48. Jahrgang

datenschutz-berater.de

DSB 09/2024

DATENSCHUTZ-BERATER

» Ihr zuverlässiger Partner für Datenschutz und Datensicherheit

ISSN 0170-7256

dfv Mediengruppe

Dr. Olaf Koglin und Raphael Köllner

Der Verantwortliche und seine Copiloten: Datenschutz und Vertragsbedingungen bei den KI-Produkten von Microsoft

Schon bald nach dem Start vom ChatGPT-Boom hat Microsoft im März 2023 seine „Copilot" genannten KI-Dienste zur Verfügung gestellt. Dabei ist Microsoft die Verbindung mit OpenAI zugutegekommen – die Copiloten basieren auf den GPT-LLM's von OpenAI in einer Microsoft-Umgebung. Heute sind Varianten der Copiloten in den Microsoft-Lizenzpaketen Education, Business und Enterprise enthalten. Dies bedeutet, dass Unternehmen die Copiloten ohne gesonderte Lizenz nutzen können. Der Beitrag erklärt die diversen Copilot-Versionen, die datenschutzrechtlichen Unterschiede und die anstehenden Veränderungen.

Copilot – die KI-Dienste von Microsoft

Microsoft stellt unter der Bezeichnung Copilot verschiedene KI-Dienste zur Verfügung. In der Chat-basierten Version ähneln sie ChatGPT, sind aber in einen Microsoft-Rahmen eingebettet. Wichtig ist bei der datenschutzrechtlichen Betrachtung zunächst, dass es nicht den einen Microsoft Copilot gibt. Vielmehr stellt Microsoft verschiedene Varianten des Copilot zur Verfügung.

Diese unterscheiden sich erheblich in Hinblick auf Funktionsumfang, verwendetem Large Language Model („LLM") und Geschwindigkeit. Von rechtlicher Relevanz sind vor allem die Unterschiede bei Bereitstellung und Einbindung, Datenschutz, rechtlicher Absicherung (wie der Verwendung von Prompts für das Training sowie Garantien gegen Urheberrechtsverletzungen) und Lizenzierung. Darauf basierende Unklarheiten erschweren Verantwortlichen und allen bei der rechtlichen Einschätzung Beteiligten eine verlässliche Bewertung.

Datenschutz bei Cloud-basierten Dienstleistungen

Cloud-basierte Dienste, wie Suchmaschinen, Übersetzungstools oder KI-Dienste, werden häufig in einer kostenlosen Basisversion angeboten, die primär auf Endnutzer ausgerichtet ist. Parallel gibt es eine teurere Version für Unternehmen (dieser Begriff soll in diesem Beitrag auch Vereine, öffentliche Stellen und andere Organisationen umfassen). Typischerweise gibt es bei der „Unternehmensversion" gewisse datenschutzrechtliche Absicherungen wie eine Auftragsverarbeitung und Zusicherungen dazu, dass die mit den Anfragen übermittelten Daten vom Anbieter nicht für andere Zwecke verwendet werden.

Nutzung von Endkunden-Tools bei Personenbezug

Eine häufige Missinterpretation ist dabei, dass datenschutzrechtlich „unsaubere" Endkunden-Tools niemals für personenbezogene Daten genutzt werden dürften. Wie bei klassischen Suchmaschinen und Übersetzungstools dürfen auch KI-Tools von Unternehmen genutzt werden, um unkritische Informationen einzugeben: Für Prompts oder Suchanfragen wie „in welcher Partei ist Olaf Scholz" dürfte ebenso ein berechtigtes Interesse vorliegen wie für „wie heißt die neue Bundesdatenschutzbeauftragte?" Wichtig ist in Unternehmen vielmehr die Sensibilisierung, welche personenbezogenen Daten und Unternehmensinformationen unkritisch sind und welche Tools für die Verarbeitung der sonstigen (d. h. nicht unkritischen) Daten freigegeben wurden.

Differenzierung zwischen Endkunden- und Unternehmenstools bei Microsoft-Produkten

Auch Microsoft nimmt eine solche Aufteilung in Endkunden- und Unternehmensprodukte vor; hier heißen die Endkunden-Dienste meist Consumer-Dienst.

Datenschutz bei Consumer-Diensten

Consumer-Dienste werden lediglich von den allgemeinen Datenschutzbestimmungen (privacy.microsoft.com/de-de/privacystatement) und den produktbezogenen Nutzungsbedingungen (für Bing: www.bing.com/new/termsofuse) erfasst. Eine Auftragsverarbeitung wird nicht vereinbart, sodass Microsoft die eingegeben Daten (wohl) als eigener Verantwortlicher verarbeitet.

Der „kommerzielle Datenschutz" bei Microsoft

Bei den B2B-Diensten erhält der Kunde Zusagen durch die „Commercial Data Protection" (deutsch: „kommerzieller Datenschutz", use365.ms/Copilot-CDP). Mit diesem und weiteren Bedingungen (Terms of Use für Copilot; learn.microsoft.com/en-us/copilot/terms-of-use) sowie den allgemeinen Datenschutzhinweisen sagt Microsoft Folgendes zu:

1. Kundendaten werden nicht zum Trainieren der Modelle verwendet;

2. kein Zugriff auf Kundendaten durch andere Anwendungen; und
3. Chatdaten werden nicht gespeichert.

Ergänzt wird dies u. a. durch das Copilot Copyright Commitment, nach dem Microsoft seine Commercial-Kunden unter bestimmten Voraussetzungen (u. a. Lizenz, keine Deaktivierung des Compliance Monitoring) bei Klagen wegen AI-verursachter Urheberrechtsverletzung freistellen will.

„Enterprise Data Protection" und das Microsoft-DPA

Erst mit dem Level der sog. Enterprise Data Protection wird mit dem Kunden auch eine Auftragsverarbeitungsvereinbarung abgeschlossen. Denn für diese Kunden gilt das Data Protection Addendum von Microsoft (sog. DPA, aka. ms/DPA). Dies enthält eine Auftragsverarbeitungsvereinbarung (zum DPA und AVV Koglin, DSB 2022, S. 38 ff.).

Hierfür sind bislang Volumenlizenzen der sog. Enterprise-Pläne erforderlich, wovon es ab September 2024 für viele Copiloten Ausnahmen geben wird (s. u.).

Überblick über die Copilot-Varianten von Microsoft

Die Microsoft-„Copiloten" können nach der ggf. zugeordneten Lizenz sowie nach der Nutzung (Browser/App) aufgeteilt werden. Sie unterscheiden sich erheblich in der datenschutzrechtlichen Bewertung.

Consumer-Dienste: Copilot und Copilot Pro in Bing ohne Anmeldung mit einem Geschäftskonto

Die am einfachsten zugängliche Variante ist der Chat-basierte Copilot, der ohne Anmeldung als Zusatzprodukt zur Suchmaschine Bing kostenlos zur Verfügung gestellt wird (www.bing.com/chat) und sich dadurch primär an private Nutzer richtet. Mit „Copilot Pro" steht auch eine schnellere Version zur Verfügung; diese ist kostenpflichtig und benötigt daher eine Registrierung. Beide Copilot-Versionen sind typische Endkunden-Produkte im Sinne der obigen Definition; es gilt nur die Consumer Data Protection von Microsoft.

Damit ist bei diesen Diensten weder der „kommerzielle" noch die Enterprise Data Protection anwendbar; Verantwortlicher ist Microsoft. Daher sollte dieser Copilot im Kontext eines Unternehmens nicht für sensible Informationen eingesetzt werden; die URL lässt sich jedoch nicht generell sperren.

Copilot in Bing bei Anmeldung mit Geschäftskonto

Die Nutzung des Bing-Copiloten erfolgt ebenfalls über die Bing-Website, wenn der Nutzer sich mit einem – wie es bei Microsoft heißt – „Geschäfts- oder Schulkonto anmeldet". In Gegensatz zu der Anmeldung mit einem „persönlichen Konto" ist der Nutzer nun nicht mehr lediglich in der Welt der Consumer-Dienste, sondern hat die Zusagen der Commercial Data Protection (s. o.).

Für diese Anmeldung benötigen die Nutzer eine entsprechende Microsoft 365-Lizenz. Neben den Enterprise-Lizenzen ist dies auch mit den sog. Business-Lizenzen möglich, die vor allem von kleinen und mittelständischen Unternehmen genutzt werden. Nach entsprechender Anmeldung wird dem Nutzer in Bing ein rundes grünes Icon mit Schildsymbol angezeigt, das die Geltung des „kommerziellen Datenschutzes" von Microsoft bestätigt. Dies darf jedoch nicht darüber hinwegtäuschen, dass keine „Enterprise Data Protection" vorliegt, also u. a. kein DPA und damit keine Auftragsverarbeitungsvereinbarung anwendbar ist. Auch diese Copilot-Variante sollte also nicht für sensible Informationen verwendet werden.

Microsoft Copilot in Edge

Bing und die soeben vorgestellten, darauf basierenden Copilot-Varianten können in jedem Browser genutzt werden. Besonderheiten gibt es bei deren Nutzung in Edge, dem früher als „Internet Explorer" bezeichneten Microsoft-Browser. Hierbei ist die Nutzung der oben dargestellten Bing-Copiloten in einem aufklappbaren Menü möglich. Dabei kann Copilot Zugriff auf den aktuell geöffneten Browserinhalt eingeräumt werden, was die Einwilligung des Nutzers oder des Administrators voraussetzt.

Dies ist vor allem dann problematisch, wenn Intranet-Seiten, im Browser geöffnete Dokumente oder andere vertrauliche Informationen vom Copilot-Zugriff betroffen sind. Im Übrigen fällt die datenschutzrechtliche Bewertung wie bei der Nutzung von Copilot in Bing aus, d. h. es ist zwischen der Nutzung als Endkunde (keine datenschutzrechtliche Absicherung) und der Nutzung mit einem Geschäftskonto (dann gilt der „kommerzielle Datenschutz") zu differenzieren.

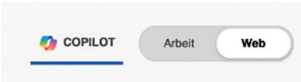
Seit August 2024 gibt es bei Copilot for Edge zusätzlich eine Konfigurationsmöglichkeit des „CopilotCDPPageContext", für den Zugriff auf Browser-Inhalte („Page Context") den kommerziellen Datenschutz („CDP") zu aktivieren.

Microsoft 365 Copilot

Die bislang dargestellten Copiloten (Copilot in Bing, Copilot for Edge) sind strikt zu trennen von den Copiloten-Versionen, die in Microsoft 365 enthalten sind oder hinzugebucht werden können. Diese werden als Funktion in Microsoft Teams, im Copilot for Edge oder auch auf der Webseite www.bing.com/Business/chat zur Verfügung gestellt. Anders als die oben vorgestellten Varianten des Bing-Chats kann die Business-Version nicht ohne Geschäftskonto und Lizenz genutzt werden.

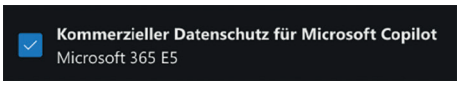
Sofern dem Nutzer eine Copilot for Microsoft 365 Lizenz

zugeordnet wurde, kann er in Bing mittels eines Schiebereglers (sog. Toggle, siehe Abbildung) aus den Bing-Copiloten zum Copilot for Microsoft 365 wechseln:



So erhält der Copilot des Microsoft 365-Nutzers den Zugriff auf Unternehmensdaten und verliert den Zugriff auf die Bing-Dienste, sofern dies Administrator-seitig so eingestellt wurde.

Auf Copilot for Microsoft 365 ist (mit Ausnahme von Web-Content) der kommerzielle Datenschutz mit Enterprise-Niveau anwendbar. Damit gilt das Microsoft-DPA, was auch eine Auftragsverarbeitungsvereinbarung umfasst. Dabei ist jedoch darauf zu achten, dass dem jeweiligen Nutzer tatsächlich eine (kostenpflichtige) Copilot for Microsoft 365-Lizenz zugewiesen wird (siehe Abbildung).



Erweiterte Anwendbarkeit der Enterprise Data Protection ab September 2024

Microsoft hat für September 2024 Ergänzungen des Datenschutzes für diejenigen Nutzer angekündigt, die Copilot ohne eigene „Copilot for Microsoft 365"-Lizenz nutzen und daher bislang keine Auftragsverarbeitung mit Microsoft vereinbaren können.

Sofern sich diese Personen mit ihrer „Entra ID", also dem oben erwähnten Geschäfts- oder Schulkonto anmelden, gilt über den „kommerziellen Datenschutz" hinaus der „Enterprise-Datenschutz" (Enterprise Data Protection, EDP). Damit ist das DPA und die enthaltende Auftragsverarbeitungsvereinbarung anwendbar. Daneben gibt es Zusagen wie das EU Data Boundary Programm, wonach die Daten von Microsoft nur in der EU gespeichert werden. Ausnahmen gibt es u. a. wieder für Bing-Dienste.

Zusammenfassung

Diese Übersicht zeigt, wie komplex das Zusammenspiel von verschiedenen Copiloten, Lizenzierungen und Einstellungen ist – und dass sich bei einem innovativen Thema wie KI (und dessen Vermarktung) laufend Veränderungen ergeben. Zudem gibt es weitere Copiloten wie Windows Copilot und Copilot Studio.

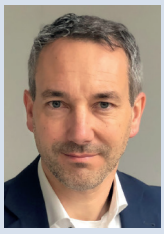
Wichtig ist daher für den Einsatz im Unternehmen, wie generell bei Software as a Service, nicht eine einmalige Freigabe eines Produkts vorzunehmen, sondern einen Prozess für die laufende Überprüfung und Dokumentation zu implementieren, der auch eine klare Kommunikation der Do's und Dont's an die Beschäftigten vorsieht.

Kriterien für den Einsatz Künstlicher Intelligenz

Mit der jüngst erlassenen KI-Verordnung („AI Act") und den ersten Positionierungen der Datenschutz-Aufsichtsbehörden (Überblick im „ONKIDA" des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg, www.baden-wuerttemberg.datenschutz.de/onkida/) gibt es erste Rahmen für die rechtliche Prüfung des KI-Einsatzes. Wie aber manche Reaktionen auf das lesenswerte Diskussionspapier des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit zum Verhältnis von DSGVO zu LLMs (datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/240715_Diskussionspapier_HmbBfDI_KI_Modelle.pdf) zeigen, sind diese – wie auch die Vorgaben der KI-VO – noch stark auslegungsbedürftig. Zudem sind Positionen der Aufsichtsbehörde nicht mit geltendem Recht zu verwechseln. Damit bleibt es Aufgabe und Risiko des jeweiligen Verantwortlichen oder Auftragsverarbeiters, die konkreten Kriterien für die juristische Prüfung der von ihm eingesetzten KI-Dienste in rechtlich vertretbarer Weise festzulegen und anzuwenden.

Konkret für den Einsatz der Microsoft-Copiloten bedeutet dies, intern ebenso Transparenz über die verwendeten Varianten und Lizenzierungen zu haben wie über die Kategorien von Daten, Betroffenen und Zwecken. Ab dem Enterprise-Niveau liegt eine Auftragsverarbeitungsvereinbarung vor. Bekanntlich sehen die Aufsichtsbehörden die Produkte US-amerikanischer Konzerne meist skeptisch. Gleichwohl hat der Landesbeauftragte für den Datenschutz Niedersachsen den Einsatz von Microsoft Teams auf Basis des DPA – jedenfalls mit einer Zusatzvereinbarung – akzeptiert (Koglin, DSB 2024, S. 126), und zahlreiche öffentliche Stellen setzen Microsoft 365 ein. Daher scheint es bei Berücksichtigung individueller Besonderheiten vertretbar, mit dem Enterprise-Datenschutz die Copiloten auch für Unternehmenszwecke zu nutzen.

Autoren: **Rechtsanwalt Dr. Olaf Koglin ist Geschäftsführer des Datenschutzdienstleisters LegalCheck. Daneben ist er Director Legal & Operations der Nachrichten-App upday und Mentor beim Frühphasen-Investor APX.**



Raphael Köllner ist Konzerndatenschutzbeauftragter sowie Geschäftsführer des Microsoft-Partners Kölln-Service GmbH, Microsoft MVP und Microsoft Regional Director.