

Inhaltsübersicht

Vorwort	IX
Inhaltsverzeichnis	XV
Abkürzungsverzeichnis	XXVII
Herausforderungen der datenschutzrechtlichen Compliance im Unternehmen	1
Kapitel 1: Datenschutz-Managementsysteme	5
A. Begriffsannäherung	6
I. Kodifizierungen in Landesregelungen.	7
1. Datenschutzverordnung Schleswig-Holstein	7
2. Bremische Datenschutzauditverordnung	10
II. Aufsichtsbehördliche Modellierung	11
III. Praktische Standards	14
1. BSI-Standards	15
2. ISO-Normenreihe	16
3. VdS-Richtlinien.	19
IV. Rezeption im datenschutzrechtlichen Schrifttum	20
V. Parallelen zu Compliance-Managementsystemen.	23
B. Konkretisierung des Begriffs	26
I. Einordnung des Datenschutz-Managements	26
1. Einbezug betriebswirtschaftlicher Kalküle	27
2. Übertragung auf das Datenschutz-Management	29
3. Erweiterung zum Datenschutz-Compliance-Management.	29
II. Datenschutz-Managementsysteme	30
1. Abgrenzung zum Datenschutz-Compliance-Management.	30
2. Wesensmerkmale des Datenschutz-Managementsystems	32
3. Funktionen des Datenschutz-Managementsystems.	35
C. Definitionsvorschläge	37
Kapitel 2: Datenschutzrechtliche Einrichtungspflichten	38
A. Datenschutzrechtliche Auslegungsgrundsätze	39
I. Normative Determinanten der Auslegung	39
1. Unionsrechtliche Verortung des Datenschutzrechts	39
2. Unmittelbarkeit und Vorrang der DSGVO	42
3. Zusammenwirken im Mehrebenensystem.	44
II. Auslegungsprinzipien	45
1. Unionsrechtliche Methode des Gerichtshofs	45

2. Auslegung durch die mitgliedstaatlichen Gerichte	55
3. Interpretationen der Aufsichtsbehörden	59
III. Folgen für die Auslegung datenschutzrechtlicher Einrichtungs- pflichten	60
B. Unmittelbare Einrichtungspflicht.	63
I. Risikoorientierung der organisatorischen Kardinalpflichten.	63
1. Zweck des risikobasierten Ansatzes	64
2. Begriffliche Einordnung des Risikos der Verarbeitung.	65
3. Risikobeurteilung	75
4. Risikoanalyse und -festlegung	82
5. Bedeutung für die Untersuchung von Einrichtungs- pflichten.	83
II. Kardinalpflichten zur Einhaltung und Sicherstellung der Datenschutz-Compliance.	84
1. Rechenschaftspflicht	84
2. Allgemeine Sicherstellungspflicht	102
3. Zwischenergebnis	129
III. Kardinalpflicht zur rechtskonformen Gestaltung der Ver- arbeitung	131
1. Datenschutz durch Gestaltung.	131
2. Datenschutz durch datenschutzfreundliche Voreinstellun- gen.	153
3. Beurteilung einer Einrichtungspflicht.	159
4. Zwischenergebnis	162
IV. Kardinalpflicht zur Sicherheit der Verarbeitung	163
1. Funktion	164
2. Sicherheitsmaßnahmen	168
3. Verhältnis zu den anderen Kardinalpflichten	179
4. Beurteilung einer Einrichtungspflicht.	182
5. Zwischenergebnis	187
V. Würdigung der unmittelbaren Einrichtungspflicht	188
C. Abgeleitete Einrichtungspflicht.	190
I. Einzelpflichten.	190
1. Verzeichnis von Verarbeitungstätigkeiten.	191
2. Datenschutz-Folgenabschätzung.	204
3. Data Breach Notifications.	237
4. Zwischenergebnis	278
II. Pflichtenkomplexe.	279
1. Sicherstellung der Rechtmäßigkeit der Verarbeitung	280
2. Pflichten gegenüber betroffenen Personen	300
3. Zwischenergebnis	317
III. Würdigung der abgeleiteten Einrichtungspflicht.	318

D. Konsequenzen für das Bestehen datenschutzrechtlicher Ein- richtungspflichten.	319
Kapitel 3: Kriterien zur Bestimmung der Einrichtungspflicht . . .	322
A. Risiken der Verarbeitung	323
I. Risikofaktoren	324
II. Risikoniveau	324
III. Abhängigkeit von der Verarbeitung.	325
B. Verarbeitungsrahmen beim Verantwortlichen	326
I. Parameter der Verarbeitung	326
1. Art der Verarbeitung	327
2. Umfang der Verarbeitung	328
3. Umstände der Verarbeitung	329
4. Zwecke der Verarbeitung	331
II. Präzisierte Verarbeitungskriterien	332
1. Verarbeitungsumstände	332
2. Organisationsumstände	342
C. Wirtschaftliche und technische Erwägungen	352
I. Einrichtungskosten und wirtschaftliche Leistungsfähigkeit . .	352
II. Stand der Technik	354
D. Erkenntnisse	355
Kapitel 4: Schlussbetrachtung	357
Literatur	360
Webverzeichnis.	393