Datenschutz-Berater

Datenschutz bei Microsoft 365 und Copilot

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

Dr. Olaf Koglin

Fachmedien Recht und Wirtschaft I dfv Mediengruppe I Frankfurt am Main

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.

ISBN 978-3-8005-1957-6

dfv Mediengruppe

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 [#Berarbeiterhinweis].

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-

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.

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

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 Abwehranspruch des Bürgers gegen den Staat ging, nicht um Rechtsfragen zwischen privaten Stellen.

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.

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 verfügenden 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; Ehmann/Selmayr/*Selmayr/Ehmann*, DS-GVO, Einf. Rn. 97.

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

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 Praxen[132] 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 Sekundärecht 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_Gewaehrleistung_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.

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**

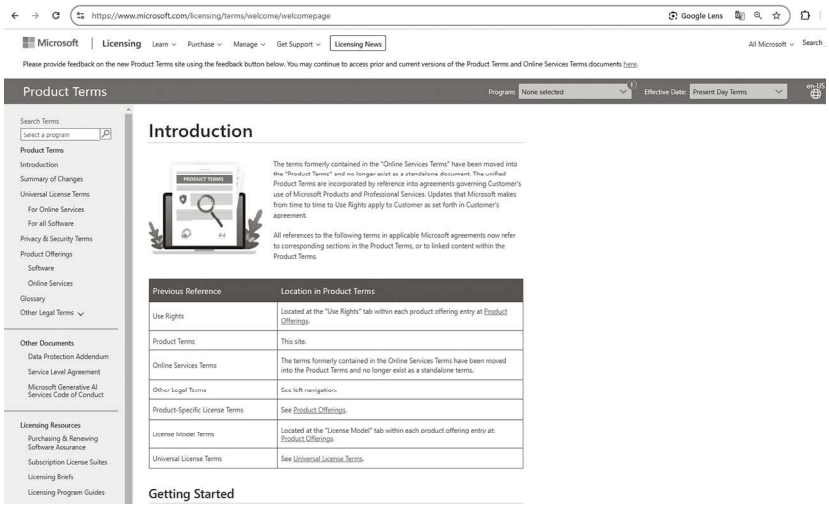

Abbildung 10: Screenshot: Product Terms mit den Unterbereichen (links), darunter auch das Data Protection Addendum[135]

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

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:

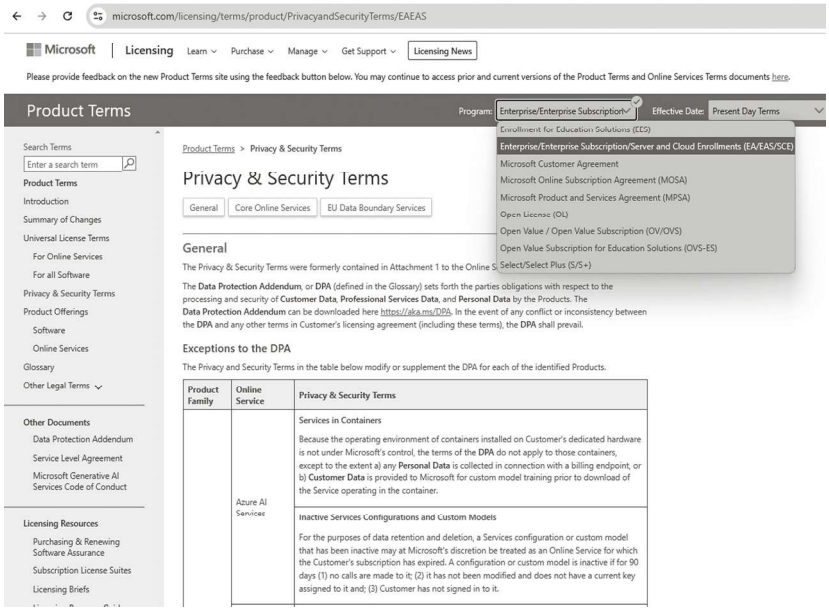

Abbildung 11: Screenshot: Privacy & Security Terms und Auswahl des Lizenzwegs via Drop-Down-Menü

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**

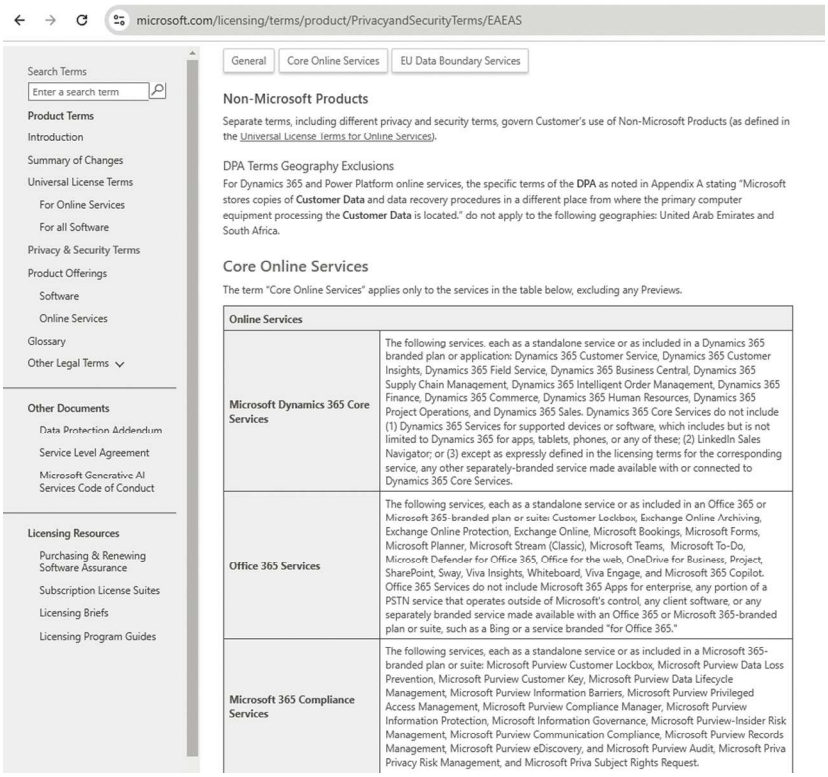

Abbildung 12: Screenshot: Definition der Core Online Services;[138] hier findet sich auch noch der Begriff „Office 365“

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.