betroffene Abteilungen (insbesondere Personal und Datenschutz)	195
b)	Checkliste für Revision und Wirtschaftsprüfung	196
III.	Zulässigkeit der Verarbeitung von Mitarbeiter- und Kundendaten in Research Systemen	197
1.	Abgrenzung zur datenschutzrechtlichen Zulässigkeit der Aufdeckung von begangenen Straftaten	197
2.	Die Regelung zum Research in § 25 h KWG	198
3.	§ 25 h KWG und der Datenschutz	198
4.	Vorschlag für die Praxis	199
5.	Checklisten	200
a)	Hausintern (Fraud, Geldwäsche und Datenschutz)	200
b)	Checkliste für Revision und Wirtschaftsprüfung	203
IV.	Erhebung von Beschäftigtendaten zur Aufdeckung von Straftaten/behördliche Ermittlungsbefugnisse	204
1.	Aufdeckung von Straftaten und behördliche Ermittlungsbefugnisse	204
a)	Grundlagen zur Aufdeckung von Straftaten	204
b)	Behördliche Ermittlungsbefugnisse	206

c) Aufdeckung von Straftaten durch die Videüberwachung (BAG vom 23.08.2018, 2 AZR 133/18)	207
2. Checklisten	208
a) Checklisten Aufdeckung von Straftaten	208
b) Checklisten Behördliche Ermittlungsbefugnisse	210
V. Zusammenfassende Praxistipps	211
VI. Literaturhinweise	211
G. Technische und organisatorische Maßnahmen	213
I. Einführung	215
1. Grundlagen und Begriffsbestimmung	215
2. Rechtliche Einordnung	216
3. Änderungen durch die DSGVO	217
II. Überblick über die technischen und organisatorischen Maßnahmen	218
1. Vertraulichkeit	219
a) Wesentliche Inhalte	219
b) Risiken	219
c) Maßnahmen	220
d) Checkliste	226
e) Praxishinweise	229
2. Integrität	229
a) Wesentliche Inhalte	229
b) Risiken	229
c) Maßnahmen	230
d) Checkliste	232
e) Praxishinweise	232
3. Verfügbarkeit/Belastbarkeit	232
a) Wesentliche Inhalte	232
b) Risiken	233
c) Maßnahmen	233
d) Checkliste	239
e) Praxishinweise	242

4.	Wiederherstellbarkeit bei physischen oder technischen Zwischenfällen	242
	a) Wesentliche Inhalte	242
	b) Risiken	243
	c) Maßnahmen	243
	d) Checkliste	248
	e) Praxishinweise	249
5.	Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit	249
	a) Wesentliche Inhalte	249
	b) Risiken	250
	c) Maßnahmen	250
	d) Checkliste	252
	e) Praxishinweise	253
6.	Pseudonymisierung und Verschlüsselung personenbezogener Daten	253
	a) Wesentliche Inhalte	253
	b) Risiken	254
	c) Maßnahmen	254
	d) Checkliste	256
	e) Praxishinweise	257
III.	Wahl der geeigneten Maßnahmen	258
	1. Grundsätzliches	258
	2. Nutzung von Standards und Normen	261
	3. Standard-Datenschutzmodell	263
IV.	Sicherheit der Verarbeitung bei Auftragsverarbeitungen und Auftragsverarbeiter	264
	1. Vorgaben an Auftragsverarbeitungen und Auftragsverarbeiter	264
	a) Rechtliche Grundlagen	264
	b) Risiken	264
	c) Maßnahmen	264
	d) Checkliste	266
	e) Praxishinweise	267

2. Überwachung der Einhaltung	267
a) Vor-Ort-Kontrollen	268
b) Nachweise, Zertifikate oder Testate	268
c) Praxishinweise	269
V. Literaturverzeichnis	269
H. Aktuelle Sonderthemen des Datenschutzes	271
I. Messengerdienste	273
1. Beschreibung des Themas	273
2. Datenschutzrechtliche Einordnung	274
3. Praxishinweise	290
II. ePrivacy-VO	290
1. Ausblick	290
2. Praxistipps	296
III. Literaturverzeichnis	297
I. Datenschutz bei Datenauswertungen & Big Data	299
I. Reichweite des Begriffs »personenbezogene Daten«	301
II. Einführung eines BI-Tools	302
1. Organisatorische Rahmenbedingungen	302
2. Datenschutzrechtliche Beurteilung	302
a) Rechtmäßigkeit und Zweckbindung	303
b) Datenminimierung und Speicherbegrenzung	306
c) Richtigkeit	307
d) Integrität und Vertraulichkeit	307
3. Checkliste	309
III. Datenschutz-Folgenabschätzung	310
1. Vorprüfung	310
2. Durchführung der Folgenabschätzung	311
a) Beschreibung der Verarbeitung	311
b) Notwendigkeit und Verhältnismäßigkeit	312
c) Risikobewertung	312

INHALTSVERZEICHNIS

d) Maßnahmen	312
e) Standpunkt der Betroffenen	313
f) Restrisiko	313
IV. Datenauswertungen	314
1. Organisatorische Rahmenbedingungen	314
2. Datenschutzrechtliche Beurteilung	315
a) Rechtmäßigkeit und Zweckbindung	315
b) Datenminimierung und Speicherbegrenzung	316
c) Richtigkeit	316
d) Integrität und Vertraulichkeit	317
V. Checkliste	318



A.

Vorwort





A. Vorwort

Zum 25. Mai 2018 trat die Europäische Datenschutz-Grundverordnung (EU-DSGVO) in Kraft und ersetzte das bisherige Bundesdatenschutzgesetz (BDSG) als maßgebende Rechtsvorschrift in Sachen Datenschutz. Parallel zur EU-DSGVO trat das neue Bundesdatenschutzgesetz in Kraft und konkretisiert die für die EU-Mitgliedsstaaten in der EU-DSGVO enthaltenen Öffnungsklauseln. 1

Im Jahre 1970 verabschiedete Hessen das erste Datenschutzgesetz der Welt und schuf somit den ersten Meilenstein des deutschen Datenschutzrechts. Seitdem folgten zahlreiche technische und rechtliche Entwicklungen und der Schutz personenbezogener Daten gewann zunehmend an Bedeutung. Aufgrund dieser Historie verwundert es nicht, dass auch in der Neuregelung des Datenschutzrechts altbekannte Themen in mehr oder minder bekanntem Umfang wiederzufinden sind. Trotz alledem ist die EU-DSGVO mehr als alter Wein in neuen Schläuchen, denn ihre Einführung brachte umfangreiche Änderungen und Herausforderungen mit sich, welche Verantwortliche Stellen noch heute beschäftigen. Die Spannbreite der Handlungsfelder reicht von Dokumentations- und Nachweispflichten, über die Umsetzung von Betroffenenrechten und technisch-organisatorischen Maßnahmen, bis hin zu Sonderkonstellationen bei Datenübermittlungen innerhalb und außerhalb eines Unternehmens oder einer Unternehmensgruppe, sowohl im europäischen In- als auch im Ausland. 2

Die Summe der einzelnen Themen und deren Verknüpfung untereinander erforderte die Einführung eines Datenschutzmanagements zur rechtskonformen Umsetzung regulatorischer Anforderungen und der gleichzeitig möglichst hohen Effektivität getroffener Maßnahmen. In seiner neuen Ausrichtung unter der EU-DSGVO wurde die Datenschutzfunktion mehr und mehr an bestehende Compliance-Funktionen angepasst und verortet sich nunmehr als Bestandteil der zweiten Verteidigungslinie im Modell der three-lines-of-defense. 3

Dieses Buch dient sowohl als Arbeitsunterlage für Datenschutzbeauftragte, Syndikusrechtsanwälte, Rechtsanwälte, Berater und Wissenschaftler, sowie als Prüfungshilfe für Revisoren und Datenschutzauditoren. Es befasst sich sowohl mit den Grundlagen des Datenschutzes als auch themenspezifischen Herausforderungen, sowie aktuellen rechtlichen Entwicklungen und Erfahrungen der Aufsichtsbehörden und unterstützt durch zahlreiche praxisorientierte Checklisten im Alltag. 4





B.

Aufsichtliche Würdigung





B. Aufsichtliche Würdigung

I. Inhalte und Bedeutung des Datenschutzmanagements

Auf Grund des bereits im 17. Jahrhundert bekannten Bankgeheimnisses werden die von den Kreditinstituten vorgehaltenen und generierten Kundendaten seit jeher mit großer Sorgfalt verwahrt. 5

Kreditinstitute speichern naturgemäß sehr viele personenbezogene Daten. Sowohl die Kontaktinformationen als auch die mit dem Zahlungsverkehr verbundenen Informationen enthalten personenbezogene Daten. Informationen des Zahlungsverkehrs können besonders schützenswerte personenbezogene Daten enthalten, da sich beispielsweise aus Arztrechnungen, Gewerkschaftsmitgliedsbeiträgen oder Spenden an Parteien Rückschlüsse ziehen lassen. Fragen des Datenschutzes sind beim operationellen Risiko zu berücksichtigen. Datenschutzverletzungen können auch Folgen für die Reputation eines Kreditinstituts haben. Da die Verstöße gegen datenschutzrechtliche Regelungen auch sehr hohe Bußgelder nach sich ziehen können, ist ein effektives Datenschutzmanagementsystem für den Verantwortlichen von großer Bedeutung. 6

Die Verantwortung für die Einhaltung von Datenschutzregelungen ist die Aufgabe des Verantwortlichen, auch wenn die Geschäftsleitung diese Aufgabe gelegentlich beim Datenschutzbeauftragten sieht. Die DS-GVO und die nationalen Vorschriften enthalten eine klare Aufgabenzuweisung beim Verantwortlichen. Der Datenschutzbeauftragte berät die Geschäftsleitung hinsichtlich der Einhaltung von datenschutzrechtlichen Vorschriften und führt ggf. entsprechende Kontrollen durch. Darüber hinaus ist die Beratungsfunktion des Datenschutzbeauftragten sowohl für Mitarbeiter als auch für Externe von großer Bedeutung. Datenschutzaufsichtsbehördlicher Sicht ist der Datenschutzbeauftragte neben dem Verantwortlichen selbst der Ansprechpartner bei datenschutzrechtlichen Fragestellungen. Durch regelmäßige Schulungen der Mitarbeiter können diese für die Fragen des Datenschutzes im Arbeitsalltag sensibilisiert werden. Erfahrungsgemäß lassen sich mittels Hinweisen und einfachen Hilfestellungen einige Datenschutzverstöße vermeiden. Eine regelmäßige Überprüfung der internen Vorgaben und deren Handhabung ist ratsam, damit der Verantwortliche bei einer Kontrolle durch die Aufsichtsbehörde diesbzgl. gut vorbereitet ist. 7

II. Zuständigkeiten und Zusammenspiel der Behörden

- 8 Die DS-GVO enthält in ihrem sechsten Kapitel (Art. 51 bis 59 DS-GVO) Regelungen für die unabhängigen Aufsichtsbehörden. Diese werden durch die nationalen Regelungen des BDSG ergänzt.
- 9 Die Aufsichtsbehörden sind in jedem Mitgliedsstaat der EU bis zum 25. Mai 2018 einzurichten gewesen. Die Aufsichtsbehörden bilden ein Netzwerk bei einem materiell weitgehend harmonisierten Datenschutzrecht¹. Dabei ist in das Netzwerk auf der Ebene der EU-Mitgliedsstaaten und das föderale System in der Bundesrepublik Deutschland zu unterscheiden. Die Datenschutzaufsichtsbehörden sind unabhängige Kontroll- und Aufsichtsstellen, Art. 52 Abs. 1 DS-GVO².

1. Bundesrepublik Deutschland

- 10 Auf Grund des Föderalismus in der Bundesrepublik Deutschland ist die Datenschutzaufsicht föderal organisiert. Jedes Land verfügt über mindestens eine Datenschutzaufsichtsbehörde, darüber hinaus hat auch der Bund eine eigene Datenschutzaufsichtsbehörde. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ist zuständig für die Einrichtungen des Bundes sowie die Post- und Telekommunikationsunternehmen. Im Fall der Bundesgerichte erstreckt sich die Zuständigkeit nur auf Verwaltungstätigkeiten und nicht die Aufgaben der Justiz³. Darüber hinaus ist er auch im Bereich der Finanzbehörden im Anwendungsbereich der Abgabenordnung zuständig, durch Landesgesetz können im Bereich der Finanzbehörden weitere Aufgaben übertragen werden. Bislang hat hiervon lediglich die Freie und Hansestadt Hamburg Gebrauch gemacht. Für die Rundfunkanstalten und Religionsgemeinschaften⁴ existieren gesonderte Datenschutzbeauftragte, auf die hier nicht eingegangen wird. Die Landesbeauftragten sind für die Aufsicht über die Landesbehörden und im Regelfall auch für den nichtöffentlichen Bereich zuständig, also die Privatwirtschaft⁵.

1 Von Lewinski, Datenschutzaufsicht als Netzwerk in Europa, NVwZ 2017, 1483.

2 So bereits zur Richtlinie 95/46/EG Urteil des EuGH (Große Kammer) vom 9. März 2010, C-518/07, Kommission/Deutschland.

3 Vgl. § 9 Abs. 2 BDSG.

4 Dies ermöglichen Art. 85 und 91 DS-GVO.

5 In Bayern wurde entschieden, die Datenschutzaufsicht für den öffentlichen und nicht-öffentlichen Bereich auf zwei Behörden aufzuteilen.

Die Datenschutzaufsichtsbehörden unterstützen sich u. a. im Wege der Amtshilfe. Hierzu dürfen auch personenbezogene Daten übermittelt werden, §§ 16 Abs. 5 S. 2, 40 Abs. 3 S. 1 Hs. 2 BDSG. 11

Damit die deutschen Datenschutzaufsichtsbehörden das Recht gleich auslegen, existieren nationale Koordinierungsgremien, in denen datenschutzrechtliche Fragen diskutiert werden. Im Arbeitskreis Kreditwirtschaft, einem Arbeitskreis der Datenschutzkonferenz, tauschen sich die deutschen Aufsichtsbehörden zu datenschutzrechtlichen Fragen der Kreditwirtschaft aus. An diesen Treffen nehmen auch regelmäßig Vertreter der Kreditwirtschaft teil. 12

Darüber hinaus existiert die sogenannte zentrale Anlaufstelle beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Diese Stelle ist jedoch organisatorisch von diesem getrennt⁶. Sie ist die Anlaufstelle für Aufsichtsbehörden anderer Mitgliedsstaaten, den Europäischen Datenschutzausschuss und die Kommission⁷, um eine schnelle und reibungslose Zusammenarbeit mit den deutschen Aufsichtsbehörden zu gewährleisten. Durch die zentrale Anlaufstelle müssen außerhalb der Bundesrepublik Deutschland nicht die innerstaatlichen Zuständigkeiten bekannt sein. Auch die deutschen Aufsichtsbehörden können sich der zentralen Anlaufstelle bedienen, wenn sie mit den Aufsichtsbehörden oder europäischen Institutionen in Kontakt treten möchten⁸. 13

Der zentralen Anlaufstelle kommt folglich eine Unterstützungsfunktion zu und ist besonders bei den sog. Kohärenzverfahren von Bedeutung. Hoheitliche Befugnisse hat die zentrale Anlaufstelle nicht⁹. 14

2. EU

Auch auf EU-Ebene sind die Datenschutzaufsichtsbehörden der Mitgliedsstaaten miteinander vernetzt und koordinieren die Auslegung der DS-GVO. In Kapitel VII der DS-GVO (Art. 60 bis Art. 76 DS-GVO) sind die Zusammenarbeit und das Kohärenzverfahren geregelt. 15

Neben der Zusammenarbeit zwischen federführender und anderer betroffener Aufsichtsbehörde (Art. 60 DS-GVO) und der Amtshilfe (Art. 61 DS-GVO) gibt es die gemeinsamen Maßnahmen der Aufsichtsbehörden (Art. 62 16

⁶ BT-Drs. 18/11325, S. 90.

⁷ EG 119 der DS-GVO und § 17 Abs. 1 BDSG.

⁸ BT-Drs. 18/11325, S. 89.

⁹ BT-Drs. 18/11325, S. 89.

DS-GVO). Zu den gemeinsamen Maßnahmen gehören u. a. gemeinsame Untersuchungen und gemeinsame Durchsetzungsmaßnahmen.

- 17 In der Praxis ist wohl die Zusammenarbeit zwischen der federführender und anderen betroffenen Aufsichtsbehörden bei grenzüberschreitenden Sachverhalten gem. Art. 60 DS-GVO der häufigste Fall. Auf Grund des One-Stop-Shop-Prinzips ist die Behörde, an dem die Hauptniederlassung eines Unternehmens seinen Sitz hat, grundsätzlich die federführende Behörde. Betroffene Behörde ist die Aufsichtsbehörde bei der ggf. eine Niederlassung in einem anderen Mitgliedsstaat besteht oder an die sich ein Bürger wegen eines etwaigen Datenschutzverstoßes des Unternehmens wendet. Die federführende Aufsichtsbehörde koordiniert das Vorgehen gegen den Verantwortlichen. Können sich die federführende und die betroffene Aufsichtsbehörde auf ein Vorgehen einigen, so erlässt die federführende Aufsichtsbehörde den Entscheid gegenüber dem Unternehmen (Art. 60 Abs. 7 DS-GVO). Die Kommunikation mit der betroffenen Person obliegt der Behörde, an die sich der Bürger gewendet hat. Kommt es zu keiner Einigung, kommt es zum Kohärenzverfahren.
- 18 Das Kohärenzverfahren ist in Art. 63 ff. DS-GVO geregelt. Das Verfahren dient der einheitlichen Anwendung der DS-GVO in den Mitgliedsstaaten. Das Kohärenzverfahren wird durch den Europäischen Datenschutzausschuss durchgeführt. Mit Hilfe dieses Verfahrens sollen bei grenzüberschreitenden Sachverhalten widersprüchliche Entscheidungen der Datenschutzaufsichtsbehörden vermieden werden¹⁰.
- 19 Plant die zuständige Aufsichtsbehörde eine im Katalog des Art. 64 Abs. 1 S. 2 DS-GVO aufgeführte Entscheidung zu treffen, so ist der Entwurf des Beschlusses dem Europäischen Datenschutzausschuss zu übermitteln. Da eine entsprechende Entscheidung von allgemeiner Bedeutung sein kann, auch wenn kein grenzüberschreitender Bezug gegeben ist, gibt der Europäische Datenschutzausschuss eine entsprechende Stellungnahme ab. Der Europäische Datenschutzausschuss sieht von einer Stellungnahme ab, wenn er in einer solchen Angelegenheit bereits schon einmal eine Stellungnahme abgegeben hat (Art. 64 Abs. 3 DS-GVO).
- 20 Empfehlende Stellungnahmen gibt der Europäische Datenschutzausschuss auch ab, wenn er von der zuständigen Aufsichtsbehörde, der Kommission oder dem eigenen Vorsitzenden einen entsprechenden Antrag erhalten hat,

¹⁰ Selmayr/Ehmann, in: Ehmann/Selmayr (Hrsg.), DS-GVO, Einführung Rn. 71.

Art. 64 Abs. 2 DS-GVO. Es muss sich dann um eine Angelegenheit mit allgemeiner Geltung oder mit Auswirkung in einem Mitgliedsstaat handeln.

Stellungnahmen sind zwar nicht binden, aber werden sie nicht befolgt, so können sie Anlass für einen bindenden Beschluss sein, vgl. Art. 65 Abs. 1 lit. c DS-GVO. 21

Die bindenden Beschlüsse sind in Art. 65 DS-GVO geregelt. Sie sind ein Mittel der Streitbeilegung. Sie finden Anwendung, wenn sich die federführende und die betroffene Datenschutzaufsichtsbehörde nicht einigen können, unklar ist, welcher Aufsichtsbehörde die Federführung obliegt oder im Fall des Art. 64 Abs. 1 DS-GVO keine Stellungnahme eingeholt wurde oder die Aufsichtsbehörde der Stellungnahme nicht folgen möchte, Art. 65 Abs. 1 DS-GVO. 22

Das bisherige EU-weite Abstimmungsgremium zu datenschutzrechtlichen Fragestellungen Art.-29-Gruppe wurde am 25. Mai 2018 durch den Europäischen Datenschutzausschuss ersetzt. Der Europäische Datenschutzausschuss handelt unabhängig, Art. 69 DS-GVO. Seine Aufgaben sind in Art. 70 DS-GVO klar festgelegt. 23

Die Art.-29-Gruppe hatte lediglich beratende Funktion, der Europäische Datenschutzausschuss berät u. a. die Kommission und kann Leitlinien und Stellungnahmen veröffentlichen. Seine Beschlüsse sind gegenüber den mitgliedstaatlichen Aufsichtsbehörden verbindlich¹¹. Sie können vor dem EuGH angegriffen werden. 24

Regelungen zum Europäischen Datenschutzausschuss finden sich in den Art. 68 ff. DS-GVO. Er verfügt über eine eigene Rechtspersönlichkeit und besteht aus den Leitern der Datenschutzaufsichtsbehörden der Mitgliedsstaaten sowie dem Europäischen Datenschutzbeauftragten. Verfügt ein Mitgliedsstaat – wie Deutschland – über mehr als eine Datenschutzaufsichtsbehörde, so wird ein gemeinsamer Vertreter benannt. Für Deutschland ist dies der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit¹². Der Stellvertreter wird durch den Bundesrat aus dem Kreis der Landesdatenschutzbeauftragten gewählt¹³. Die Kommission kann an den Sitzungen und Tätigkeiten des Europäischen Datenschutzausschusses teilnehmen, verfügt jedoch nicht über ein Stimmrecht. Die Kommission wird über die Tätigkeiten des Europäischen Datenschutzausschuss durch dessen Vorsitzenden unterrichtet. 25

11 Albrecht, in: Ehmann/Selmayr (Hrsg.), DS-GVO, Art. 68 Rn. 1.

12 § 17 Abs. 1 S. 1 BDSG.

13 § 17 Abs. 1 S. 2 BDSG.

3. Zusammenarbeit mit anderen Staaten

- 26 Denkbar ist, dass an der Klärung eines Falles Aufsichtsbehörden in mehreren Mitgliedsstaaten zuständig sind. Grenzüberschreitende Fälle treten auf Grund von international tätigen Unternehmen vermehrt auf und erfordern eine Zusammenarbeit der Aufsichtsbehörden, da diese nur im Hoheitsgebiet ihres Mitgliedsstaates tätig werden können. Auch die Mobilität der Menschen und die Regelungen der DS-GVO tragen dazu bei, denn es ist möglich, dass sich eine betroffene Person bei einer Datenschutzaufsichtsbehörde beschwert, obwohl sich der Sachverhalt in einem anderen Mitgliedsstaat zugetragen hat. Die DS-GVO sieht eine Beschwerdemöglichkeit unabhängig vom Wohnsitz der betroffenen Person auch in einem anderen Mitgliedsstaat ausdrücklich vor. Eine Aufsichtsbehörde ist nach Art. 4 Nr. 22 DS-GVO immer betroffen, wenn der Verantwortliche oder Auftragsverarbeiter im Hoheitsgebiet dieser Aufsichtsbehörde niedergelassen ist, die Verarbeitung erhebliche Auswirkungen auf betroffenen Personen mit Wohnsitz im Mitgliedsstaat dieser Aufsichtsbehörde hat oder eine Beschwerde bei dieser Aufsichtsbehörde eingereicht wurde.
- 27 Für den Fall, dass mehrere Aufsichtsbehörden betroffen sind, ist grundsätzlich die Aufsichtsbehörde am Sitz der Hauptniederlassung des Verantwortlichen oder des Auftragsverarbeiters die federführende Aufsichtsbehörde¹⁴.
- 28 Die Aufsichtsbehörden arbeiten dann nach den Regelungen des Art. 60 DS-GVO zusammen und bemühen sich um eine konsensuale Entscheidungsfindung. Die betroffenen Aufsichtsbehörden leisten Amtshilfe¹⁵ und führen gemeinsame Maßnahmen¹⁶ durch. Die federführende Behörde teilt die ihr vorliegenden zweckdienlichen Informationen mit den betroffenen Behörden und erarbeitet einen Beschlussentwurf. Die betroffenen Behörden können zu diesem Entwurf Stellung nehmen. Die federführende Behörde trägt diesen Stellungnahmen gebührend Rechnung¹⁷. Die federführende Behörde setzt den Verantwortlichen oder Auftragsverarbeiter über die Entscheidung in Kenntnis, die Kommunikation mit der betroffenen Person bzw. dem Beschwerdeführer ist Aufgabe der beteiligten Aufsichtsbehörde¹⁸.

14 Nach dem One-Stop-Shop-Prinzip ist die Aufsichtsbehörde am Sitz des Unternehmens die zuständige Aufsichtsbehörde.

15 Art. 61 DS-GVO.

16 Art. 62 DS-GVO.

17 Art. 60 Abs. 3 DS-GVO.

18 Art. 60 Abs. 7, 8 DS-GVO.

Konnten sich die beteiligten Aufsichtsbehörden nicht einigen, leitet die federführende Aufsichtsbehörde das Kohärenzverfahren ein¹⁹. Der Europäische Datenschutzausschuss entscheidet darin mittels eines verbindlichen Entschlusses den Streit zwischen den Aufsichtsbehörden²⁰. Dieser Entschluss liegt dann der Entscheidung zu Grunde, die die Aufsichtsbehörden treffen und dem Verantwortlichen/Auftragsverarbeiter und Beschwerdeführer gegenüber bekanntgeben. Die Entscheidung des Europäischen Datenschutzausschusses wird publiziert.

4. Aufgaben und Befugnisse der Aufsichtsbehörden

Art. 57 DS-GVO enthält einen Katalog an Aufgaben, für die die Datenschutzaufsichtsbehörden zuständig sind. Sie können in Untersuchungs-, Abhilfe-, Genehmigungsaufgaben und Beratung sowie etwaige Aufgaben nach nationalem Recht²¹ unterteilt werden. Darüber hinaus haben die unabhängigen Aufsichtsbehörden auch die Aufgabe, die DS-GVO einheitlich anzuwenden, Art. 51 Abs. 2 DS-GVO.

Für betroffene Personen und für Datenschutzbeauftragte ist das Tätigkeitwerden der Datenschutzaufsichtsbehörde grds. kostenlos. Gebühren dürfen nur bei offenkundig unbegründeten oder exzessiven Anfragen erhoben werden, Art. 57 Abs. 4 S. 1 DS-GVO. Unternehmen können sich von ihrer zuständigen Aufsichtsbehörde ebenfalls beraten lassen.

Aus den Aufgaben lassen sich entsprechende Befugnisse ableiten. Diese sind in Art. 58 DS-GVO festgelegt. Neben den Untersuchungs-, Abhilfe- und Genehmigungsbefugnissen kommt den Aufsichtsbehörden auch die Möglichkeit zu, gegen Entscheidungen der Kommission und des EDSA zu klagen.

In der Praxis von Bedeutung ist für das einzelne Institut sind die Möglichkeiten der Datenschutzaufsichtsbehörde der Möglichkeit der Durchführung von Kontrollen, wobei der Aufsichtsbehörde Zutritt zu sämtlichen Räumen zu gewähren ist und Informationen bereitzustellen sind. Darüber hinaus sind in der Praxis auch die Abhilfebefugnisse der Aufsichtsbehörden von großem Interesse, wie etwa die Verwarnung, die Anordnung, das Verhängen von Bußgeldern sowie die Untersagung von Datenverarbeitungen und Datentransfers in Drittstaaten, Art. 58 Abs. 2 DS-GVO.

¹⁹ Art. 60 Abs. 4 DS-GVO.

²⁰ Art. 65 Abs. 2 DS-GVO.

²¹ Bei diesen Vorschriften handelt es sich um die Umsetzung von Art. 46 DSRL-JI.

III. Datenschutzkontrollen und Zertifizierungen

- 34 Kontrollen sind eine effektive Möglichkeit, um die Einhaltung datenschutzrechtlicher Vorgaben und Empfehlungen zu überprüfen. Sie ermöglichen die Begutachtung wie der Datenschutz vor Ort gelebt und umgesetzt wird. Darüber hinaus geben die Aufsichtsbehörden bei Kontrollen Hinweise zu gesetzlichen Neuerungen und sprechen Best-Practice-Empfehlungen aus. Der Besuch der Aufsichtsbehörde gibt auch Raum für die Klärung von Fragen des Verantwortlichen. Fragen beantworten die Datenschutzaufsichtsbehörden auch außerhalb von Prüfungen, es ist der gesetzliche Auftrag an die Aufsichtsbehörden beratend tätig zu sein.
- 35 Denkbar ist, dass ein Verantwortlicher ein Verarbeitungsverfahren nach Art. 42 DS-GVO zertifizieren lässt. Die Zertifizierung dient dem Nachweis der Einhaltung datenschutzrechtlicher Vorschriften. Zertifizierungen haben einen präventiven Charakter²². Es handelt sich hierbei um eine freiwillige Überprüfung und erfolgt in einem transparenten Verfahren²³. Die Datenschutzaufsichtsbehörden sind nicht durch die Zertifizierung gebunden, auch wenn sie diese fördern. Die Zertifizierung gilt für drei Jahre und kann verlängert sowie widerrufen werden²⁴. Trotz Zertifizierung besteht die Verantwortung für den Verarbeitungsprozess weiterhin²⁵. Die Zertifizierung ist nur durch eine akkreditierte Stelle möglich²⁶. Für Verantwortliche außerhalb der EU eignet sich die Zertifizierung zum Nachweis eines angemessenen Datenschutzniveaus²⁷. Die erteilten Zertifizierungsverfahren werden in ein Register beim Europäischen Datenschutzausschuss aufgenommen und in geeigneter Weise veröffentlicht²⁸.

22 Will, in: Ehmann/Selmayr, DS-GVO, Art. 42 Rn. 2.

23 Art. 42 Abs. 3 DS-GVO.

24 Art. 43 Abs. 7 DS-GVO.

25 Art. 42 Abs. 4 DS-GVO.

26 Vgl. Art. 43 DS-GVO.

27 Vgl. Art. 46 Abs. 1 lit. f DS-GVO.

28 Art. 42 Abs. 8 DS-GVO.