

Microsoft 365 Copilot in der Verwaltung: Datenschutz, Rechtsgrundlage, DSFA

Es gibt in jedem Copilot-Projekt einen Moment, in dem die Stimmung kippt. Meistens liegt er ungefähr drei Wochen nach der Vorführung im Verwaltungsvorstand, bei der jemand eine Beschlussvorlage zusammenfassen ließ und alle beeindruckt waren. Dann kommt die E-Mail der oder des behördlichen Datenschutzbeauftragten. Sie hat keinen aggressiven Ton. Sie hat nur eine Liste. Fünf Fragen, höchstens sieben, sachlich formuliert – und jede einzelne davon ist geeignet, ein Projekt für ein halbes Jahr stillzulegen, wenn niemand sie beantworten kann.

Das ist keine Schikane, das ist der Job. Und ehrlicherweise sind es genau die Fragen, die man vor der Vorführung hätte klären sollen und nicht danach. Dieser Beitrag beantwortet sie der Reihe nach: Wo werden die Daten verarbeitet? Werden sie zum Training verwendet? Was genau sieht Copilot? Brauchen Sie eine Datenschutz-Folgenabschätzung, und wie sieht die aus? Und was steht eigentlich im Vertrag zur Auftragsverarbeitung?

Was Sie hier **nicht** finden: Prompting-Tipps. Es gibt genug Beiträge darüber, wie man Copilot hübsch bittet. Dieser hier handelt davon, wie Sie das Werkzeug in eine Verwaltung bekommen, ohne dass die Aufsichtsbehörde später Post schreibt – und ohne dass Sie sich in einer Beschlussvorlage auf Formulierungen festlegen, die technisch nicht haltbar sind.

WICHTIG · Das hier ist keine Rechtsberatung

Paragraphen, Fristen und Schwellenwerte stehen hier als Orientierung. Datenschutz im öffentlichen Bereich ist zu wesentlichen Teilen Landesrecht, und die Landesdatenschutzgesetze unterscheiden sich in genau den Punkten, die hier zählen – von der Rechtsgrundlage für Beschäftigtendaten bis zur Frage, wer eine DSFA freigibt.

Für kirchliche Träger gilt ohnehin ein eigener Rechtsrahmen. Prüfen Sie jede Aussage gegen Ihr Landesrecht beziehungsweise gegen DSGVO-EKD oder KDG, bevor Sie sie in ein Dokument übernehmen, das am Ende jemand unterschreibt.

Verarbeitungsorte, Trainingsausschluss, Unterauftragsverarbeiter

Die erste Frage auf der Liste ist fast immer dieselbe, und sie klingt einfacher, als sie ist: Wo werden die Daten verarbeitet? Die kurze Antwort lautet „im Wesentlichen in der EU“. Die brauchbare Antwort braucht ein paar Sätze mehr, denn „im Wesentlichen“ ist genau das Wort, an dem sich eine Prüfung festbeißt.

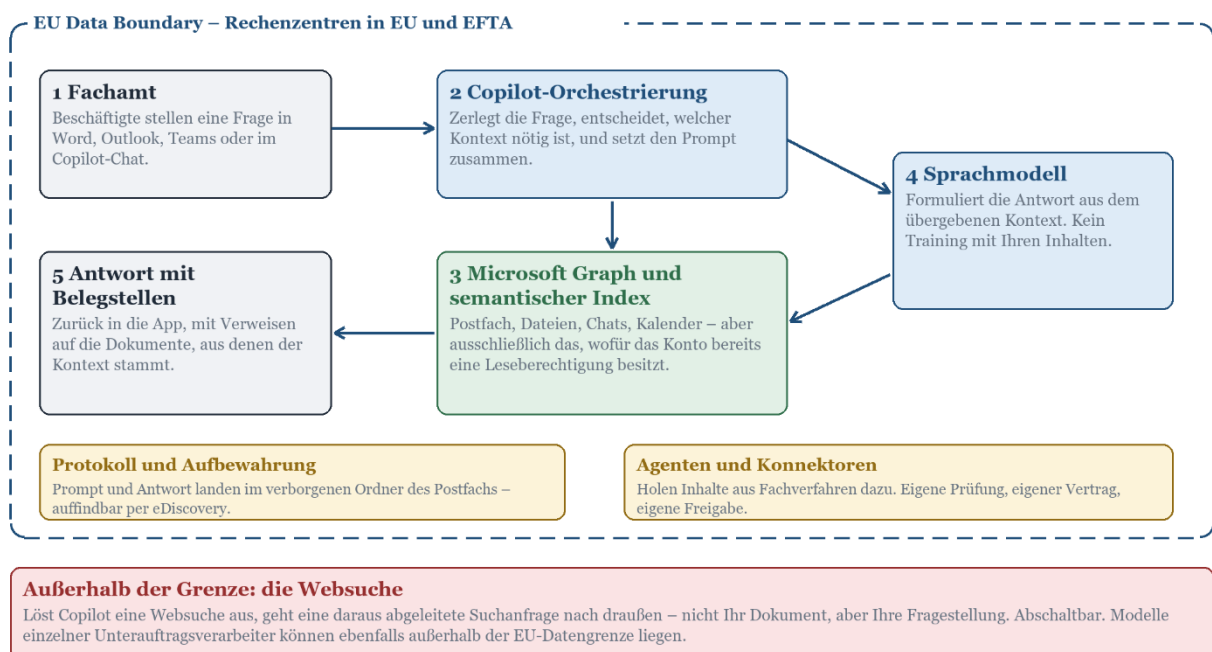
Die EU-Datengrenze und was sie umfasst

Mit der EU Data Boundary hat Microsoft vertraglich zugesagt, Kundendaten und pseudonymisierte personenbezogene Daten aus Systemprotokollen für die einbezogenen Onlinedienste in Rechenzentren innerhalb der EU und der EFTA zu speichern und zu verarbeiten; Daten aus Professional Services werden dort zumindest ruhend gespeichert. Der räumliche Geltungsbereich umfasst die 27 EU-Staaten sowie Island, Liechtenstein, Norwegen und die Schweiz. Copilot wird seit dem 1. März 2024 als abgedeckte Arbeitslast in den Zusagen zur Datenresidenz in den Produktbestimmungen geführt und ist für Mandanten mit Anmeldeort in der EU ein Dienst innerhalb der EU-Datengrenze.

Zwei Details, die in Prüfungen regelmäßig übersehen werden. Erstens: Wer Multi-Geo-Funktionen gebucht hat, fällt aus dem Geltungsbereich der EU-Datengrenze heraus – auch dann, wenn der Mandant in einem EU-Land registriert ist. Für Kommunen ist das selten relevant, für Landesbehörden mit Auslandsbezug und für große Träger gelegentlich schon. Zweitens: Der mandantenweite semantische Index wird für Organisationen innerhalb der EU-Datengrenze in einem Rechenzentrum in der EU oder EFTA gespeichert, und zwar in einem isolierten Container des jeweiligen Mandanten. Der nutzerbezogene Indexanteil liegt dort, wo das Postfach liegt.

Die ehrliche Einschränkung gehört gleich mit dazu: Modelle, die Anthropic als Unterauftragsverarbeiter bereitstellt, sind derzeit vom Geltungsbereich der EU-Datengrenze ausgenommen. Das ist kein Skandal, sondern eine dokumentierte Ausnahme – aber sie gehört in die DSFA und in die Entscheidung, welche Modelle Sie im Mandanten überhaupt zulassen. Diese Auswahl ist eine Administrationsentscheidung, keine Naturkonstante.

Wohin ein Prompt reist – und wohin nicht



Skizze 1: Der Datenweg einer Copilot-Anfrage. Die gestrichelte Linie ist die vertraglich zugesagte EU-Datengrenze – nicht jede Funktion liegt innerhalb.

Der Trainingsausschluss: klar formuliert, oft zu weit zitiert

Die Aussage ist eindeutig und steht so in der Produktdokumentation: Prompts, Antworten und die über Microsoft Graph erreichten Daten werden nicht zum Training der Basismodelle verwendet, auch nicht der Modelle, die Copilot selbst nutzt. Dasselbe gilt für Daten, die über die semantische Indizierung erschlossen werden. Für die Missbrauchsüberwachung mit menschlicher Sichtung, wie sie im Azure OpenAI Service grundsätzlich existiert, hat sich Microsoft für die Copilot-Dienste ausdrücklich abgemeldet.

Wo der Satz häufig überdehnt wird: Optionales Feedback, das Beschäftigte aktiv abschicken – der Daumen nach oben oder unten samt Freitextkommentar – fließt in die Produktverbesserung ein. Nicht in das Training der Basismodelle, aber es verlässt die gewohnte Betrachtung. Diese Funktion lässt sich zentral steuern, und in einer Verwaltung sollte die Entscheidung darüber bewusst und schriftlich fallen, nicht über eine Standardeinstellung. Ein Feedback-Kommentar mit dem

Wortlaut „die Zusammenfassung der Personalakte von Herrn M. war unbrauchbar“ ist im Zweifel der interessantere Datensatz als das gesamte Modelltraining.

FAKTEN · Was Copilot sieht

Alles, was das anfragende Konto lesen darf. Nicht mehr, nicht weniger. Der semantische Index respektiert die identitätsbasierte Zugriffsgrenze: Die Fundierung greift ausschließlich auf Inhalte zu, für die die anfragende Person berechtigt ist.

Postfach, Dateien, Chats, Kalender, Kontakte – also Exchange, SharePoint, OneDrive und Teams des eigenen Mandanten, dazu der Arbeitskontext: die laufende Besprechung, der Mailverlauf zum Thema, der Chat von letzter Woche.

Der mandantenweite Index wird aus textbasierten SharePoint-Online-Dateien erzeugt – Word, PowerPoint, PDF, OneNote, ASPX-Seiten. Der nutzerbezogene Index deckt zusätzlich das eigene Postfach ab. **Nicht** erfasst: delegierte Postfächer, freigegebene Postfächer, archivierte Postfachdaten, archivierte SharePoint-Daten.

Externe Fachverfahren nur, wenn Sie sie über Konnektoren oder Agenten anbinden. Das ist eine bewusste Entscheidung mit eigener Prüfung – keine Nebenwirkung der Lizenz.

Nicht erfasst: Papier in der Registratur, Fachverfahren ohne Anbindung, Netzlaufwerke außerhalb von Microsoft 365, das lokale Dateisystem. Wer diese Grenze in der DSFA sauber zieht, halbiert den Prüfumfang.

Indiziert wird laufend: Dokumente im Postfach nahezu in Echtzeit, neue Dateien auf SharePoint-Websites, die zwei oder mehr Personen zugänglich sind, täglich; Änderungen an bereits indizierten Dokumenten sofort. Eine Berechtigungskorrektur wirkt also – aber nicht zwingend in derselben Minute.

Wer den größeren Zusammenhang sucht, in dem diese Fragen stehen – Betriebsmodell, Beschaffung, Schutzbedarf, Betrieb – findet ihn in der Übersicht [Microsoft 365 in der öffentlichen Verwaltung](#). Dieser Beitrag setzt dort an, wo die Grundsatzentscheidung für die Plattform bereits gefallen ist und Copilot als zusätzliche Verarbeitung obendrauf kommt.

Und die souveräne Alternative?

Die Frage kommt, spätestens im Personalrat. Mit der Delos Cloud existiert eine Plattform, die Microsoft-Technologie unter dem Betrieb einer SAP-Tochter in Deutschland bereitstellen soll, mit Betriebspersonal in Deutschland und angestrebten Nachweisen entlang von BSI C5, ISO 27001 und IT-Grundschutz. Der Aufbau erfolgt schrittweise; welche Dienste in welchem Ausbaustand verfügbar sind, verändert sich, und Copilot in vollem Funktionsumfang ist eine andere Frage als eine Infrastrukturplattform.

Die nüchterne Konsequenz für Ihre Planung: Treffen Sie keine Entscheidung, die von einem Termin abhängt, den Sie nicht selbst kontrollieren. Wer heute eine DSFA für Copilot im kommerziellen Mandanten braucht, braucht sie heute. Eine mittelfristige Migrationsoption ist ein Argument für die Vertragsgestaltung und für eine Ausstiegsklausel in der Vergabe – kein Argument fürs Abwarten. Details zum Angebot und zu den offenen Punkten stehen in [Delos Cloud für Kommunen: Was das Angebot ist, wen es betrifft und was fehlt](#); die Betriebsmodellfrage dahinter behandelt [Standard-Tenant oder Hybrid: Die Betriebsmodell-Entscheidung für Verwaltungen](#).

Das Berechtigungsprinzip – und warum es trotzdem Ihr größtes Risiko ist

Der Satz, den man in jeder zweiten Präsentation hört, lautet: „Copilot sieht nur, was die Nutzerin oder der Nutzer ohnehin sehen darf.“ Der Satz stimmt. Er ist technisch korrekt, er ist dokumentiert

– und er ist gleichzeitig der gefährlichste Satz im ganzen Projekt, weil er beruhigt, ohne zu beruhigen.

Was technisch tatsächlich passiert

Copilot führt keine eigene Rechteverwaltung. Die Fundierung greift auf Microsoft Graph und den semantischen Index zu, und beide respektieren dieselbe identitätsbasierte Zugriffsgrenze wie jede andere Suche im Mandanten. Verschlüsselung durch Vertraulichkeitsbezeichnungen wird beachtet: Wer ein Dokument aufgrund der Nutzungsrechte nicht öffnen darf, bekommt es auch nicht zusammengefasst. Für den Zugriff durch Agenten lässt sich programmatischer Zugriff in den Nutzungsrechten sogar gezielt ausschließen.

Das Problem liegt nicht in der Technik. Es liegt darin, dass „darf sehen“ und „findet“ in einer gewachsenen Verwaltungsablage zwei völlig verschiedene Dinge sind. In einer Stadtverwaltung, die wir bei der Bereinigung ihrer SharePoint-Landschaft im Sozialbereich begleitet haben, war formal alles korrekt: Jede Website hatte einen Eigentümer, jede Berechtigung war irgendwann bewusst vergeben worden. Nur hatte niemand je nachgesehen, was aus einer Freigabe geworden war, die vor Jahren für ein Projekt an „Alle Beschäftigten“ gesetzt wurde. Das blieb lange folgenlos, weil niemand danach gesucht hat. Copilot sucht immer.

WARNUNG · Der Suchindex ist ehrlicher, als Ihnen lieb ist

Bevor Sie Lizenzen verteilen, lassen Sie sich die Berichte zur Datenzugriffs-Governance zeigen: Wie viele Websites sind für „Jeder“ oder „Alle Personen außer externen Benutzern“ freigegeben? Wie viele Freigabelinks ohne Ablaufdatum existieren? Erfahrungsgemäß sind die Zahlen in gewachsenen Umgebungen dreistellig – und die Reaktion im Raum ist Stille.

Ein Pilot mit zwanzig Lizenzen in der Kämmerei ist kein Berechtigungsproblem. Ein Rollout über alle Fachämter ohne vorherige Bereinigung ist eines. Der Unterschied ist nicht die Technik, sondern die Zahl der Menschen, die zufällig die richtige Frage stellen.

Die ausführliche Behandlung dieses Themas samt Vorgehensmodell steht in [Oversharing im Verwaltungs-Tenant: Warum Copilot die Personalakte findet](#).

Die Hebel, die Sie tatsächlich haben

Zwischen „gar nichts tun“ und „zwei Jahre Berechtigungsprojekt vor dem ersten Prompt“ liegt ein brauchbarer Mittelweg. Die folgende Übersicht zeigt die Stellschrauben, die in Verwaltungsprojekten regelmäßig gezogen werden – samt der Grenze, an der jede von ihnen aufhört zu helfen.

Hebel	Wirkung	Grenze
Berechtigungen bereinigen, Websiteeigentümer benennen	Behebt die Ursache. Wirkt auf Suche, Copilot, Agenten und Freigaben gleichzeitig.	Dauert. Braucht die Fachämter, nicht nur die IT. Ohne Zuständigkeitsklärung endlos.
Website aus der Suche nehmen („Suche und Offlineverfügbarkeit“ auf Nein)	Nimmt die gesamte Website aus dem mandantenweiten Index – und damit aus Copilot.	Wirkt immer auf Microsoft Search und semantischen Index zugleich. Kein selektives Abschalten. Die Beschäftigten finden dort dann ebenfalls nichts mehr.
Restricted Content Discovery	Hält einzelne Websites aus organisationsweiter Suche und Copilot-Antworten heraus, während die Berechtigungsprüfung läuft.	Setzt entsprechende Lizenzierung für die erweiterte SharePoint-Verwaltung voraus. Wer zu viel einschränkt, macht Copilot nutzlos.
Vertraulichkeitsbezeichnungen mit Verschlüsselung	Nutzungsrechte werden respektiert. Programmatischer Zugriff durch	Erfordert ein durchdachtes Bezeichnungskonzept. Nachträglich

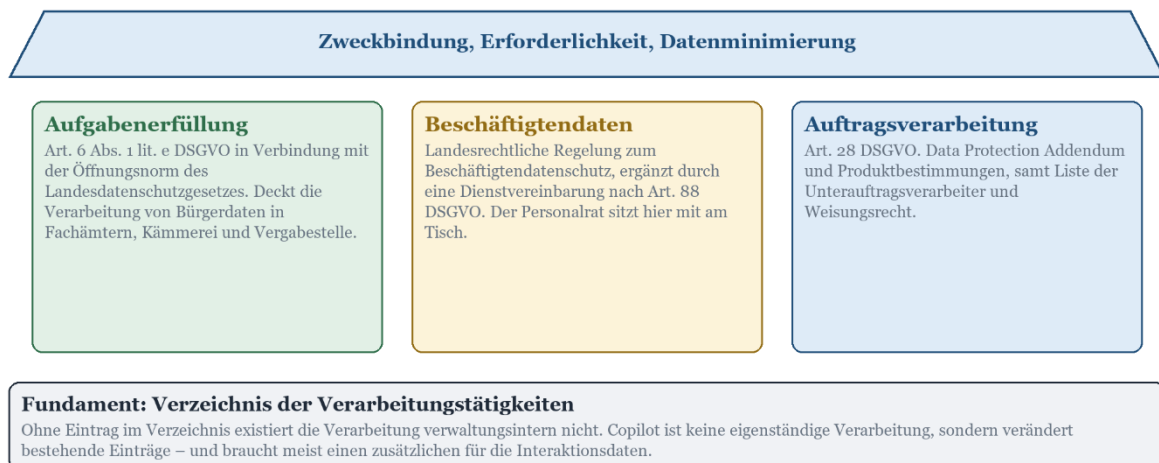
	Agenten kann ausgeschlossen werden.	Millionen Dokumente zu klassifizieren ist ein eigenes Projekt.
Websuche zentral abschalten	Verhindert, dass aus Prompts abgeleitete Suchanfragen den Mandantenkontext verlassen.	Kostet Funktion. Für Recherchen zu Förderprogrammen oder Normen durchaus schmerzhaft.
Agenten im Administrationsportal steuern	Sie entscheiden, welche Agenten zugelassen sind, und sehen deren Berechtigungen und Datenzugriff.	Nur so gut wie der Prozess dahinter. Ohne Freigabeverfahren wandert die Entscheidung ins Fachamt.
Aufbewahrungsrichtlinie für Copilot-Interaktionen	Definiert, wie lange Prompts und Antworten aufbewahrt und wann sie gelöscht werden.	Löschung braucht Zeit (siehe unten). Und ein Hold sticht jede Löschregel.

Eine Reihenfolge, die sich bewährt hat: erst messen, dann die zehn schlimmsten Websites einschränken, dann pilotieren, dann bereinigen, dann ausrollen. Nicht umgekehrt. Wer die vollständige Bereinigung vor den Pilot setzt, verliert die Aufmerksamkeit der Fachämter, bevor sie je einen Nutzen gesehen haben – und Berechtigungsreinigung ohne Fachämter ist Raten mit Administratorrechten.

Rechtsgrundlage: die Frage, die keine Software beantwortet

Hier endet der Teil, den man konfigurieren kann. Keine Einstellung im Administrationsportal schafft eine Rechtsgrundlage. Und die häufigste Antwort, die in Beschlussvorlagen steht – „Einwilligung der Beschäftigten“ – ist im Beschäftigungsverhältnis regelmäßig die schlechteste, weil sich die Freiwilligkeit im über- und untergeordneten Verhältnis kaum tragfähig begründen lässt. Und weil niemand ernsthaft die oder den Einzelnen fragen möchte, ob das Word-Fenster künstliche Intelligenz anzeigen darf, um anschließend mit drei Nein umzugehen.

Drei Säulen – und keine ersetzt die andere



Skizze 2: Rechtsgrundlage, Beschäftigtenschutz und Auftragsverarbeitung sind drei getrennte Prüfungen. Eine gute Antwort auf eine Säule beantwortet die anderen beiden nicht.

Verarbeitung zur Aufgabenerfüllung

Für den Kern der Verwaltungstätigkeit ist die einschlägige Konstruktion in der Regel Art. 6 Abs. 1 lit. e DSGVO in Verbindung mit der jeweiligen landesrechtlichen Öffnungsnorm. Entscheidend ist dabei ein Gedanke, den man nicht überspringen darf: Copilot ist kein neuer Zweck. Wenn das Sozialamt Anträge bearbeitet, bleibt der Zweck die Antragsbearbeitung, ob mit oder ohne

Zusammenfassungsfunktion. Was sich ändert, ist das Mittel – und damit die Erforderlichkeitsprüfung und die technisch-organisatorischen Maßnahmen, nicht der Zweck.

Das ist eine gute Nachricht für den Umfang der Dokumentation und eine schlechte für alle, die gehofft hatten, Copilot als eigenständige, sauber abgrenzbare Verarbeitung beschreiben zu können. In Wahrheit legt sich die Funktion quer über sämtliche bestehenden Verarbeitungstätigkeiten. Praktisch heißt das: Sie ergänzen die vorhandenen Einträge im Verzeichnis um den Hinweis auf die KI-gestützte Verarbeitung und legen einen zusätzlichen Eintrag für die Verarbeitung der Interaktionsdaten selbst an – Prompts, Antworten, Protokolle.

Beschäftigtendaten und der Personalrat

Die zweite Säule ist die heiklere. Copilot verarbeitet Beschäftigtendaten in einem Umfang, der eine eigene Betrachtung verlangt: Wer hat wann welche Frage gestellt, welche Dokumente wurden dabei herangezogen, wie oft wird das Werkzeug genutzt. Das sind Daten, aus denen sich – mit etwas bösem Willen und einer Auswertung im falschen Kontext – Verhaltens- und Leistungsaussagen ableiten ließen. Genau deshalb greift in aller Regel die Mitbestimmung nach dem jeweiligen Personalvertretungsrecht Ihres Landes.

Microsoft hat an dieser Stelle etwas getan, das in Diskussionen mit dem Personalrat hilft: Es gibt ausdrückliche Schutzmaßnahmen gegen Schäden im Arbeitsverhältnis. Ableitungen, Bewertungen oder Urteile über Beschäftigte auf Basis ihrer arbeitsbezogenen Kommunikation – zu Leistung, Haltung, innerem oder emotionalem Zustand oder persönlichen Eigenschaften – sind produktseitig eingeschränkt. Das ersetzt keine Dienstvereinbarung, aber es ist ein belastbarer Baustein darin.

Die Dienstvereinbarung selbst ist der Ort, an dem die Auswertungsfrage abschließend geregelt wird: Wer darf welche Protokolldaten zu welchem Zweck auswerten, in welcher Aggregation, mit welcher Beteiligung. Eine Vereinbarung, die pauschal jede Auswertung verbietet, ist genauso unbrauchbar wie eine, die keine Grenzen kennt – die erste verhindert Fehlersuche, die zweite die Zustimmung. Bausteine, Formulierungen und die typischen Streitpunkte stehen in [Copilot und Personalrat: Bausteine einer Dienstvereinbarung](#).

Kirchliche Träger

Für Einrichtungen in evangelischer oder katholischer Trägerschaft gilt nicht das Landesdatenschutzrecht, sondern DSG-EKD beziehungsweise KDG – mit eigenen Aufsichtsstrukturen und einer Mitarbeitervertretung anstelle des Personalrats. Die Systematik ähnelt der DSGVO stark, die Zuständigkeiten und einzelne Anforderungen weichen ab. Wer eine Einrichtung der Diakonie oder einen Caritas-Verband berät und die kommunale Vorlage einfach übernimmt, produziert ein Dokument mit den richtigen Sätzen und den falschen Adressaten. Die Unterschiede im Detail behandelt [Microsoft 365 in Kirche, Diakonie und Caritas: DSG-EKD, KDG und Mitarbeitervertretung](#).

Auftragsverarbeitung: was im Ordner liegen muss

Die dritte Säule ist die formalste und deshalb die, an der man am schnellsten liefern kann. Die Verarbeitung erfolgt im Auftrag; die vertragliche Grundlage bilden die Produktbestimmungen und das Data Protection Addendum, in denen auch die Zusagen zur Datenresidenz und zur EU-Datengrenze verankert sind. Was Ihre Akte braucht, steht in der folgenden Tabelle – und zwar tatsächlich als Dokument, nicht als Erinnerung an ein Gespräch.

Nachweis	Was darin stehen muss	Wer liefert
Vertrag zur	Produktbestimmungen und Data Protection	Vergabestelle, gemeinsam

Auftragsverarbeitung	Addendum in der zum Vertragsschluss geltenden Fassung, archiviert. Nicht der Link, das Dokument.	mit dem Vertragspartner
Liste der Unterauftragsverarbeiter	Aktueller Stand, inklusive der Modellanbieter. Die Änderungsbenachrichtigung muss bei jemandem ankommen, der sie auch liest.	Datenschutz, mit Wiedervorlage
Zusagen zur Datenresidenz	Belegstelle, dass Copilot als abgedeckte Arbeitslast geführt wird, und der Anmeldeort des Mandanten.	IT-Leitung
Verzeichnis der Verarbeitungstätigkeiten	Ergänzte Bestandseinträge plus neuer Eintrag für Interaktionsdaten, Protokolle und Aufbewahrung.	Datenschutz, mit den Fachämtern
Technisch-organisatorische Maßnahmen	Nicht die allgemeine Anlage des Anbieters, sondern Ihre eigenen: Berechtigungskonzept, Protokollierung, Rollenmodell, Schulungsstand.	IT-Leitung und Organisationsamt
Weisungen und Ansprechpersonen	Wer darf im Namen der Verwaltung Weisungen erteilen, wer wird bei einer Datenschutzverletzung auf welchem Weg erreicht.	Verwaltungsspitze, schriftlich

Ein Hinweis aus der Praxis, der Ärger erspart: Wenn ein kommunales Rechenzentrum oder ein Systemhaus den Mandanten betreibt, entsteht eine Kette. Wer administriert, ist regelmäßig ebenfalls Auftragsverarbeiter und braucht einen eigenen Vertrag samt eigener Beschreibung der Maßnahmen – auch dann, wenn man seit fünfzehn Jahren gut zusammenarbeitet und bislang alles geklappt hat. Wie sich diese Schnittstelle sauber schneiden lässt, steht in [Microsoft 365 und das kommunale Rechenzentrum: Rollen, Schnittstellen, Zweitmeinung](#). Und wer privilegierte Konten sauber trennt, kann in der DSFA an mehreren Stellen kürzer schreiben; das Rollenmodell dazu behandelt [Privilegierte Konten in der Verwaltungs-IT: Rollen, PIM und der Fall des einen Admins](#). Für die vertragliche Seite der Beschaffung ist [Microsoft 365 rechtssicher beschaffen: Vergabe, Leistungsbeschreibung, Rahmenverträge](#) der passende Anschluss.

TIPP • Die Reihenfolge, die Zeit spart

Schreiben Sie die Rechtsgrundlage **vor** der DSFA, nicht umgekehrt. Eine Folgenabschätzung, deren Rechtsgrundlage sich während des Schreibens noch ändert, muss man zweimal schreiben – und die zweite Fassung liest niemand mehr mit derselben Sorgfalt.

Und klären Sie mit dem Personalrat zuerst das Verfahren, dann den Inhalt: Wer wird wann beteiligt, wie oft wird berichtet, wann wird nachgesteuert. Verfahrensklarheit nimmt achtzig Prozent der Spannung aus der inhaltlichen Diskussion, weil niemand mehr befürchten muss, übergangen zu werden.

Die DSFA: Struktur, die trägt

Jetzt zu dem Dokument, das am Ende in der Akte liegt. Vorweg die unpopuläre Wahrheit: Eine DSFA ist kein Formular. Es gibt Vorlagen, sie sind hilfreich, und sie werden regelmäßig so ausgefüllt, dass am Ende ein Dokument entsteht, das formal vollständig und inhaltlich leer ist. Der Unterschied zwischen beidem liegt in Baustein 5 – den Risiken – und daran erkennt eine Aufsichtsbehörde in vier Minuten, welche Sorte Dokument sie vor sich hat.

Schwellwertprüfung: Brauchen Sie überhaupt eine?

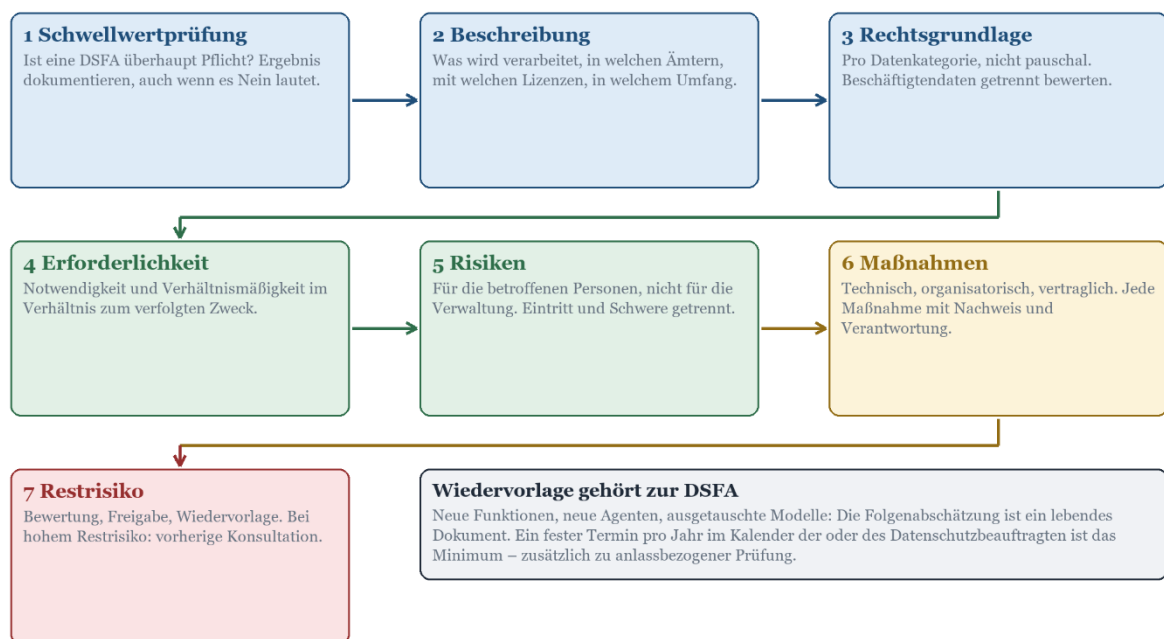
Art. 35 DSGVO verlangt eine DSFA, wenn eine Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Die Aufsichtsbehörden führen dazu

Listen von Verarbeitungen, bei denen eine DSFA verpflichtend ist; diese Listen unterscheiden sich zwischen den Ländern und zwischen öffentlichem und nichtöffentlichem Bereich. Prüfen Sie die Liste Ihrer Aufsichtsbehörde – nicht die eines Nachbarlandes, auch wenn deren Vorlage hübscher formatiert ist.

Kriterium	Bei Copilot in der Verwaltung	Konsequenz
Einsatz neuer Technologien	Ja. Große Sprachmodelle sind in der Breite neu, auch wenn sie sich vertraut anfühlen.	Spricht deutlich für eine DSFA
Umfangreiche Verarbeitung besonderer Kategorien	Häufig ja – Sozialamt, Jugendamt, Gesundheitsamt und Personalverwaltung liegen im selben Mandanten.	Spricht deutlich für eine DSFA
Systematische umfassende Bewertung persönlicher Aspekte	In der Regel nein, sofern Sie keine Auswertung der Nutzung zu Leistungszwecken vorsehen.	In der Dienstvereinbarung ausschließen und das dokumentieren
Beschäftigtendaten mit Auswertungsmöglichkeit	Ja, allein durch Protokollierung und Interaktionsdaten.	Mitbestimmung und eigene Risikobetrachtung
Innovative Nutzung mit begrenzter Nachvollziehbarkeit	Ja. Warum ein Modell genau diese Antwort gibt, lässt sich nicht vollständig erklären.	Transparenzmaßnahmen und Vier-Augen-Prinzip beschreiben
Verarbeitung im Drittland	Grundsätzlich innerhalb der EU-Datengrenze, mit dokumentierten Ausnahmen.	Ausnahmen benennen, nicht verschweigen

Kurz: In den allermeisten Verwaltungen kommt bei einer ehrlichen Schwellwertprüfung eine DSFA-Pflicht heraus. Und selbst wenn nicht – das Ergebnis der Prüfung muss dokumentiert sein. Ein unbeschriebenes Blatt ist keine Verneinung, sondern eine Lücke, und Lücken sind genau das, wonach in einer Prüfung gesucht wird. Wer den Schutzbedarf ohnehin gerade erhebt, erledigt beides in einem Aufwasch; das Vorgehen dazu steht in [Schutzbedarf und Microsoft 365: IT-Grundschutz-Abgleich für die Praxis](#).

Die DSFA in sieben Bausteinen



Skizze 3: Die Reihenfolge zählt. Wer bei Baustein 6 beginnt, schreibt eine Maßnahmenliste – keine Folgenabschätzung.

Die Risiken, die man wirklich schreiben muss

Die häufigste Schwäche in Verwaltungs-DSFAs: Es werden Risiken für die Verwaltung beschrieben – Reputationsschaden, Aufsichtsmaßnahmen, Kosten – statt Risiken für die betroffenen Personen. Die Verordnung meint aber die Menschen, deren Daten verarbeitet werden: die Antragstellerin, den Beschäftigten, das Kind in der Jugendhilfeakte. Die folgende Tabelle zeigt die Risiken, die im Copilot-Kontext tatsächlich tragen, samt der Maßnahmen, die dagegen wirken.

Risiko für betroffene Personen	Maßnahme	Restrisiko
Unbefugte Kenntnisnahme durch Beschäftigte, weil Berechtigungen zu weit gefasst sind	Berechtigungsvereinbarung vor dem Rollout, Suchausschluss oder eingeschränkte Auffindbarkeit für sensible Bereiche, Bericht zur Zugriffs-Governance quartalsweise	Gering bis mittel, abhängig vom Bereinigungsstand
Falsche Sachentscheidung auf Basis einer fehlerhaften Zusammenfassung	Verbindliche Regel: keine belastende Entscheidung ohne Blick in das Originaldokument. Schulung. Kennzeichnung KI-gestützter Entwürfe im Entwurfsstadium	Mittel – verbleibt beim Menschen, nicht bei der Technik
Verarbeitung besonderer Kategorien ohne Erforderlichkeit	Bereichsscharfer Rollout: kein Copilot in Ämtern mit hohem Anteil besonderer Kategorien, solange die Ablage nicht sortiert ist	Gering bei sauberer Abgrenzung
Leistungs- und Verhaltenskontrolle durch Auswertung der Protokolle	Dienstvereinbarung mit ausdrücklichem Auswertungsverbot außer für definierte Sicherheitszwecke, Vier-Augen-Prinzip beim Zugriff auf Protokolle	Gering bei belastbarer Vereinbarung
Verlust der Löschkontrolle, weil Interaktionen an unerwarteter Stelle liegen	Aufbewahrungsrichtlinie für Copilot-Erlebnisse, dokumentierte Löschfristen, Kenntnis der Verzögerung durch die Zwischenspeicherung	Gering, aber mit Fristenpuffer in Auskunftszusagen
Übermittlung außerhalb der EU-Datengrenze durch Websuche oder Modellauswahl	Websuche bewusst konfigurieren, zugelassene Modelle im Mandanten festlegen, Ausnahmen in der DSFA benennen	Gering bei bewusster Konfiguration

Auffällig an dieser Liste: Die meisten Risiken sind keine Copilot-Risiken. Es sind Ablage- und Organisationsrisiken, die durch Copilot lediglich sichtbar und abrufbar werden. Das ist die eigentliche Botschaft an die Verwaltungsspitze – und gleichzeitig das beste Argument für das Vorhaben: Eine Verwaltung, die ihre Berechtigungen sortiert hat, ist auch ohne Copilot besser dran. Nur macht es ohne Copilot niemand.

Freigabe, Beteiligung, Wiedervorlage

Die DSFA wird von der verantwortlichen Stelle durchgeführt, also von der Verwaltungsleitung, unter Einbindung der oder des Datenschutzbeauftragten. Datenschutzbeauftragte beraten und prüfen – sie unterschreiben nicht stellvertretend. Diese Unterscheidung verwischt in kleinen Verwaltungen regelmäßig, und sie fällt spätestens dann auf die Füße, wenn ein Vorgang streitig wird.

Bleibt nach allen Maßnahmen ein hohes Restrisiko, ist die Aufsichtsbehörde vorab zu konsultieren. In der Praxis ist das bei sauber gebautem Copilot-Einsatz die Ausnahme – aber es lohnt sich, den Fall im Dokument zu benennen und die Entscheidung zu begründen, statt ihn zu übergehen. Und

legen Sie eine Wiedervorlage fest. Copilot von heute ist nicht Copilot von in zwölf Monaten: Modelle werden ausgetauscht, Funktionen kommen hinzu, Agenten verändern den Datenfluss. Ein Modellwechsel ändert die vertraglichen Zusagen zu Sicherheit, Datenschutz und Compliance nicht – den Funktionsumfang und damit die Risikobetrachtung aber durchaus.

TIPP • Konzentriert erarbeiten statt im Umlauf verlieren

Eine DSFA lässt sich in wenigen konzentrierten Tagen erarbeiten, wenn die richtigen Personen gleichzeitig im Raum sitzen: IT-Leitung, Organisationsamt, Datenschutz, Personalrat, ein bis zwei Fachämter. Was in dieser Konstellation an einem Vormittag geklärt wird, dauert im Umlaufverfahren vier Monate.

Wie eine solche Konzeptionsphase samt Beschlussvorlage aufgebaut ist, steht in [Microsoft-365-Einführung in der Verwaltung: Konzeptionsphase in 4,5 Tagen und die Beschlussvorlage](#). Wenn Sie dafür externe Begleitung brauchen: [Microsoft 365 Beratung für Verwaltungen](#).

Nachweise, Protokolle und die Grenze zur Akte

Der letzte Fragenblock der oder des Datenschutzbeauftragten betrifft die Nachweisfähigkeit. Er ist der angenehmste, weil die Antworten hier überwiegend technisch und überprüfbar sind – und weil dieselben Nachweise, die der Datenschutz braucht, das Rechnungsprüfungsamt ebenfalls sehen will.

Was protokolliert wird

Interaktionen mit Copilot werden im einheitlichen Überwachungsprotokoll erfasst. Dort steht, wann welches Konto mit welchem KI-Werkzeug interagiert hat, samt Verweisen auf die Dateien, die während der Interaktion herangezogen wurden, und samt der angewandten Vertraulichkeitsbezeichnungen. Der volle Wortlaut der Prompts und Antworten steht dort **nicht** – das Protokoll führt lediglich eine Kennung des Gesprächsverlaufs. Wer den Wortlaut braucht, arbeitet mit den Purview-Werkzeugen für generative KI oder mit eDiscovery.

Diese Trennung ist datenschutzrechtlich sinnvoll und praktisch angenehm: Die Routineprotokollierung erzeugt kein zweites Volltextarchiv sämtlicher Gespräche, und der Zugriff auf den Inhalt ist ein eigener, protokollierter, an Rollen gebundener Vorgang. Genau so sollte es auch in der Dienstvereinbarung stehen. Was daraus für Prüfungen folgt und welche Nachweise eine Verwaltung ohnehin vorhalten sollte, behandelt [Microsoft 365 Audit-Log und Rechnungsprüfung: Nachweise, die Verwaltungen liefern müssen](#).

Aufbewahrung und Löschung der Interaktionen

Prompts und Antworten werden hinter den Kulissen in einem verborgenen Ordner des Postfachs derjenigen Person abgelegt, die das Werkzeug genutzt hat. Dieser Ordner ist weder für die Beschäftigten noch für die Administration direkt zugänglich; er dient dazu, dass Compliance-Verantwortliche die Daten mit eDiscovery durchsuchen können. Aufbewahrungsrichtlinien für Copilot-Erlebnisse steuern, wie lange das gilt – seit der Trennung von den Teams-Chats als eigener Speicherort.

Der Ablauf danach ist bemerkenswert und gehört in jede Auskunftszusage: Nach Ablauf der Frist verschiebt ein Timerjob die Einträge in einen zweiten verborgenen Ordner, wo sie mindestens einen Tag verbleiben, bevor sie endgültig gelöscht werden. Der Timerjob läuft typischerweise alle ein bis sieben Tage. Eine Löschregel mit einem Tag Frist kann deshalb in der Summe rund zwei Wochen brauchen, bis der Eintrag nicht mehr in eDiscovery-Suchen auftaucht. Und: Ein Hold –

aus einem Rechtsstreit, einer Prüfung oder einer laufenden Ermittlung – setzt die endgültige Löschung aus. Aufbewahrung sticht Löschung, immer.

Lebenszyklus einer Copilot-Interaktion



Skizze 4: Zwischen dem Löschen im Chatfenster und der endgültigen Löschung können mehr als zwei Wochen liegen. Planen Sie das in Fristenzusagen ein.

Was in der Oberfläche sichtbar ist, sagt übrigens nichts darüber aus, was im Hintergrund noch existiert. Beschäftigte können ihren Aktivitätsverlauf löschen; der Eintrag verschwindet damit aus der Ansicht, nicht zwingend aus dem Bestand. Wenn Sie in einer Auskunft nach Art. 15 DSGVO oder in einer Löschbestätigung etwas anderes behaupten, behaupten Sie etwas Falsches. Formulieren Sie stattdessen entlang der tatsächlichen Fristen. Wer wissen möchte, wie sich das Zusammenspiel aus Aufbewahrungsrichtlinien im Alltag verhält und was passiert, wenn es aussetzt, findet eine Störungsanalyse in [Wenn die Aufbewahrungsrichtlinie einfach aufhört: SharePoint-Störungsanalyse in der Verwaltung](#).

Wo die Akte anfängt – und Copilot aufhört

WARNUNG · Copilot-Interaktionen sind kein Schriftgut

Ein Prompt ist keine Aktennotiz, und eine Copilot-Antwort ist kein Dokument im Sinne der Schriftgutverwaltung. Was aktenrelevant ist, muss bewusst in die Akte gelegt werden – mit Zuordnung zum Aktenplan, Aufbewahrungsbezeichnung und allem, was später für die Aussonderung gebraucht wird.

Die Grenze zur E-Akte richtet sich nach dem E-Government-Recht Ihres Landes. SharePoint mit Aufbewahrungsbezeichnungen ist eine strukturierte Ablage; ob und unter welchen Bedingungen daraus ein aktenführendes System wird, entscheidet nicht der Hersteller, sondern das Landesrecht. Behandeln Sie diese Frage getrennt von der Copilot-Frage, sonst vermischen sich zwei Diskussionen mit unterschiedlichen Zuständigkeiten – und am Ende diskutiert die Registratur über Sprachmodelle.

Zum Weiterlesen: [Schriftgutverwaltung mit Microsoft 365: Vom Aktenplan zur Aufbewahrungsbezeichnung](#), [SharePoint als E-Akte? Was geht, was nicht und wo die Grenze nach Landesrecht liegt](#) und [Aufbewahrung und Aussonderung mit Purview: Fristen, Disposition, Vernichtungsnachweis](#).

Betroffenenrechte in der Praxis

Auskunft, Berichtigung, Löschung, Einschränkung: Die Rechte gelten unverändert, auch für Interaktionsdaten. Praktisch heißt das, dass Ihr Auskunftsprozess um eine Suchquelle erweitert werden muss. Wer heute bei einem Auskunftersuchen Postfach, Fachverfahren und Ablage

durchsucht, muss künftig auch die Copilot-Interaktionsdaten einbeziehen – technisch über dieselben eDiscovery-Werkzeuge, organisatorisch über eine Zeile mehr in der Checkliste.

Ein großer Landschaftsverband, mit dem wir dieses Thema durchgespielt haben, hat daraus die pragmatischste Lösung gemacht, die mir bisher begegnet ist: eine Aufbewahrungsfrist für Copilot-Interaktionen, die kurz genug ist, um den Auskunftsaufwand klein zu halten, und lang genug, um eine Fehleranalyse zu ermöglichen. Das Ergebnis war eine dreistellige Zahl von Tagen, verbindlich beschlossen, in der Dienstvereinbarung verankert und in der DSFA begründet. Nicht elegant. Aber verteidigungsfähig, und das ist am Ende die Währung.

Damit die Regeln in den Fachämtern ankommen, braucht es außerdem Vermittlung: Was darf man hineinschreiben, was nicht, wann muss ins Original geschaut werden, was passiert mit den Protokollen. Dafür gibt es [Microsoft 365 Schulung für Verwaltungen](#) – denn eine Dienstvereinbarung, die niemand kennt, ist eine Aktennotiz mit Unterschriften.

Häufige Fragen

Brauchen wir zwingend eine Datenschutz-Folgenabschätzung?

In den meisten Verwaltungen ja. Die Kombination aus neuer Technologie, umfangreicher Verarbeitung besonderer Kategorien im selben Mandanten und Beschäftigtendaten mit Auswertungspotenzial erreicht die Schwelle regelmäßig. Maßgeblich ist die Liste Ihrer Aufsichtsbehörde. Und selbst wenn die Prüfung Nein ergibt: Das Ergebnis muss dokumentiert sein.

Werden unsere Daten zum Training verwendet?

Nein. Prompts, Antworten und die über Microsoft Graph beziehungsweise die semantische Indizierung erreichten Daten werden nicht zum Training der Basismodelle verwendet. Die Missbrauchsüberwachung mit menschlicher Sichtung ist für die Copilot-Dienste ausgewählt. Achten Sie auf die Ausnahme: Optionales Feedback ist eine eigene Verarbeitung und lässt sich zentral steuern.

Bleiben alle Daten in der EU?

Für Mandanten mit Anmeldeort in der EU ist Copilot ein Dienst innerhalb der EU-Datengrenze; Datenverkehr aus der EU bleibt darin. Es gibt dokumentierte Ausnahmen – Modelle einzelner Unterauftragsverarbeiter sind derzeit ausgenommen, und wer Multi-Geo gebucht hat, fällt aus dem Geltungsbereich heraus. Die Websuche führt abgeleitete Suchbegriffe nach draußen und ist abschaltbar. Diese drei Punkte gehören in die DSFA, nicht in eine Fußnote.

Kann Copilot die Personalakte lesen?

Nur, wenn das anfragende Konto sie lesen darf. Copilot vergibt keine Rechte und umgeht keine. Die unangenehme Rückseite: In vielen gewachsenen Umgebungen dürfen mehr Konten mehr lesen, als irgendjemand annimmt. Das ist ein Berechtigungsproblem mit einem neuen Scheinwerfer, kein KI-Problem.

Reicht eine Einwilligung der Beschäftigten als Rechtsgrundlage?

In aller Regel nicht. Die Freiwilligkeit ist im Beschäftigungsverhältnis schwer zu begründen, und ein Werkzeug, das nur für die Zustimmenden funktioniert, ist organisatorisch kaum handhabbar. Der übliche Weg ist die Kombination aus landesrechtlicher Grundlage und Dienstvereinbarung nach Art. 88 DSGVO.

Kann der Personalrat die Einführung blockieren?

Er kann sie verzögern, und er hat dafür meist gute Gründe, wenn die Auswertungsfrage ungeklärt ist. Konstruktiver ist es, die Mitbestimmung als Bauplan zu nutzen: Was darf ausgewertet werden, von wem, zu welchem Zweck, mit welcher Kontrolle. Wer diese vier Fragen vorab beantwortet, verhandelt über Formulierungen statt über Grundsatzfragen.

Müssen wir Copilot-Chats in die Akte nehmen?

Nein, nicht als solche. Aktenrelevant ist das Ergebnis, wenn es Grundlage einer Entscheidung wird – und dann als ordentliches Dokument mit Zuordnung zum Aktenplan, nicht als Gesprächsprotokoll. Ob und wie eine SharePoint-Ablage aktenführend sein kann, richtet sich nach dem E-Government-Recht Ihres Landes.

Was ändert der EU-KI-Rechtsakt daran?

Er kommt als zweite Ebene hinzu und ersetzt die datenschutzrechtliche Prüfung nicht. Der Zeitplan hat sich verschoben: Mit dem im Juli 2026 in Kraft getretenen Omnibus-Rechtsakt wurden die Pflichten für eigenständige Hochrisiko-Systeme auf Dezember 2027 verlegt, für in Produkte eingebettete Systeme auf August 2028. Die Anforderungen an KI-Kompetenz und Transparenz greifen bereits. Für Verwaltungen heißt das: nicht abwarten, sondern Schulung und Dokumentation jetzt aufsetzen – und die Einstufung des eigenen Einsatzszenarios in der DSFA gleich mitdokumentieren.

Sollen wir auf eine souveräne Plattform warten?

Wenn Sie heute einen Bedarf haben, lösen Sie ihn heute. Bauen Sie stattdessen Wechselfähigkeit ein: klare Datenhaltung, dokumentierte Konfiguration, Ausstiegsregelungen in der Vergabeunterlage. Wer auf einen Termin wartet, den er nicht selbst setzt, wartet erfahrungsgemäß länger als geplant – und hat am Ende weder das eine noch das andere.

Fazit

Die Liste der oder des Datenschutzbeauftragten ist beantwortbar. Sie ist sogar erstaunlich gut beantwortbar, weil Microsoft an den technischen Punkten dokumentiert und prüfbar geliefert hat: Verarbeitung innerhalb der EU-Datengrenze mit benannten Ausnahmen, kein Training der Basismodelle, ein Berechtigungsmodell ohne Sonderweg, Protokollierung ohne Volltextarchiv, steuerbare Aufbewahrung. Was nicht geliefert wird und auch nicht geliefert werden kann, ist die Rechtsgrundlage, die Dienstvereinbarung, das Berechtigungskonzept und die Entscheidung, in welchen Fachämtern das Werkzeug überhaupt etwas zu suchen hat.

Genau dort liegt die Arbeit. Und ehrlich betrachtet ist es Arbeit, die ohnehin ansteht: Eine Verwaltung, die nicht weiß, wer auf welche Ablage zugreifen darf, hat auch ohne künstliche Intelligenz ein Problem – sie merkt es nur nicht. Copilot ist in dieser Hinsicht kein Risiko, sondern ein unangenehm gut funktionierendes Diagnosewerkzeug. Das ist die schlechte Nachricht für den Zeitplan und die gute für die Organisation.

Wenn Sie eine Reihenfolge brauchen: Schutzbedarf klären, Berechtigungen messen, Rechtsgrundlage schreiben, Personalrat einbinden, DSFA konzentriert mit den richtigen Leuten erarbeiten, bereichsscharf pilotieren, protokollieren, nachsteuern. Nicht schnell, aber geradeaus – und am Ende steht ein Dokument, das eine Prüfung übersteht, statt einer Präsentation, die einen Verwaltungsvorstand beeindruckt hat.

- › [Microsoft 365 in der öffentlichen Verwaltung](#)
- › [Oversharing im Verwaltungs-Tenant: Warum Copilot die Personalakte findet](#)
- › [Copilot und Personalrat: Bausteine einer Dienstvereinbarung](#)
- › [Schutzbedarf und Microsoft 365: IT-Grundschutz-Abgleich für die Praxis](#)
- › [Microsoft 365 in der Kommune: Was Sie wirklich entscheiden müssen \(und was nicht\)](#)
- › [Microsoft 365 Lizenzen für Verwaltungen: E3, E5, F3 und die Behördenkonditionen](#)
- › [Dokumenten-KI in der Verwaltung: Posteingang, Anträge und Klassifizierung](#)
- › [Gäste in Teams und SharePoint: Planungsbüros, Träger und Gremienmitglieder sicher einbinden](#)
- › [Conditional Access für Verwaltungen: Regelwerk für Rathaus, Bauhof und Homeoffice](#)
- › [Microsoft 365 Audit-Log und Rechnungsprüfung: Nachweise, die Verwaltungen liefern müssen](#)