

Datenschutz-Berater

Datenschutz bei Microsoft 365 und Copilot

Rechtliche Begründung, interne Freigabe,
Datenschutz-Folgenabschätzung und
Compliance-Prozesse

Dr. Olaf Koglin

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.de> abrufbar.

I S B N 9 7 8 - 3 - 8 0 0 5 - 1 9 5 7 - 6

dfv Mediengruppe

© 2025 Deutscher Fachverlag GmbH, Fachmedien Recht und Wirtschaft, Mainzer Landstr. 251, 60326 Frankfurt am Main, buchverlag@ruw.de

www.ruw.de

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Druck: Beltz Grafische Betriebe GmbH, 99947 Bad Langensalza

Printed in Germany

Zur Verwendung dieses Buchs

Dieses Werk enthält für Ihren konkreten Einsatz von Microsoft 365 Muster, also generische Dokumente. Anpassungen an die eigene individuelle Sach- und Rechtslage, darauf basierende Risikobewertungen und die Festlegung entsprechender Maßnahmen sind vom Verantwortlichen durchzuführen. Zur einfacheren Suche in einem digitalen Format sind hierfür in Mustertexten Bearbeiterhinweise mit einem # markiert und in eckige Klammern gestellt [#Bearbeiterhinweis].

Soweit nicht anders angegeben, wurden URLs zuletzt im Zeitraum Dezember 2024/Januar 2025 aufgerufen. Das Manuskript basiert größtenteils auf dem Stand von Ende Januar 2025. Letzte Aktualisierungen einschließlich der DPA-Fassung vom 01.04.2025 erfolgten bis Anfang April 2025.

Zu unpräzisen Begriffen in diesem Buch: Die weibliche oder männliche Form sowie Formulierungen im Plural schließen hier stets sämtliche Personen (w/m/d) mit ein. Viele rechtliche Pflichten, die Verantwortliche treffen, sind auch von Auftragsverarbeitern zu erfüllen. Letztere werden dabei in diesem Buch nicht zusätzlich genannt. Statt des Begriffs des Verantwortlichen werden häufig auch rechtlich unpräzise Formulierungen wie Unternehmen, Behörde oder Organisation verwendet. Dies erfolgt bewusst und zur anschaulicheren Darstellung. Entsprechendes gilt u. a. für Begriffe wie „Geschäftsführer“ als Synonym für Organe.

Die „Standardvertragsklauseln“ heißen korrekt Standarddatenschutzklauseln. Dennoch wird hier die verbreitete Abkürzung SCC verwendet. Auch wird in diesem Buch bisweilen von einem „europäischen Gesetzgebungsprozess“ gesprochen, obschon es natürlich nicht den Kontinent Europa, sondern die Europäische Union betrifft. Unterabsätze wie in Art. 6 Abs. 1 DSGVO werden z. T. als „S. 1“ oder gar nicht näher zitiert. Es wird gebeten, diese und ähnliche Präzisionsdefizite zugunsten der besseren Lesbarkeit zu entschuldigen.

Für alle

„Für alle“ – so hatte ich das Vorwort zu meiner ersten Monografie überschrieben. Es war meine Dissertation, in der ich Rechtsfragen von Open Source Software analysiert hatte. Damals waren die Open-Source-Community, zu der ich zählte, und Microsoft Erzfeinde. Das Geschäftsmodell von Microsoft war die Lizenzierung von „proprietärer Software“, und proprietäre Software wurde durch die „Free Software“-Bewegung in Frage gestellt. Damals galten Konzerne als sichere Quelle für Software, und Kollektive, die ohne Bezahlung Freie Software programmierten, als obskure Konstruktion aus Hacker-Kreisen. Ein Großteil meiner persönlichen Arbeit und der des „Instituts für Rechtsfragen der Freien und Open Source Software“ (ifrOSS) bestand darin, Argumentationen gegen diese Bedenken aufzuzeigen und darzulegen, weshalb Open Source Software ohne unangemessene Risiken eingesetzt werden kann.

In den über 20 Jahren, die seitdem vergangen sind, hat sich die Welt verändert: Heute gelten Konzerne und insbesondere die „Hyperscaler“ aus den USA als obskures Feindbild, während nationale Anbieter und Open Source Software von Aufsichtsbehörden gerne als goldener Weg propagiert werden. Das Geschäftsmodell von Microsoft besteht nicht mehr vorrangig aus dem Verkauf von Softwarelizenzen, sondern aus Cloud Services wie Azure und der Software-as-a-Service-Lösung „Microsoft 365“. Ein Großteil meiner persönlichen Arbeit und der meines Startups LegalCheck besteht darin, Argumentationen gegen die Bedenken der Aufsichtsbehörden aufzuzeigen und darzulegen, weshalb Microsoft 365 und Copilot ohne unangemessene Risiken eingesetzt werden können.

Habe ich mich nun vom Saulus vom Paulus gewandelt, oder mag ich es nur, gegen die „herrschende Meinung“ zu argumentieren – vor allem, wenn sie vom Staat vorgetragen wird oder von jenen, die die Deutungshoheit für sich in Anspruch nehmen? Oder versuchte ich in beiden Fällen lediglich, ungeklärte Rechtsfragen rechtswissenschaftlich zu analysieren? Ich weiß es nicht. Zumindest aber hoffe ich, mit diesem Buch die rechtliche Betrachtung des Einsatzes von Microsoft 365 und Copilot auf juristische, datenschutzrechtliche Themen zu begrenzen und von (industrie-)politischen Aspekten wie der „digitalen Souveränität“ zu befreien.

Dabei freue ich mich auf Gegenrede und wissenschaftliche Diskussionen, zu denen viele der in diesem Buch angesprochenen Themen Anlass geben werden – von A bis Z wie der Auftragsvereinbarung und ihren Details, den Grenzen des Telekommunikationsrechts, dem Umgang mit Restrisiken und den (eigenen) Zwecken der Datenverarbeitung. Daher hoffe ich, dass die-

Für alle

ses Buch nicht nur von jenen gelesen wird, die ohnehin Microsoft-Produkte einsetzen oder für sie argumentieren, sondern gerade auch von jenen, die andere Auffassungen vertreten. In diesem Sinne ist die Widmung auch dieses Werks wieder: **Für alle.**

Für alle gleichermaßen? Nicht ganz. An einen Menschen möchte ich speziell erinnern: Herrn Prof. Dr. Spindler hatte ich im Vorwort zu meiner Dissertation besonders gedankt, und dazu hatte ich allen Grund. Er war stets an neuen Themen interessiert, und hat junge Menschen wie damals mich gerne und selbstlos gefördert. Leider ist Gerald Spindler 2023 viel zu früh verstorben. Ich weiß nicht, ob er gewollt hätte, dass ein so produktbezogenes Buch wie dieses ihm gewidmet wird. Zumindest aber möchte ich mit diesem Vorwort seiner gedenken.

Das Buch enthält viele Inhalte und Bewertungen aus meiner Beschäftigung mit Microsoft-Verträgen und -produkten in der Rolle des Inhouse-Datenschützers, als Rechtsanwalt, Autor und durch LegalCheck. Es war mit dem Verlag ursprünglich als knapp 100-seitiges, kleines Praxishandbuch geplant. Mit der Ausarbeitung und ständigen Vertiefung von Manuskriptteilen, der Übernahme von Inhalten aus meinen Vorträgen und Einarbeitung von aktuellen Themen wurde es immer länger. Auch bei Abgabe der Druckfassung denke ich bei fast jedem Absatz und jedem Argument, dass es noch so viel zu vertiefen, produktseitig oder technisch zu ergänzen, an Argumenten und Gegenargumenten zu verfeinern, und mit anderen Produkten oder Rechtsgebieten zu vergleichen gäbe.

Doch an einem bestimmten Punkt muss bei einem Manuskript der „Code Freeze“ stattfinden, und ich möchte jetzt schon beim Verlag und den zahlreichen Kunden, die das Buch vorbestellt hatten, für die Verzögerung um Entschuldigung bitten. Danken möchte ich in diesem Zusammenhang dem dfv Verlag und Torsten Kutschke für die Aufnahme in diese Reihe sowie Patrick Orth für die gute Betreuung und das professionelle Nudging zur baldigen Abgabe. Ein ganz besonderer Dank geht an Nadine Grüttner für das unermüdliche Nachtragen von Ergänzungen oder Änderungen, und für die vielen guten Ideen. Für viele angenehme Veranstaltungen und tiefgehende rechtliche und technische Diskussionen, bei denen ich sehr viel lernen durfte, möchte ich ganz herzlich Dr. Stefan Brink, Dom Côté, Prof. Dr. Alexander Golland, Stephan Hansen-Oest, Prof. Niko Härting, Raphael Köllner, Dr. Kevin Leibold, Johannes Nehlsen, Wiebke Löck, Iris Phan, Dr. Carlo Piltz, Phillip Reck, Frederick Richter, Heiko Roth, Prof. Dr. Kay Schumann, Ralf Wigand und – ganz besonders – Herrn Michael Will danken. Nicht unerwähnt lassen möchte ich an dieser Stelle auch Stefan Hessel und den immer unkomplizierten und offenen Austausch unter uns. Sehr dankbar für die Unterstützung, Anregungen und Korrekturen bin ich Karol Czuba und Josefine Schulte sowie Jessica Preiß.

VIII

Für alle

Vor allem aber möchte ich meinen tollen Mandanten, Kunden und früheren Kollegen danken, mit denen ich zu diesen Themen in immer wieder anders gearteten Projekten zusammenarbeiten konnte. Ohne Euch/Sie hätte dieses Buch nicht diesem Umfang und das breite Spektrum an Unterthemen.

Last but not least geht eine aufrichtige Bitte um Entschuldigung und großer Dank an meine Familie, die ich durch dieses Buchprojekt an viel zu vielen Abenden, Ferientagen und Wochenenden vernachlässigt habe. Love you, EMGI!

Berlin, April 2025

Olaf Koglin

Grußwort von Dr. Stefan Brink

Wer als Datenschützer den Einsatz von Microsoft 365 und Copilot analysiert, der sieht sich mit einer Fülle von Fragen konfrontiert: Was hat sich an der weltweit verbreiteten „Standard-Software“ dadurch verändert, dass sie als Software as a Service aus der Cloud heraus angeboten wird? Welche Datenflüsse sind zu erwarten, welche nicht? Lässt sich das Produkt in einem Sinne beherrschen, der mit dem Anspruch der Datenschutz-Grundverordnung vereinbar ist, Rechenschaft (!) über alle (!) Datenverarbeitungen abzulegen? Und wie gelingt das bei den Anwendungen, die auf Künstliche Intelligenz setzen?

Das sind gebotene Fragen – aber die Aufgabe von uns Datenschützern besteht eben nicht nur darin, die richtigen Fragen zu stellen; vielmehr müssen wir uns auch und sogar vorrangig darum bemühen, gute, vertretbare und vor allem hilfreiche Antworten auf diese Fragen zu finden. Und dass dieses Buch genau dazu beiträgt, gute Antworten auf notwendige Fragen zu finden, zeichnet es aus.

Berlin, im Januar 2025

*Dr. Stefan Brink**

* Geschäftsführender Direktor des wissenschaftlichen Instituts für die Digitalisierung der Arbeitswelt wida/Berlin; Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg a. D.

Grußwort von Frederick Richter

Suchen Sie ein Buch zu einer komplexen Datenschutzaufgabe, in dem es nicht nur darum geht, was alles für Bedenken bestehen und was alles für Risiken drohen und was alles einer Lösung im Weg stehen mag? Dann sollten Sie sich vielleicht dem vorliegenden Werk nähern. Denn darin wird recht unbeirrt auf ein Ziel zugesteuert: Den Einsatz eines kommerziellen Produkts eines internationalen Anbieters in datenschutzgerechter Weise unter vertretbarem Aufwand zu ermöglichen. Aufwand erfordert das Gehen des Weges zu diesem Ziel unbestritten, doch nimmt der Autor die Ratsuchenden so konkret an die Hand, dass jener sich meistern lässt.

Fallstricke mag es vor einem datenschutzkonformen Einsatz von vernetzten Microsoft-Produkten durchaus ein paar geben. Auch die Warnungen von Aufsichtsbehörden tragen nicht dazu bei, dieses Compliance-Thema beschwingt anzugehen. Doch mit Ratgebern wie dem vorliegenden lassen sich die Aufgaben beherzt in Angriff nehmen: Die Kritikpunkte der Datenschutzbehörden werden alle aufgegriffen und bewertet, um aufzuzeigen, wie mit ihnen in der Praxis umgegangen werden kann. Wer sich mit den Argumenten auseinandersetzt und sodann zeigt, wie der eigene Einsatz des Microsoft-Produkts risikodämpfend vorgenommen wird, sollte gegen Pauschalkritik gut gewappnet sein.

Frederick Richter, LL.M.
Vorstand der Stiftung Datenschutz

Grußwort von Michael Will

Ein ganzes Buch über Microsoft 365, nur zum Datenschutz, noch dazu beachtlichen Umfangs? War das wirklich nötig?

Gute Gründe sich mit diesem Werk und seinem Thema, den nicht wenigen datenschutzrechtlichen Fragen rund um den Einsatz von Microsoft 365 und seine KI-Komponente Copilot zu beschäftigen, gibt es freilich genug. Beginnend mit der fast ubiquitären Verbreitung des Produkts, seinen fast unerschöpflich anmutenden Funktionalitäten bis hin zu den aus Sicht der Datenschutzpraxis natürlich im Mittelpunkt stehenden unterschiedlichsten Verarbeitungstätigkeiten, die mit und manchmal auch erst Dank Microsoft 365 durchgeführt werden, ergibt sich eine Vielzahl von Fragestellungen, die die kommenden Seiten angehen. Dabei handelt es sich fast immer um Prüfpunkte und mitunter gar um Herausforderungen, die zudem Microsoft 365 nicht exklusiv mit sich bringt, sondern die genauso auch die datenschutzrechtliche Beurteilung anderer Software-as-a-Service-Angebote bestimmen.

Es ist deshalb das besondere Verdienst des Autors, mit einem genauen Blick immer wieder auch den systematischen Kontext der jeweiligen Fragestellungen und ihre teilweise bereits umfangreichere Diskussionsgeschichte durch die verschiedenen Akteure des Datenschutzes wie Beratern, Praxisvertretern oder die deutschen und europäischen Datenschutzaufsichtsbehörden mit in den Blick zu nehmen. Für all' die, die sich ihrer datenschutzrechtlichen Verantwortung beim Einsatz von Microsoft 365 für ihre Verarbeitungstätigkeiten entschlossen stellen wollen, versprechen die folgenden Seiten auf diese Weise facettenreiche Erkenntnisse sowie hoffentlich zielführende Hinweise zu guten und alltagstauglichen, datenschutzgerechten Lösungen.

Ansbach, im März 2025

Michael Will
Präsident des Bayerischen Landesamts
für Datenschutzaufsicht

Inhaltsverzeichnis

Zur Verwendung dieses Buchs	V
Für alle	VII
Grußwort von Dr. Stefan Brink	XI
Grußwort von Frederick Richter	XIII
Grußwort von Michael Will	XV
Abkürzungsverzeichnis	XXVII
1. Kapitel: Überblick über die zentralen Themen	1
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
2. Kapitel: Herangehensweise und Prüfungsumfang beim Microsoft 365-Projekt	7
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
3. Kapitel: Risiken beim Einsatz von Microsoft 365, insb. aus Sicht der Aufsichtsbehörden	13
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

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
4.	Kapitel: Argumentationslinien für einen Einsatz von Microsoft 365	59
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: Auftragsverar- beitung und Standarddatenschutzklauseln	70
4.2.3.5	Data Protection Addendum: Rangfolge- regelungen.	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 aufsichts- behördlichen Positionen	81
4.3.1	Rechtsnatur und Relevanz der Datenschutzkonferenz	82
4.3.2	Keine Verbindlichkeit der Positionen von Aufsichts- behörden	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-Goverance	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
5.	Kapitel: Restrisiken, Prüfungstriefe und Business Judgment Rule	127
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
6.	Kapitel: Individuelle Projektbeschreibung; Technische und Organisatorische Massnahmen	137
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
7.	Kapitel: Datenschutz-Folgenabschätzung (DSFA)	151
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

7.2	Erforderlichkeit der DSFA im konkreten Fall	152
7.2.1	Vorprüfung: Ist eine DSFA durchzuführen (sog. „Schwellwertanalyse“)?	153
7.2.2	Ergebnis: Zumindest 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 Folgen- abschätzung: 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
8.	Kapitel: Entscheidung und Rat des Datenschutzbeauftragten	185
8.1	Rat des Datenschutzbeauftragten im Rahmen der DSFA	185
8.2	Entscheidung des Verantwortlichen (durch die Geschäftsführung)	186
9.	Kapitel: Transfer Impact Assessment (TIA)	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	196
	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
10. Kapitel: Eintrag im Verarbeitungsverzeichnis	217
10.1	Einleitung	217
10.2	Vorlage Verarbeitungsverzeichnis	218
11. Kapitel: Copilot-Varianten und Datenschutz	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
11.4 Fallgruppen bei der Verwendung von Copilot	243
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
11.5 Datenschutz-Folgenabschätzungen zu Microsoft (365) Copilot	250
12. Kapitel: Anlagen.	253
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

4. Kapitel: Argumentationslinien für einen Einsatz von Microsoft 365

Nach der Zusammenfassung der aufsichtsbehördlichen Kritik an Microsoft 365 soll diese mit der geltenden Rechtslage abgeglichen werden. Zudem werden Argumente und Argumentationslinien aufgezeigt, die die Zulässigkeit der Datenverarbeitung mit M365 begründen. **185**

4.1 Überblick über den Rechtsrahmen von Verfassungen und Datenschutzrecht

Die Datenschutz-Grundverordnung ist nicht die einzige und alles andere überragende Norm in der Europäischen Union. Vielmehr gibt es auf der Ebene der EU, des Bundes und der Länder jeweils Verfassungen, die ihrerseits Grundrechte und zahlreiche weitere Vorgaben enthalten, und zahlreiche weitere Gesetze. **186**

4.1.1 Datenschutz-Basics: Verfassungen, Primärrecht und EU-Grundrechte-Charta

Auf Ebene der EU gehört hierzu die EU-Grundrechtecharta (GRCh),¹²⁵ auf Bundesebene das Grundgesetz und auf Landesebene die Landesverfassungen. Diese Verfassungen gewähren ihren Bürgern, Unternehmen und sonstigen Organisationen Grundrechte, die sich im Detail unterscheiden. So ist der Schutz personenbezogener Daten nur in der Grundrechte-Charta (Art. 8 GRCh) explizit genannt, jedoch nicht im Grundgesetz, wo er nach dem Volkszählungs-Urteil des Bundesverfassungsgerichts als „Recht auf informationelle Selbstbestimmung“ aus dem allgemeinen Persönlichkeitsrecht hervorgeht.¹²⁶ Alle Verfassungen eint aber der freiheitlich-demokratische, individualistische und marktwirtschaftliche Ansatz, der dem Einzelnen **187**

¹²⁵ Charta der Grundrechte der Europäischen Union, 2000/C 364/01.

¹²⁶ „Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des GG Art 2 Abs. 1 in Verbindung mit GG Art 1 Abs. 1 umfaßt. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.“, 1. Leitsatz, BVerfG, Urt. v. 15.12.1983, Az. 1 BvR 209/83 u. a. Dabei ist zu beachten, dass es im Volkszählungs-Fall um ein Abwehranspruchs des Bürgers gegen den Staat ging, nicht um Rechtsfragen zwischen privaten Stellen.

Kap. 4 Argumentationslinien für einen Einsatz von Microsoft 365

Menschenwürde und viele Freiheitsrechte einräumt und zugleich das Prinzip der Marktwirtschaft und der unternehmerischen Freiheit umsetzt, also auch Firmen unternehmerische Freiheit und Recht an ihrem Eigentum explizit gewährt (vgl. Art. 16, 17 GRCh; Art. 9 Abs. 1, 12, 14 GG).

- 188** Dabei liegt auf der Hand, dass einzelne Grundrechte im Widerspruch zueinander stehen können – insbesondere, wenn sie von verschiedenen Grundrechtsakteuren geltend gemacht werden, wie einem Datenverarbeiter und einem Bürger. Auf Ebene der EU wie auch im GG und den Landesverfassungen schlägt nicht ein „Supergrundrecht“ pauschal das andere. Nach dem Grundsatz der „praktischen Konkordanz“ sind bei einer Kollision von Grundrechten diese abzuwägen und so in Einklang zu bringen, dass beide in ihrer Wesensart möglichst weitgehend verwirklicht werden.¹²⁷
- 189** Dies gilt für die Ebene zwischen den Grundrechten. Die EU-GRCh gehört mit dem EU-Vertrag (EUV) und dem Vertrag über die Arbeitsweise der Europäischen Union (AEUV, dem Nachfolger des EG-Vertrags) zum sog. Primärrecht der Europäischen Union (vgl. Art. 1 Abs. 2 AEUV), also zum ranghöchsten Recht der EU. Dem untergeordnet ist das Sekundärrecht. Dies besteht aus den „normalen“ Gesetzen und Beschlüssen, in der Terminologie der EU die Rechtsakte nach Art. 288 AEUV („Verordnungen, Richtlinien, Beschlüsse, Empfehlungen und Stellungnahmen“). Bekanntlich gelten Verordnungen wie die DSGVO unmittelbar, während Richtlinien wie die ePrivacy-RL oder die NIS-2-Richtlinie erst noch von jedem einzelnen Mitgliedstaat umgesetzt werden müssen – was häufig nicht oder verspätet erfolgt.

4.1.2 Relevanz von Erwägungsgründen

- 190** Die Rechtsakte der EU sind nach dem 2. (Unter-)Absatz des Art. 296 AEUV „mit einer Begründung zu versehen und nehmen auf die in den Verträgen vorgesehenen Vorschläge, Initiativen, Empfehlungen, Anträge oder Stellungnahmen Bezug.“ Dies ist der Grund, weshalb die DSGVO und andere EU-Normen vor den Artikeln, also der eigentlichen Norm, ausführliche Erwägungsgründe (ErwG) führen, die teils als ausufernd, als überflüssig (wenn sie den identischen Inhalt haben wie der betreffende Artikel) oder als widersprüchlich (wenn sie einen anderen Inhalt haben als der betreffende Artikel) erscheinen.
- 191** Leider werden die Erwägungsgründe im europäischen Gesetzgebungsprozess oft dazu missbraucht, nicht durchsetzbare Forderungen im Rahmen von Kompromissen zumindest in einem ErwG unterzubringen. Die ErwG ent-

¹²⁷ Für das Grundgesetz BVerfG, Urt. v. 15.01.1958 (Lüth-Entscheidung), BVerfGE 7, 198.

4.1 Rechtsrahmen von Verfassungen und Datenschutzrecht (Überblick) **Kap. 4**

halten dann nicht wie in Art. 296 AEUV vorgesehen die Begründung für den beschlossenen Rechtsakt, sondern enthalten Aussagen oder Andeutungen, die in der Norm gerade nicht umgesetzt wurden. So lässt sich, salopp gesagt, für fast jede Interpretation ein normatives Argument finden. Dies erschwert eine eindeutige und einheitliche Auslegung des Rechts.

Zugleich gibt es auch durchaus sinnvolle und hilfreiche ErwG, etwa ErwG 26 DSGVO mit seiner Definition zum Personenbezug von Daten. Doch leider scheinen der EuGH und andere Gerichte ihn ungern umzusetzen. Dies führt zur Frage der Relevanz der ErwG für die Auslegung der „echten“ Artikel der DSGVO, was den Umfang dieses Buchs sprengen würde. Die Funktion der Begründungspflicht soll primär die Ermöglichung einer externen Kontrolle der Organ der EU sein,¹²⁸ also nicht eine Auslegungshilfe oder Ersatz für juristische Kommentare. Sie gehören nicht zum verfügbaren Teil des jeweiligen Rechtsaktes und sind daher nicht verbindlich.¹²⁹ Gleichwohl haben die Erwägungsgründe große faktische Bedeutung, und der EuGH greift in seinen Entscheidungen regelmäßig auf sie zurück.¹³⁰ **192**

4.1.3 DSGVO als Sekundärrecht unter der EU-GRCh

Hierarchisch unterhalb des Primärrechts mit seinen Grundrechten aus der GRCh folgt das Sekundärrecht, darunter die DSGVO. Die DSGVO ist daher erstens gegenüber anderen Rechtsakten (also insb. anderen Verordnungen und Richtlinien der EU) nicht überlegen, sondern im Einklang mit diesen auszulegen. Dies gilt nicht, soweit eine klare – oder im Fall des Art. 95 DSGVO eher eine schwammige – Regelung zu anderem Sekundärrecht vorliegt. **193**

Zweitens sind DSGVO und weitere sekundäre Rechtsakte nach den Wertungen des Primärrechts auszulegen, hier also insbesondere nach den Grundrechten der EU-GRCh. Ähnlich ist es in der Bundesrepublik, wo das nationale Recht im Lichte der im GG gewährten Grundrechte (und bei Landesrecht zusätzlich nach der jeweiligen Landesverfassung) auszulegen ist und diese nicht verletzen darf. **194**

128 Calliess/Ruffert/*Callies*, EUV/AEUV, Art. AEUV 296 Rn. 11. Lesenswert zur Auslegung im Hinblick auf die verschiedenen Sprachfassungen *Colneric*, Auslegung des Gemeinschaftsrechts und gemeinschaftsrechtskonforme Auslegung, ZEuP 2005, S. 225 (insb. 226 ff.).

129 „Die Begründungserwägungen eines Rechtsaktes der Gemeinschaften sind rechtlich nicht verbindlich und können nicht zur Rechtfertigung einer Abweichung von den Bestimmungen des betreffenden Rechtsaktes angeführt werden.“ (zum damaligen Gemeinschaftsrecht) EuGH, Urt. v. 19.11.1998, Az. C-162/97 (Nilsson u. a.), Rn. 54; Ehmman/Selmayr/*Selmayr/Ehmann*, DS-GVO, Einf. Rn. 97.

130 Ehmman/Selmayr/*Selmayr/Ehmann*, DS-GVO, Einf. Rn. 97 a.E. unter Hinweis auf EuGH, Urt. v. 13.05.2014, C-131/12 (Google Spain).

Kap. 4 Argumentationslinien für einen Einsatz von Microsoft 365

- 195** Wie beschrieben gibt es bei dieser Auslegung kein Super-Grundrecht, das andere Grundrechte stets „schlagen“ würde. Vielmehr sind die Grundrechte für den jeweiligen Fall in Einklang zu bringen. Dies kann – auch bei der konkreten Auslegung zur Bewertung des Einsatzes von M365 – zu unterschiedlichen Wertungen führen, die z. B. von den individuellen Situationen von Betroffenen, Mitarbeitenden oder Kunden, Zwecken und Hintergrund, sowie der M365 einsetzenden Stelle abhängt.

4.1.4 Weitere, insb. nationale Normen

- 196** Neben zahlreichen weiteren Rechtsakten der Union zu Datenschutz und Informationssicherheit existieren auch von Bund, Ländern und weiteren „Herausgebern“ beinahe unüberschaubar viele Normen mit Bezug zum Datenschutz und verwandten Rechtsgebieten. Diese befinden sich zum Teil unterhalb des Geltungsbereichs der DSGVO, müssen also im Einklang mit dieser erlassen und ausgelegt werden. Zum Teil liegen sie außerhalb des Anwendungsbereichs der DSGVO oder gar außerhalb der Zuständigkeit der EU, müssen sich im letzten Fall auch nicht an der GRCh messen lassen.¹³¹
- 197** Zu den nicht direkt vom Bundestag erlassenen Normen zählen z. B. die von der kassenärztlichen Bundesvereinigung herausgegebene „Richtlinie nach § 75b SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit“ in vertragsärztlichen -psychotherapeutischen Praxen¹³² oder das ebenfalls für den Gesundheitsdatenschutz relevante „C5-Testat“, das auf dem vom BSI erstellten „Cloud Computing Compliance Criteria Catalogue“ (C5) und einer entsprechenden Auditierung (Testat) von Wirtschaftsprüfern beruht.¹³³

4.1.5 Zusammenfassung

- 198** Somit sind die DSGVO und andere Datenschutz-Normen nicht isoliert heranzuziehen, sondern müssen im Lichte der GRCh und im Einklang mit anderem Sekundärrecht ausgelegt werden. Zu den zu berücksichtigen Grundrechten gehören nicht nur das Grundrecht auf Schutz personenbezogener Daten (Art. 8 GRCh), sondern auch zahlreiche weitere Grundrechte, darunter die gleich-

¹³¹ Siehe hierzu die Aufteilung des BDSG in seine Teile 2, 3 und 4.

¹³² https://www.kbv.de/media/sp/RiLi___75b_SGB_V_Anforderungen_Gewahrleistung_IT-Sicherheit.pdf. Für die vertragsärztliche Versorgung ist die Rechtsgrundlage nicht mehr § 75b SGB V, sondern § 390 Abs. 1 SGB V.

¹³³ https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/C5_Einfuehrung/C5_Einfuehrung_node.html.

4.2 Überblick über das Vertragswerk zu Microsoft 365 **Kap. 4**

rangigen Grundrechte von Unternehmen. Der Wortlaut der Erwägungsgründe kann nicht unmittelbar zur rechtlichen Bewertung herangezogen werden.

4.2 Überblick über das Vertragswerk zu Microsoft 365

Das Vertragswerk für Microsoft 365 und andere Online-Dienste wird von Microsoft durch die „Product Terms“ eingerahmt. Sie sind öffentlich zugänglich, können also nicht nur von Microsoft-Kunden gelesen und überprüft werden.¹³⁴ **199**

4.2.1 Product Terms als Rahmen einzelner Dokumente

Aufgrund des früheren Titels „Product and Services Terms“ werden sie auch heute teilweise noch als „PST“ bezeichnet. Noch früher wurde der Begriff „Online Services Terms“ (OST) verwendet; auf ihn wird in der Einleitung der Product Terms immer noch Bezug genommen. Bei den Product Terms handelt es sich nicht um klassische Vertragsdokumente im Sinne von Papier-, Word- oder pdf-Dokumenten, sondern zunächst um eine Website, auf der verschiedene Unterbereiche „aufgeklappt“ werden können. **200**

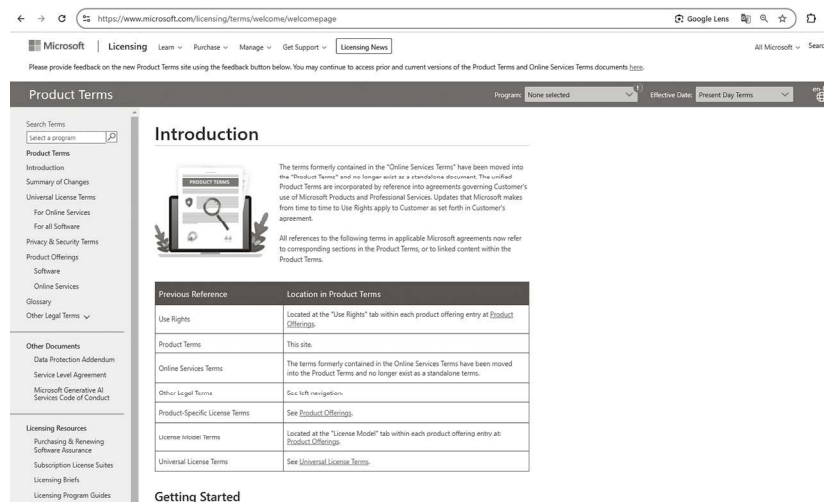


Abbildung 10: Screenshot: Product Terms mit den Unterbereichen (links), darunter auch das Data Protection Addendum¹³⁵

¹³⁴ Kurzlink <https://use365.ms/PT> oder <https://www.microsoft.com/licensing/terms/>.

¹³⁵ <https://www.microsoft.com/licensing/terms/>.

Kap. 4 Argumentationslinien für einen Einsatz von Microsoft 365

4.2.2 Privacy & Security Terms: Definition der Core Services und EU Data Boundary

- 201 Im Bereich „Privacy & Security Terms“ findet sich eine Einordnung der verschiedenen Produktfamilien (wie Azure, Bing, Microsoft 365) und ihrer jeweiligen Bestandteile zu verschiedenen Aspekten des Datenschutzes und der Datensicherheit von Microsoft. Hier finden sich insb. Ausnahmen von der Anwendbarkeit des Data Protection Addendums, die Qualifikation als „Core Online Services“ und die Einbindung in die Zusage des „EU Data Boundary“. Für detailliertere Informationen kann dabei oben rechts als „Progam“ der Lizenzweg ausgewählt werden, etwa „Enterprise“ (Enterprise Agreement, EA) oder „Microsoft Customer Agreement“ (MSA). Zudem kann ein bestimmter zeitlicher Geltungsbereich angegeben werden:



The screenshot shows the Microsoft Licensing website interface. The main content area is titled "Privacy & Security Terms" and includes a "General" section with a paragraph explaining the Data Protection Addendum (DPA) and its applicability. Below this is a table titled "Exceptions to the DPA" which lists specific product families and online services with their corresponding privacy and security terms. A dropdown menu is open, showing a list of license programs including "Enterprise/Enterprise Subscription", "Enrollment for Education Solutions (EES)", "Enterprise/Enterprise Subscription/Server and Cloud Enrollments (EA/EAS/SCE)", "Microsoft Customer Agreement", "Microsoft Online Subscription Agreement (MOSA)", "Microsoft Product and Services Agreement (MPSA)", "Open License (OL)", "Open Value / Open Value Subscription (OV/OVS)", and "Open Value Subscription for Education Solutions (OVS-ES)".

Product Family	Online Service	Privacy & Security Terms
		Services in Containers Because the operating environment of containers installed on Customer's dedicated hardware is not under Microsoft's control, the terms of the DPA do not apply to those containers, except to the extent a) any Personal Data is collected in connection with a billing endpoint, or b) Customer Data is provided to Microsoft for custom model training prior to download of the Service operating in the container.
Azure AI Services		Inactive Services Configurations and Custom Models For the purposes of data retention and deletion, a Services configuration or custom model that has been inactive may at Microsoft's discretion be treated as an Online Service for which the Customer's subscription has expired. A configuration or custom model is inactive if for 90 days (1) no calls are made to it; (2) it has not been modified and does not have a current key assigned to it and; (3) Customer has not signed in to it.

Abbildung 11: Screenshot: Privacy & Security Terms und Auswahl des Lizenzwegs via Drop-Down-Menü

4.2 Überblick über das Vertragswerk zu Microsoft 365 **Kap. 4**

Im weiteren Verlauf der Seite finden sich die Angaben, welche Dienste als „Core Online Services“¹³⁶ bzw. als „EU Data Boundary Services“¹³⁷ definiert werden: **202**

The screenshot shows the Microsoft licensing terms page for Core Online Services. The page is titled "microsoft.com/licensing/terms/product/PrivacyandSecurityTerms/EAEAS". The navigation menu on the left includes sections for "Search Terms", "Product Terms", "Other Documents", "Licensing Resources", and "Glossary". The main content area has tabs for "General", "Core Online Services", and "EU Data Boundary Services". The "Core Online Services" tab is selected, showing a table of services.

Core Online Services	
Microsoft Dynamics 365 Core Services	The following services, each as a standalone service or as included in a Dynamics 365 branded plan or application: Dynamics 365 Customer Service, Dynamics 365 Customer Insights, Dynamics 365 Field Service, Dynamics 365 Business Central, Dynamics 365 Supply Chain Management, Dynamics 365 Intelligent Order Management, Dynamics 365 Finance, Dynamics 365 Commerce, Dynamics 365 Human Resources, Dynamics 365 Project Operations, and Dynamics 365 Sales. Dynamics 365 Core Services do not include (1) Dynamics 365 Services for supported devices or software, which includes but is not limited to Dynamics 365 for apps, tablets, phones, or any of these; (2) LinkedIn Sales Navigator; or (3) except as expressly defined in the licensing terms for the corresponding service, any other separately-branded service made available with or connected to Dynamics 365 Core Services.
Office 365 Services	The following services, each as a standalone service or as included in an Office 365 or Microsoft 365-branded plan or suite: Customer Lockbox, Exchange Online, Archiving, Exchange Online Protection, Exchange Online, Microsoft Bookings, Microsoft Forms, Microsoft Planner, Microsoft Stream (Classic), Microsoft Teams, Microsoft To-Do, Microsoft Defender for Office 365, Office for the web, OneDrive for Business, Project, SharePoint, Sway, Viva Insights, Whiteboard, Viva Engage, and Microsoft 365 Copilot. Office 365 Services do not include Microsoft 365 Apps for enterprise, any portion of a PSTN service that operates outside of Microsoft's control, any client software, or any separately branded service made available with an Office 365 or Microsoft 365-branded plan or suite, such as a Bing or a service branded "for Office 365."
Microsoft 365 Compliance Services	The following services, each as a standalone service or as included in a Microsoft 365-branded plan or suite: Microsoft Purview Customer Lockbox, Microsoft Purview Data Loss Prevention, Microsoft Purview Customer Key, Microsoft Purview Data Lifecycle Management, Microsoft Purview Information Barriers, Microsoft Purview Privileged Access Management, Microsoft Purview Compliance Manager, Microsoft Purview Information Protection, Microsoft Information Governance, Microsoft Purview-Insider Risk Management, Microsoft Purview Communication Compliance, Microsoft Purview Records Management, Microsoft Purview eDiscovery, and Microsoft Purview Audit, Microsoft Priva Privacy Risk Management, and Microsoft Priva Subject Rights Request.

Abbildung 12: Screenshot: Definition der Core Online Services;¹³⁸ hier findet sich auch noch der Begriff „Office 365“

136 <https://www.microsoft.com/licensing/terms/product/PrivacyandSecurityTerms/all#CoreOnlineServices>.

137 <https://www.microsoft.com/licensing/terms/product/PrivacyandSecurityTerms/all#EUDataBoundaryServices>.

138 <https://www.microsoft.com/licensing/terms/product/PrivacyandSecurityTerms/all#CoreOnlineServices>.