
Inhaltsverzeichnis

Vorwort	V
Literaturverzeichnis	XI
Abkürzungsverzeichnis	XXI
Zum Autor	XXV
NATIONAL	1
1. Verantwortung	3
1.1. Entscheidung über Zweck und Mittel	3
1.2. Abgrenzung und Beispiele	7
1.3. Art, Umfang, Umstände, Zwecke	10
1.4. Nachweis und Vertragsrecht	13
1.5. Haftung und Schadenersatz	16
1.6. Sanktionen/Geldbußen	19
2. Gemeinsame Verantwortung – „Joint Controllership“	21
2.1. Allgemein	21
2.2. Stellungnahme WP 169 & Guidelines EDPB	26
2.3. Abgrenzung und Beispiele	27
2.4. Judikatur	32
2.4.1. EuGH „Facebook-Fanpages“	32
2.4.2. EuGH „Zeugen Jehovas“	35
2.4.3. EuGH „Fashion ID“	35
2.4.4. CNIL „UBER“	37
2.4.5. EuGH „Covid-App Litauen“ inkl Checkliste zur gemeinsamen Verantwortung	37
2.4.6. EuGH „IAB Europe“	39
2.5. Vertrag zwischen gemeinsam Verantwortlichen (VGV) – Joint Controller Agreement – wichtige Vertragsklauseln	40
2.5.1. Vertragsgegenstand – gemeinsame Verantwortung	40
2.5.2. Art, Zweck und Ort der Datenverarbeitung	41
2.5.3. Zuordnung der Verantwortlichkeiten	42
2.5.4. Gesamtschuld/Haftung	45
2.5.5. Anlaufstelle	46
2.5.6. Sicherheit der Verarbeitung	46
2.5.7. Data Breach Notification Duty	47
2.5.8. Dauer der Vereinbarung	49
2.5.9. Vorrangregelung	50
2.5.10. Auftragsverarbeiter im Rahmen des VGV	50
2.6. Zurverfügungstellung	51
2.7. Gemeinsame Verantwortung und DSFA	52
2.8. Gemeinsame Verantwortung und Aufsichtsbehörden	53
2.9. Sanktionen	54
2.10. Muster Joint Controller Agreement	55

3. Auftragsverarbeitung	63
3.1. Allgemein	63
3.2. Stellungnahme WP 169 & Guidelines EDPB	66
3.3. Abgrenzung und Beispiele	68
3.4. Sonderfall Wartungsverträge	75
3.4.1. Meinung 1: Auftragsverarbeitungsvertrag notwendig	75
3.4.2. Meinung 2: Kein Auftragsverarbeitungsvertrag notwendig	76
3.4.3. Schlussfolgerung – eigene Wertung	77
3.5. Eigene datenschutzrechtliche Pflichten	79
3.6. Auftragsverarbeitervertrag (AVV) – wichtige Vertragsklauseln	80
3.6.1. Allgemein	80
3.6.2. Vertrag oder Standardvertragsklauseln	80
3.6.2.1. Ergänzung/Änderungen SCC	81
3.6.2.2. Individueller Vertrag	81
3.6.3. Kernelemente	83
3.6.4. Dokumentierte Weisungen	85
3.6.5. Geheimhaltungsverpflichtung	87
3.6.6. Maßnahmen zur Sicherheit der Verarbeitung	88
3.6.7. Weitere Auftragsverarbeiter	89
3.6.8. Unterstützung und Zusammenarbeit	94
3.6.9. Data Breach Notification Duty	97
3.6.10. Löschung oder Herausgabe	100
3.6.11. Kontrollrechte des Verantwortlichen (Entgelt), Audit	102
3.6.12. Haftung, Freistellung und Vertragsstrafe (Pönale)	106
3.6.12.1. Haftungsklausel	106
3.6.12.2. Freistellung, Schad-/Klagelohaltung	107
3.6.12.3. Vertragsstrafe (Pönale)	108
3.6.13. Vorrangregelung	109
3.6.14. Dauer der Vereinbarung	110
3.6.15. Weiterverarbeitung durch Auftragsverarbeiter	111
3.7. Vertrag und elektronisches Format	113
3.8. Vertrag oder anderes Rechtsinstrument	114
3.8.1. Ausgangslage	114
3.8.2. Europäischer Datenschutzausschuss (EDSA – EDPB)	115
3.8.3. Meinungsstand in der Literatur	115
3.8.4. Eigene Wertung	116
3.8.5. Umsetzung	116
3.8.6. Gesetzlich angeordnete Auftragsverarbeitung und Vertrag	117
3.9. Vertrag und AGB	118
3.10. Sanktionen	119
3.11. Verhaltensregeln/Zertifizierungen Auftragsverarbeiter	121
3.12. Standardvertragsklauseln Auftragsverarbeiter	122

4. Mehrere Verantwortliche – alleinige Verantwortung	137
4.1. Allgemein	137
4.2. Abgrenzung und Beispiele	138
4.3. Vertrag zwischen allein Verantwortlichen – Controller-to-Controller Agreement – wichtige Vertragsklauseln	139
4.3.1. Allgemein	139
4.3.2. Vertragsklausel KI & Algorithmen	140
5. Fallbeispiele National	141
INTERNATIONAL	149
6. Internationaler Datenverkehr – Art 44 ff DSGVO	151
6.1. Allgemein	151
6.2. Angemessenheitsbeschlüsse	152
6.3. Standarddatenschutzklauseln & alternative Rechtsgrundlagen	153
6.4. Sanktionen bei Verletzung der Art 44 ff DSGVO	155
6.5. EuGH „Schrems II“	155
6.5.1. Die Entscheidung des EuGH zum Privacy Shield	155
6.5.2. Unmittelbare To-dos aufgrund des EuGH-Urteils	157
6.6. Angemessenheitsbeschluss USA – EU-US Data Privacy Framework	158
6.6.1. Einleitung/Vorgeschichte	158
6.6.2. EU-US Data Privacy Framework (DPF)	158
6.6.3. Angemessenheitsbeschluss USA	159
6.6.4. Auswirkungen für die Praxis	160
6.7. Accountability beim Transfer in Drittländer	161
6.7.1. Allgemein	161
6.7.2. Transfer Impact Assessment (TIA)	164
6.7.2.1. SCC	165
6.7.2.2. Empfehlungen EDPB	168
6.7.2.2.1. Rechtslage	169
6.7.2.2.2. Praxis (Gepflogenheiten)	169
6.7.2.2.3. Bericht & Informationsquellen	171
6.7.2.2.4. Ergebnis	172
6.8. Supplementary Measures – zusätzliche Vertragsbestimmungen	172
6.8.1. Die Vorschläge des EDPB	173
6.8.2. Die Vorschläge des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg	178
6.8.3. Die Vertragsklauseln von Microsoft	180
6.9. Standardvertragsklauseln Drittländer	183
6.9.1. Allgemein	183
6.9.2. Onward Transfer	186
6.9.3. Modul 4	186
6.9.4. Löschen und Anonymisieren	187
6.9.5. Durchführungsbeschluss (EU) 2021/914	188
6.9.6. Standardvertragsklauseln MODUL EINS: Verantwortlicher an Verantwortliche	228

Inhaltsverzeichnis

6.9.7. Standardvertragsklauseln MODUL ZWEI: Verantwortlicher an Auftragsverarbeiter	245
6.9.8. Standardvertragsklauseln MODUL DREI: Auftragsverarbeiter an Auftragsverarbeiter	262
6.9.9. Standardvertragsklauseln MODUL VIER: Auftragsverarbeiter an Verantwortliche	280
6.10. Fallbeispiele International	291
6.10.1. EDPB – Drittlandtransfer	291
6.10.2. Europäische Kommission – SCC Module & Anwendung	296
Stichwortverzeichnis	301

Das Streben nach Klarheit und Lesbarkeit veranlasst uns dazu, im Text auf die gleichberechtigte Nennung aller Geschlechter zu verzichten. Sämtliche personenbezogene Hauptwörter beziehen sich gleichermaßen auf die Entsprechungen anderer Geschlechter.