

# Inhaltsverzeichnis

<b>Zur Verwendung dieses Buchs .....</b>	<b>V</b>
<b>Für alle .....</b>	<b>VII</b>
<b>Grußwort von Dr. Stefan Brink .....</b>	<b>XI</b>
<b>Grußwort von Frederick Richter .....</b>	<b>XIII</b>
<b>Grußwort von Michael Will .....</b>	<b>XV</b>
<b>Abkürzungsverzeichnis .....</b>	<b>XXVII</b>
<b>1. Kapitel: Überblick über die zentralen Themen .....</b>	<b>1</b>
1.1 Einführung .....	1
1.2 Datenschutzrechtlicher Rahmen .....	2
1.3 Datenschutzrechtliche Risiken .....	2
1.4 Markt und Alternativen zu Microsoft 365 .....	4
1.5 Entscheidung der Geschäftsleitung und Business Judgment Rule .....	5
1.6 Maßnahmen zur Risikominimierung .....	6
<b>2. Kapitel: Herangehensweise und Prüfungs- umfang beim Microsoft 365-Projekt .....</b>	<b>7</b>
2.1 Projektmanagement zum Datenschutz bei der Microsoft 365-Migration .....	7
2.2 Eingrenzung der Themen: In Scope/Out of Scope .....	8
2.3 Datenklassifizierung zur Bewertung „Out of Scope“ .....	10
2.4 Umgang mit ausgegrenzten Themen .....	12
<b>3. Kapitel: Risiken beim Einsatz von Microsoft 365, insb. aus Sicht der Aufsichtsbehörden .....</b>	<b>13</b>
3.1 Grundsätze der DSGVO und Problemfelder bei SaaS .....	13
3.1.1 Rechtmäßigkeit der Datenverarbeitung (Art. 5 Abs. 1 lit. a DSGVO) .....	13
3.1.2 Transparenz der Datenverarbeitung (Art. 5 Abs. 1 lit. a DSGVO) .....	14
3.1.3 Erforderlichkeit der Datenverarbeitung (Art. 5 Abs. 1 lit. c DSGVO) .....	14
3.1.4 Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f, Art. 32 Abs. 1 lit. a DSGVO) .....	15
3.1.5 Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) .....	15
3.2 DSK & Co.: Struktur und Relevanz der Datenschutzaufsicht in EU und DE .....	15

XVII

## Inhaltsverzeichnis

3.2.1	Aufbau der Datenschutzaufsicht in der EU: EDSA und EDSB .....	16
3.2.2	Aufbau der Datenschutzaufsicht in Deutschland: Zahlreiche Aufsichtsbehörden .....	17
3.2.3	Datenschutzkonferenz (DSK), „Berlin Group“ und weitere inoffizielle Gruppierungen .....	18
3.2.4	Rechtliche Natur der Aufsichtsbehörden in der Gewaltenteilung .....	20
3.2.5	Zusammenfassung zu Aufsichtsbehörden und ihren nicht-behördlichen Gruppen .....	21
3.3	Darstellung der Auffassung der Aufsichtsbehörden .....	22
3.3.1	Beschluss der Art.-29-Datenschutzgruppe zum Microsoft Online Services DPA (2014) .....	22
3.3.2	Der DSK-Beschluss aus 2020 .....	23
3.3.3	Der DSK-Beschluss aus 2022 .....	24
3.3.3.1	Kritikpunkte der DSK in der beschlossenen „Festlegung“ (2022) .....	25
3.3.3.2	Weitere Kritikpunkte der DSK in der „Zusammenfassung“ (2022) .....	26
3.3.4	Stellungnahme des LfDI BW zu M365 an Schulen (2022) .....	27
3.3.5	„Praxis-Tipps“: Handreichung einiger Aufsichtsbehörden (8-9/2023) .....	28
3.3.5.1	Herausgeber/Beteiligte Behörden .....	29
3.3.5.2	Inhalt und Reaktionen .....	30
3.3.5.3	Spezifizierung der Daten und betroffenen Personen .....	31
3.3.5.4	Nutzung von E-Mail-Adressen ohne Namen .....	31
3.3.6	LfD Niedersachsen: Einsatz von Teams im Innenministerium ist akzeptabel .....	32
3.3.6.1	Hintergrund .....	32
3.3.6.2	Die niedersächsische „Zusatzvereinbarung“ .....	32
3.3.6.3	Bewertung des LfD Niedersachsen als akzeptabel .....	33
3.3.7	Weitere Stellungnahmen deutscher Aufsichtsbehörden .....	34
3.3.8	Verfahren des EDSB gegen die EU-Kommission und darauffolgende Klagen .....	35
3.3.8.1	Hintergrund: Rechtlicher Rahmen und Rolle des EDSB .....	36
3.3.8.2	Kritik des EDSB an Microsoft 365 .....	37
3.3.8.3	Entgegnung und Relevanz für den derzeitigen Einsatz von M365 .....	38

3.3.8.4	Klage der EU-Kommission und von Microsoft Irland gegen den Beschluss des EDSB .....	40
3.3.8.5	Antwort der EU-Kommission und Pressemitteilung des EDSB vom Dezember 2024 .....	40
3.3.8.6	Zusammenfassung und Bedeutung für die Praxis .....	40
3.3.8.7	Inhalt der Klagen von Kommission und Microsoft gegen den EDSB .....	42
3.3.9	Positionen zu Videokonferenzen und Abgrenzung zum Telekommunikationsrecht .....	44
3.3.9.1	Überblick über die aufsichtsbehördlichen Stellungnahmen .....	44
3.3.9.2	Komplexität und Heterogenität der Anforderungen .....	46
3.3.9.3	Beispiel: End-to-End-Verschlüsselung .....	47
3.3.9.4	Einheitlicher Bewertungsmaßstab oder zweierlei Maß? .....	49
3.3.9.5	Behördenauffassungen betr. Abgrenzung zur Telekommunikation .....	50
3.3.9.6	Bewertung und weitere Differenzierung: Connected Experiences, Exchange .....	53
3.3.9.7	Folgen falscher Abgrenzung; Zuständigkeit .....	54
3.4	Kritik in der rechtswissenschaftlichen Literatur .....	55
3.5	Weitere mögliche Kritikpunkte .....	56
3.6	Zusammenfassung des Spektrums von Meinungen und Freigaben .....	57
3.7	Ergebnis .....	58
<b>4.</b>	<b>Kapitel: Argumentationslinien für einen Einsatz von Microsoft 365 .....</b>	<b>59</b>
4.1	Überblick über den Rechtsrahmen von Verfassungen und Datenschutzrecht .....	59
4.1.1	Datenschutz-Basics: Verfassungen, Primärrecht und EU-Grundrechte-Charta .....	59
4.1.2	Relevanz von Erwägungsgründen .....	60
4.1.3	DSGVO als Sekundärrecht unter der EU-GRCh .....	61
4.1.4	Weitere, insb. nationale Normen .....	62
4.1.5	Zusammenfassung .....	62
4.2	Überblick über das Vertragswerk zu Microsoft 365 .....	63
4.2.1	Product Terms als Rahmen einzelner Dokumente .....	63
4.2.2	Privacy & Security Terms: Definition der Core Services und EU Data Boundary .....	64

## Inhaltsverzeichnis

4.2.3	Das Data Protection Addendum .....	66
4.2.3.1	Übersicht zum Data Protection Addendum ..	67
4.2.3.2	Data Protection Addendum: Vertragspartner, Lizenzen und Abschluss .....	68
4.2.3.3	Data Protection Addendum: Neue Versionen und Aktualisierung bei Bestandskunden....	70
4.2.3.4	Data Protection Addendum: Auftragsverarbeitung und Standarddatenschutzklauseln ..	70
4.2.3.5	Data Protection Addendum: Rangfolgeregelungen. ....	72
4.2.3.6	Ausschlüsse vom DPA, sog. eigene Zwecke	74
4.2.3.7	Relevanz der „Core Online Services“....	75
4.2.3.8	Angaben zu Arten der Daten, Zwecken etc..	76
4.2.3.9	Änderungen in der DPA-Fassung vom 18.02.2025 .....	77
4.2.3.10	Änderungen in der DPA-Fassung vom 01.04.2025 .....	79
4.2.4	Berufsgeheimnisträger Zusatzvereinbarung und § 203 StGB.....	79
4.2.5	Weitere Zusatzvereinbarungen und Rahmenverträge ..	81
4.3	Einordnung: Wesen der DSK und Relevanz von aufsichtsbehördlichen Positionen .....	81
4.3.1	Rechtsnatur und Relevanz der Datenschutzkonferenz	82
4.3.2	Keine Verbindlichkeit der Positionen von Aufsichtsbehörden .....	83
4.3.3	Zusammenfassung.....	84
4.4	Bewertung der Hauptkritikpunkte der Aufsichtsbehörden ..	84
4.4.1	Kritikpunkt: Einhaltung der Rechtmäßigkeit nicht nachweisbar.....	85
4.4.1.1	Inhalt der Kritik .....	85
4.4.1.2	Bewertung.....	86
4.4.1.3	Ergebnis .....	87
4.4.2	Kritikpunkt: Transparenz über „eigene Zwecke“ von Microsoft und eingesetzte Drittanbieter .....	88
4.4.2.1	Eigene Tätigkeiten .....	90
4.4.2.2	Tätigkeiten zur Leistungserbringung: Connected Experiences, Telemetrie- und Diagnosedaten.....	91
4.4.2.3	Die Connected Experiences („verbundene Erfahrungen“) .....	93
4.4.2.4	Exkurs: Darstellung von Connected Experiences.....	93

4.4.2.5	Exkurs: Darstellung der optionalen Connected Experiences, insb. „Giphy“ . . . . .	94
4.4.2.6	Telemetrie- und Diagnosedaten . . . . .	95
4.4.2.7	Bewertung zu Connected Experiences; Telemetrie und Diagnose . . . . .	96
4.4.2.8	Zusammenfassung . . . . .	98
4.4.3	Kritikpunkt: Übermittlung von Daten in die USA und Offenlegung an (US-)Sicherheitsbehörden . . . . .	98
4.4.3.1	EU-US Privacy Framework . . . . .	99
4.4.3.2	Gültigkeit des DPF . . . . .	100
4.4.4	Kritikpunkt: „Latente Übermittlung“ . . . . .	101
4.4.5	Kritikpunkt: Subunternehmer . . . . .	102
4.4.5.1	Angebliche Pflicht zur Überprüfung von Unterauftragsverarbeitern . . . . .	102
4.4.5.2	Information über Änderungen der eingesetzten Unterauftragsverarbeiter . . . . .	104
4.4.6	Besonderheit: Telekommunikationsrecht . . . . .	106
4.5	Änderungen durch das EU-US Data Privacy Framework (2023) . . . . .	107
4.6	Weitere Änderungen seit dem DSK-Beschluss aus 2022 . . . . .	108
4.7	Faktisches Argument: Nutzung von M365 durch Behörden . . . . .	109
4.8	Sekundäre Argumente gegen die Auffassung der DSK . . . . .	110
4.9	Besonderheiten bei speziellen Arten von Verantwortlichen und Branchen . . . . .	112
4.9.1	Einsatz von M365 in Behörden und anderen öffentlichen Stellen . . . . .	112
4.9.1.1	Kein „berechtigtes Interesse“ bei behördlichen Aufgaben . . . . .	112
4.9.1.2	Sensible Daten und Teilnahmezwang . . . . .	113
4.9.1.3	Privatrechtliche Gesellschaften in öffentlicher Hand . . . . .	114
4.9.2	Gesundheitsdatenschutz und branchenspezifische Regulierung . . . . .	114
4.9.3	Datenschutz bei Kirchen und religiösen Vereinigungen (Art. 91 DSGVO) . . . . .	115
4.9.4	Datenschutz bei journalistisch-redaktionellen Tätigkeiten . . . . .	115
4.10	Zusammenfassung der datenschutzrechtlichen Situation . . . . .	116
4.11	Vergleich mit Alternativen zu Microsoft 365 und IT-Governance . . . . .	117
4.11.1	Alternative Cloud-Angebote . . . . .	117
4.11.2	Digitale Souveränität . . . . .	118

## Inhaltsverzeichnis

4.11.3 Betrieb on premise und IT-Governance .....	119
4.11.4 Datensicherheit und Vermeidung von Datenpannen ..	119
4.11.5 Zusammenfassung .....	121
4.12 Zusammenfassung: Konkrete Risiken und Maßnahmen bei einem M365-Einsatz .....	122
4.13 Maßnahmenplan zur Risikoreduzierung .....	123
<b>5. Kapitel: Restrisiken, Prüfungstiefe und Business Judgment Rule .....</b>	<b>127</b>
5.1 Verbleibende Unklarheiten .....	127
5.2 Erforderliche Prüfungstiefe .....	128
5.3 Umgang mit Restrisiken .....	130
5.3.1 Handhabung im datenschutzseitigen Projektmanagement .....	131
5.3.2 Kommunikative Handhabung; Empfehlungen und „Abraten“ .....	131
5.3.3 Rechtliche Handhabung von Ungewissheiten .....	132
5.4 Management-Entscheidungen und Business Judgment Rule ..	133
5.4.1 Die Business Judgment Rule .....	133
5.4.2 Business Judgment Rule im deutschen Recht .....	134
5.4.3 Inhalt der Business Judgment Rule .....	135
5.4.4 Anwendung der Business Judgment Rule auf eine Entscheidung für M365 .....	135
5.5 Ergebnis .....	136
<b>6. Kapitel: Individuelle Projektbeschreibung; Technische und Organisatorische Massnahmen .....</b>	<b>137</b>
6.1 Beschreibung des Verantwortlichen und Projektstatus .....	137
6.2 Checkliste zur Bestandsaufnahme u. speziellen Risiken beim M365-Einsatz .....	138
6.3 In die M365-Migration einbezogene Abteilungen und Daten ..	143
6.4 Verwendete Dienste und zur Risikobegegnung vorgesehene Maßnahmen .....	143
6.5 Katalog möglicher Maßnahmen .....	144
6.6 Beispiel für technische Einstellungen: CIS-Benchmarks ..	147
<b>7. Kapitel: Datenschutz-Folgenabschätzung (DSFA) .....</b>	<b>151</b>
7.1 Überblick zur Datenschutz-Folgenabschätzung .....	151
7.1.1 Inhalt und Zweck der Datenschutz-Folgenabschätzung .....	151
7.1.2 Interne Zuständigkeit für die Erstellung der DSFA ..	151
7.1.3 Weitere Schritte und „Konsultation“ der Aufsichtsbehörde .....	152
7.1.4 Zeitpunkt der DSFA-Durchführung .....	152

## Inhaltsverzeichnis

7.2	Erforderlichkeit der DSFA im konkreten Fall .....	152
7.2.1	Vorprüfung: Ist eine DSFA durchzuführen (sog. „Schwellwertanalyse“)? .....	153
7.2.2	Ergebnis: Zum mindest vorsorgliche DSFA .....	157
7.2.3	Ausnahme bei kleinen Organisationen ohne Datenschutzbeauftragten .....	157
7.3	Durchführung der Datenschutz-Folgenabschätzung .....	158
7.3.1	Vorgehen .....	158
7.3.1.1	Gesetzliche Anforderungen an die Durchführung (Art. 35 Abs. 7 DSGVO) .....	158
7.3.1.2	Best Practices: Risikomatrix .....	159
7.3.1.3	Durchführung der DSFA nach Diensten und Phasen .....	161
7.3.1.4	Scope der Risikoanalyse: Beschränkung auf M365-spezifische Aspekte .....	161
7.3.2	Besondere Risikofaktoren beim Verantwortlichen .....	162
7.3.2.1	Rechtliche Besonderheiten .....	162
7.3.2.2	Betriebs-/ Dienstvereinbarung .....	162
7.3.2.3	Risikobezogene Besonderheiten .....	163
7.3.2.4	Organisatorische Umsetzung und laufende Änderungen .....	163
7.3.2.5	Durchführung als fortlaufende Folgenabschätzung: Initial „DSFA light“ plus M365-Gremium .....	163
7.3.3	Erfassungs- oder Vorbereitungsphase (Art. 35 Abs. 7 lit. a DSGVO) .....	165
7.3.3.1	Exchange/Outlook Online .....	165
7.3.3.2	Word/ppt/xls Online .....	165
7.3.3.3	OneDrive, SharePoint Online .....	166
7.3.3.4	Teams .....	166
7.3.4	Bewertungsphase (Art. 35 Abs. 7 lit. b und c DSGVO) .....	166
7.3.4.1	Exchange/Outlook Online .....	168
7.3.4.2	Word/PowerPoint/Excel Online .....	171
7.3.4.3	OneDrive, SharePoint Online .....	172
7.3.4.4	Teams .....	173
7.3.5	Gesamt-Risikobewertung vor Maßnahmen .....	176
7.3.6	Maßnahmenphase (Art. 35 Abs. 7 lit. d DSGVO) .....	177
7.3.7	Risikobewertung nach Maßnahmen .....	178
7.3.8	Abschließende Bewertung .....	180
7.3.9	Dokumentation zur DSFA; Änderungen und Versionskontrolle .....	181
7.4	Anhänge zur Datenschutz-Folgenabschätzung .....	181

## Inhaltsverzeichnis

7.4.1	Anhang 1: Vorbereitende Risikoanalyse .....	181
7.4.2	Anhang 2: Hilfsmittel und DSFA-Muster für M365 ..	181
7.4.2.1	Hilfsmittel zur DSFA-Erstellung .....	181
7.4.2.2	Muster und Informationen von Microsoft ..	182
7.4.2.3	Veröffentlichte DSFA-Muster zu M365 .....	183
7.4.2.4	Veröffentlichte DSFA-Muster zu Copilot .....	184
<b>8.</b>	<b>Kapitel: Entscheidung und Rat des Datenschutzbeauftragten</b> .....	185
8.1	Rat des Datenschutzbeauftragten im Rahmen der DSFA....	185
8.2	Entscheidung des Verantwortlichen (durch die Geschäftsführung) .....	186
<b>9.</b>	<b>Kapitel: Transfer Impact Assessment (TIA)</b> .....	187
9.1	Notwendigkeit eines Transfer Impact Assessments .....	188
9.2	Sinnhaftigkeit eines SCC-TIA für die USA seit Geltung des DPF.....	189
9.3	Terminologie: Drittlandtransfer, Standarddatenschutzklauseln, „EU-US“ .....	190
9.4	Anforderungen an ein Transfer Impact Assessment.....	191
9.4.1	Hintergrund: Schrems II-Entscheidung.....	191
9.4.2	Neufassung der SCC 2021 und Kodifizierung des Transfer Impact Assessment .....	192
9.4.3	Meinungsstand zu Inhalt und Ablauf .....	194
9.4.4	Zuständigkeit für das TIA und Parteien der SCC im Microsoft-DPA .....	195
9.4.5	Zeitpunkt der Durchführung und regelmäßige Überprüfung .....	196
9.4.6	Inhalt der Prüfung laut Klausel 14 SCC .....	196
9.5	Vertragswerk.....	198
9.6	Durchführung des Transfer Impact Assessments .....	199
9.6.1	Beschreibung der Übermittlung .....	200
9.6.1.1	Anwendungsbereich des „Microsoft Products and Services Data Protection Addendum“ .....	200
9.6.1.2	Kategorien der personenbezogenen Daten ..	200
9.6.1.3	Zweck der Verarbeitung .....	201
9.6.1.4	Speicherort der übermittelten Daten; EU Data Boundary .....	202
9.6.2	Identifizierung der Bestimmungen im Drittland .....	203
9.6.2.1	Erläuterung der Problematik, insb. FISA 702 und CLOUD Act .....	204

9.6.2.2	Datenschutzrechtliche Relevanz der „latenten Zugriffsmöglichkeit“ . . . . .	205
9.6.3	Identifizierung der technischen, vertraglichen und organisatorischen Maßnahmen zum Schutz der übermittelten Daten . . . . .	207
9.6.4	Datenschutzniveau unter Berücksichtigung des EU-US Data Privacy Framework . . . . .	208
9.6.4.1	Das EU-US Data Privacy Framework; Executive Order 14086 . . . . .	209
9.6.4.2	Bestand des DPF; Latombe-Klage/ „Schrems III“ . . . . .	211
9.6.4.3	Bewertung des Datenschutzniveaus im konkreten Fall . . . . .	212
9.6.5	Argumentationen jenseits des DPF . . . . .	214
9.7	Gesamtbewertung des TIA . . . . .	215
<b>10. Kapitel: Eintrag im Verarbeitungsverzeichnis</b>	217	
10.1	Einleitung . . . . .	217
10.2	Vorlage Verarbeitungsverzeichnis . . . . .	218
<b>11. Kapitel: Copilot-Varianten und Datenschutz</b>	223	
11.1	Einleitung . . . . .	223
11.2	Die Copilot-Varianten . . . . .	223
11.2.1	Microsoft 365 Copilot Chat . . . . .	225
11.2.2	Microsoft 365 Copilot . . . . .	227
11.2.3	Umgang mit laufenden Änderungen der Copiloten . . . . .	228
11.2.4	Unterscheidung in der Praxis . . . . .	228
11.2.5	Zugriff des Microsoft 365 Copilot auf eigene und Unternehmensdaten . . . . .	230
11.2.6	Zugriff des Microsoft 365 Copilot Chat auf eigene und Unternehmensdaten . . . . .	231
11.2.7	Einstellungen zu Microsoft 365 Copilot (Chat) im Admin-Center und in Teams . . . . .	233
11.3	Datenschutzregeln von Microsoft für die Copilot-Varianten . . . . .	236
11.3.1	Geltung des Data Protection Addendum (DPA) . . . . .	236
11.3.2	Copiloten als „Products and Services“ im Sinne des DPA und der Product Terms . . . . .	236
11.3.3	Copiloten als Core Online Services . . . . .	237
11.3.4	Copiloten und EU Data Boundary . . . . .	238
11.3.5	Bing-Suchanfragen und Verwendung von Web-Daten . . . . .	239
11.3.6	Commercial Data Protection und andere Datenschutz-Programme von Microsoft . . . . .	241
11.3.7	Terms of Use & AI-Zusagen von Microsoft . . . . .	241

## Inhaltsverzeichnis

11.3.8 Zusammenfassung.....	242
<b>11.4 Fallgruppen bei der Verwendung von Copilot .....</b>	<b>243</b>
11.4.1 Use Case 1: Unkritische Daten .....	243
11.4.2 Use Case 2: Mittelkritische Daten.....	244
11.4.2.1 Spezifische Risiken beim Microsoft 365 Copilot .....	245
11.4.2.2 Risikoreduzierung bei Microsoft 365 Copilot .....	246
11.4.2.3 Datenschutz-Folgenabschätzung für Microsoft 365 Copilot in Use Case 2 .....	247
11.4.3 Use Case 3: Sehr kritische Daten sowie Hochrisiko- KI i. S. d. Art. 6 KI-VO .....	248
11.4.3.1 Bewertung als Hochrisiko-KI.....	248
11.4.3.2 Datenschutz-Folgenabschätzung .....	249
<b>11.5 Datenschutz-Folgenabschätzungen zu Microsoft (365)     Copilot .....</b>	<b>250</b>
<b>12. Kapitel: Anlagen.....</b>	<b>253</b>
12.1 FAQ für Mitarbeitende und Öffentlichkeitsarbeit .....	253
12.2 Links und weiterführende Literatur .....	255
12.2.1 DSK-Dokumente zu M365 .....	255
12.2.2 Weitere Stellungnahmen der Datenschutzaufsicht ...	256
12.2.3 Links und Literatur zu Microsoft 365 .....	256
12.2.4 Berichte über die Nutzung von Microsoft 365 und Azure in öffentlichen Stellen.....	258