

# Inhaltsverzeichnis

Vorwort des Herausgebers .....	V
Geleitwort .....	VII
Abkürzungsverzeichnis .....	XIII
Verzeichnis der (abgekürzt) zitierten Literatur .....	XVII

## Kapitel 1. Einleitung

A. Zielsetzung und Handhabung der Checklisten .....	1
I. Ziele und Genese der DS-GVO .....	1
II. Die DS-GVO als EU-Verordnung .....	3
III. Öffnungsklauseln – Nationales Datenschutzrecht (BDSG) .....	3
IV. ePrivacy-Richtlinie .....	3
B. Die Auslegung der DS-GVO .....	4
C. Anwendbarkeit der DS-GVO .....	5

## Kapitel 2. Accountability: die Rechenschaftspflicht

A. Einführung .....	7
B. Erläuterungen zur Checkliste .....	7
I. Das Prinzip der Accountability .....	7
1. Explizite Verpflichtung zu Rechenschaft und Nachweis in Art. 5 DS-GVO und Art. 24 DS-GVO .....	7
2. Accountability als übergreifendes Prinzip der DS-GVO im Kontext von Managementprozessen .....	8
3. Accountability bezüglich der einzelnen Datenschutzgrundsätze gem. Art. 5 DS-GVO .....	9
II. Sicherstellung der Einhaltung der DS-GVO .....	11
1. Grundlagen der Sicherstellung .....	11
2. Vornahme geeigneter technischer und organisatorischer Maßnahmen (TOMs) und Datenschutzvorkehrungen .....	12
3. Risikobasierter Ansatz: Angemessenheit der Maßnahme .....	13
4. Komponenten der Konzeptionierung („Plan“) .....	14
5. Komponenten der Umsetzung („Do“) .....	18
III. Nachweis der Sicherstellung der Einhaltung der DS-GVO .....	20
1. Grundlagen zur Nachweispflicht .....	20
2. Risikobasierter Ansatz: Umfang der Nachweispflicht .....	21
3. Komponenten des Nachweises .....	21
IV. Überprüfungspflicht und Anpassung .....	23
1. Grundlagen der kontinuierlichen Verbesserung .....	23
2. Komponenten von Überprüfungspflicht und Anpassung („Check“ und „Act“) .....	25
V. Datenschutzmanagement und Datenschutzorganisation .....	29
1. Pflicht, ein Datenschutzmanagement zu etablieren und zu unterhalten .....	29
2. Elemente eines Datenschutzmanagements und die Datenschutzorganisation .....	30
3. Komponenten entlang der 7 Elemente des Datenschutzmanagements nach IDW PS 980 .....	32
VI. Die Bestellung eines Datenschutzbeauftragten .....	35
1. Element der Accountability .....	35

2. Pflicht zur Bestellung des DSB .....	35
3. Materielle Anforderungen an die Bestellung des DSB .....	36
4. Anforderungen an den Status des DSB gem. Art. 38 DS-GVO .....	37
5. Die Aufgaben des DSB .....	39

### **Kapitel 3. Der Kernprozess des Datenschutzes – neue Verarbeitungen erfassen, bewerten und überwachen**

A. Einführung .....	41
B. Erläuterungen zur Checkliste .....	41
I. Rechenschaftspflicht (Accountability) und Datenschutz-Kernprozess .....	41
1. Die allgemeinen Anforderungen an die Implementierung .....	41
2. Anforderungen an einen Prozess, der sicherstellt, dass neue datenschutzrelevante Verarbeitungen und Projekte erfasst und bewertet werden .....	42
II. Das Verarbeitungsverzeichnis als Kernstück der Datenschutz-Compliance .....	43
1. Die Funktion des Verarbeitungsverzeichnisses .....	43
2. Das Verarbeitungsverzeichnis des Verantwortlichen .....	43
3. Das Verarbeitungsverzeichnis des Auftragsverarbeiters (Art. 32 Abs. 2 DS-GVO) .....	48
4. Weitere Anforderungen an das Verarbeitungsverzeichnis .....	50
III. Die Datenschutz-Folgenabschätzung .....	51
1. Wird für jede (neue) Verarbeitung anhand geeigneter Kriterien geprüft, ob ein hohes Risiko gegeben ist, das zur Datenschutz-Folgenabschätzung verpflichtet? .....	51
2. Durchführung, Dokumentation und Methodik der Datenschutz-Folgenabschätzung .....	59
3. Einbindung von weiteren Akteuren und betroffenen Personen .....	61
4. Konsultation der Aufsichtsbehörde nach Art. 36 DS-GVO .....	62
5. Auditierung und Wirksamkeitsprüfung (Art. 35 Abs. 9 DS-GVO) .....	63
IV. Privacy by Design and by Default – Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DS-GVO) .....	63
1. Grundlagen von Privacy by Design and Default .....	64
2. Privacy by Design (Art. 25 Abs. 1 DS-GVO) .....	64
3. Privacy by Default (Art. 25 Abs. 2 DS-GVO) .....	69
4. Zertifizierung von Privacy by Design und by Default .....	70

### **Kapitel 4. Rechtfertigung und Rechtmäßigkeit der Verarbeitung personenbezogener Daten**

A. Einführung .....	73
B. Erläuterungen zur Checkliste .....	74
I. Rechtfertigung einer Verarbeitung personenbezogener Daten .....	74
1. Rechtfertigung durch Einwilligung (Art. 6 Abs. 1 Buchst. a DS-GVO) .....	74
2. Rechtfertigung durch Vertragsabschluss und Vertragserfüllung (Art. 6 Abs. 1 Buchst. b DS-GVO) .....	81
3. Rechtfertigung durch Erfüllung einer rechtlichen Verpflichtung (Art. 6 Abs. 1 Buchst. c DS-GVO) .....	82
4. Rechtfertigung bei Verarbeitung personenbezogener Daten zum Schutz lebenswichtiger Interessen (Art. 6 Abs. 1 Buchst. d DS-GVO) .....	83
5. Rechtfertigung bei Verarbeitung personenbezogener Daten zur Wahrnehmung einer Aufgabe im öffentlichen Interesse oder zur Ausübung öffentlicher Gewalt (Art. 6 Abs. 1 Buchst. e DS-GVO) .....	83

6. Rechtfertigung aufgrund von berechtigten Interessen (Art. 6 Abs. 1 Buchst. f DS-GVO) .....	83
7. Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 Abs. 1 DS-GVO) .....	84
8. Personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten (Art. 10 DS-GVO) .....	86
II. Weitere Anforderungen an eine Verarbeitung personenbezogener Daten .....	88
1. Allgemeines .....	88
2. Die Grundsätze für die Verarbeitung personenbezogener Daten (Art. 5 Abs. 1 DS-GVO) .....	88

### **Kapitel 5. Die Information der betroffenen Personen**

A. Einführung .....	95
B. Erläuterungen zur Checkliste .....	96
I. Vorüberlegungen .....	96
1. Gesetzliche Verantwortlichkeit für die Erteilung der Informationen nach Art. 13 DS-GVO und/oder Art. 14 DS-GVO .....	96
2. Durchführungsverantwortlichkeit für die Erteilung der Informationen nach Art. 13 DS-GVO und/oder Art. 14 DS-GVO im konkreten Fall .....	97
3. Ausnahmen von der Verpflichtung zur (konkreten) Informationserteilung an die betroffene Person .....	98
II. Ausgestaltung der Information der betroffenen Personen .....	108
1. Pflichtinhalte .....	108
2. Anforderungen an die Formulierung und Strukturierung der Pflichtinhalte .....	125
III. Anforderungen an die Implementierung .....	131
1. Zeitpunkt der Erteilung der Datenschutzinformationen .....	131
2. Darreichungsform der Datenschutzinformationen .....	134

### **Kapitel 6. Auskunft**

A. Einführung .....	137
B. Erläuterungen zur Checkliste .....	138
I. Organisatorische Anforderungen für die Auskunft .....	138
II. Formelle Anforderungen an die Antwort auf einen Antrag auf Auskunft .....	142
1. Form der Beantwortung .....	144
2. Kosten der Auskunft .....	144
III. Materielle Anforderungen an die Auskunft .....	145
1. Erste Stufe des Auskunftersuchens – Positiv oder Negativtest .....	145
2. Zweite Stufe – Beantwortung des Auskunftersuchens .....	145
3. Recht auf eine Kopie der Daten .....	152
IV. Grenzen der Auskunft .....	152

### **Kapitel 7. Sonstige Betroffenenrechte**

A. Einführung .....	155
B. Erläuterungen zur Checkliste .....	155
I. Recht auf Berichtigung .....	155
II. Recht auf Datenübertragbarkeit .....	161

### **Kapitel 8. Löschen von Daten**

A. Einführung .....	171
---------------------	-----

B. Erläuterungen zur Checkliste .....	171
I. Speicherbegrenzung – Regelmäßiges Löschen .....	171
II. Das Betroffenenrecht auf Löschen und das Recht auf Vergessenwerden .....	180

### **Kapitel 9. Datensicherheit sowie technische und organisatorische Maßnahmen**

A. Einführung .....	187
B. Erläuterungen zur Checkliste .....	187
I. Datensicherheit nach Art. 32 DS-GVO .....	187
1. Allgemeines .....	187
2. Liegt eine Datensicherheitskonzeption vor? .....	193
3. Berechtigung – „Need-to-Know-Prinzip“ .....	195
II. Praxishinweise für die Umsetzung .....	196

### **Kapitel 10. Meldungen und Benachrichtigung von Sicherheitsvorfällen**

A. Einführung .....	199
B. Erläuterungen zur Checkliste .....	199
I. Organisationspflichten des Verantwortlichen (Rechenschaftspflicht und Implementierung) .....	199
1. Allgemeine Anforderungen an die Implementierung .....	200
2. Risikoprognose .....	203
3. Besondere Anforderungen an die Implementierung .....	206
4. Dokumentationspflichten des Verantwortlichen nach Art. 33 Abs. 5 DS-GVO .....	209
II. Ausschlussstatbestände für die Benachrichtigung von betroffenen Personen (Art. 34 Abs. 3 DS-GVO) .....	210

### **Kapitel 11. Auftragsverarbeitung und gemeinsame Verantwortlichkeit**

A. Einführung .....	213
B. Erläuterungen zur Checkliste .....	214
I. Auftragsverarbeitung .....	214
1. Vorliegen einer Auftragsverarbeitung .....	215
2. (Vertrags-)Rechtliche Bindung des Auftragsverarbeiters in Bezug auf den Verantwortlichen .....	217
3. Implementierung von Kontroll- und Steuerungsmechanismen .....	232
II. Gemeinsame Verantwortlichkeit .....	236
1. Vorliegen einer gemeinsamen Verantwortlichkeit .....	237
2. Vereinbarung über die gemeinsame Verantwortlichkeit .....	240
3. Anforderungen an die Implementierung .....	247

### **Kapitel 12. Drittlandtransfers**

A. Einführung .....	249
B. Erläuterungen zur Checkliste .....	249
I. Vorliegen eines Drittlandtransfers .....	249
II. Zulässigkeit eines Drittlandtransfers .....	251

<b>Stichwortverzeichnis .....</b>	<b>263</b>
-----------------------------------	------------