Microsoft 365 datenschutzkonform? Drei Behörden sagen: Ja – unter Bedingungen

Kann Microsoft 365 datenschutzkonform eingesetzt werden? Die Datenschutzkonferenz hatte das Ende 2022 bezweifelt. Immer wieder wird dies streitig diskutiert. Mittlerweile kommen gleich drei behördliche Stimmen zu einem differenzierteren Ergebnis: Der Hessische Beauftragte für Datenschutz und Informationsfreiheit (HBDI) in einem knapp 140-seitigen Bericht, der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) nach zweijähriger technisch-organisatorischer Projektbegleitung und der Europäische Datenschutzbeauftragte (EDSB) im Rahmen seiner Prüfung des vergleichbaren M365-Einsatzes bei der EU-Kommission. Die Kernbotschaft ist einheitlich: Der Einsatz ist datenschutzkonform möglich – aber nur mit erheblichem Eigenengagement der Verantwortlichen. Welche Anforderungen die Berichte formulieren und welche kritischen Punkte offenbleiben, fassen wir hier zusammen.

Ausgangslage: Microsoft 365 zwischen Praxis und Aufsicht

Microsoft 365 ist für viele Unternehmen und Behörden ein zentrales Arbeitsmittel. Gleichzeitig ist umstritten, ob die Software die Anforderungen der DSGVO an eine datenschutzkonforme Auftragsverarbeitung erfüllt. Die Datenschutzkonferenz (DSK) hatte Ende 2022 die Auffassung vertreten, dass dies nicht der Fall sei – insbesondere, weil nicht transparent sei, welche Daten Microsoft zu welchen Zwecken verarbeite, und weil die Nutzung zwangsläufig mit Datenübermittlungen in die USA verbunden sei.

Die Feststellung der DSK führte zu erheblicher Verunsicherung in der Praxis. In Hessen führte der HBDI ein aufsichtsbehördliches Verfahren gegen eine nicht-öffentliche Stelle, das als Auslöser für die Gespräche mit Microsoft diente. Im November wurde dann ein umfassender Bericht zum Einsatz von Microsoft 365 veröffentlicht. In Hamburg begleitet der HmbBfDI seit Mitte 2023 das Projekt „BestCloud-Basis" der Senatskanzlei – mit dem Ziel, das vergleichbare Produkt

M365 für die Hamburger Verwaltung datenschutzkonform einzuführen.

Auftragsverarbeitung: Was die DSGVO verlangt

Microsoft muss beim Betrieb von Microsoft 365 als Auftragsverarbeiter tätig werden, um für Unternehmen umfassend einsetzbar zu sein, da regelmäßig keine Erlaubnisgrundlage für eine umfassende Übermittlung von Daten an Dritte gegeben ist. Die datenschutzrechtliche Verantwortung verbleibt beim Kunden – dem Unternehmen oder der Behörde, die die Software einsetzt. Wenn Microsoft als Auftragsverarbeiter tätig wird, benötigt der Verantwortliche für die Übermittlung keine eigene Erlaubnisgrundlage. Das setzt aber einiges voraus. Art. 28 DSGVO stellt an dieses Verhältnis konkrete Anforderungen, insbesondere:

- einen Vertrag, der Gegenstand, Dauer, Art und Zweck der Verarbeitung festlegt (Art. 28 Abs. 3 S. 1 DSGVO),
- die Verarbeitung nur auf dokumentierte Weisung des Verantwortlichen (Art. 28 Abs. 3 S. 2 lit. a DSGVO),
- geeignete technische und organisatorische Maßnahmen für ein angemessenes Schutzniveau (Art. 28 Abs. 3 S. 2 lit. c i.V.m. Art. 32 DSGVO),
- den Einsatz von Subunternehmern nur mit vorheriger Zustimmung (Art. 28 Abs. 2 DSGVO) und
- die Unterstützung bei einer Datenschutz-Folgenabschätzung, soweit erforderlich (Art. 28 Abs. 3 S. 2 lit. f DSGVO).

Ob Microsoft diese Anforderungen erfüllt, war der Kern der Debatte. Eine besondere Rolle spielte dabei die Frage, ob Microsoft für bestimmte Verarbeitungen – namentlich die Aggregation anonymisierter Daten für eigene „Geschäftstätigkeiten" – auf Weisung des Verantwortlichen agiert oder womöglich doch als eigener Verantwortlicher zu eigenen Zwecken handelt. Der HBDI kommt insoweit zu dem Ergebnis, dass Microsoft hierfür nur aggregierte und anonymisierte Daten verwendet und diese Verarbeitung entweder nicht der DSGVO unterfällt oder datenschutzrechtlich vertretbar ist. Auch der HmbBfDI sieht das ähnlich: Microsoft verarbeite ausschließlich pseudonymisierte Telemetrie- und Diagnosedaten zur Verbesserung der

Dienste und Fehlerbehebung. Die Rückführbarkeit auf einzelne Personen sei beinahe ausgeschlossen. Damit ist die Richtung klar, aber nicht final geklärt.

Drittlandtransfer: Lage wesentlich entschärft, aber nicht vollständig gelöst

Ein weiterer zentraler Kritikpunkt der DSK betraf die Datenübermittlung in die USA. Hier hat sich die Lage seit 2022 wesentlich verändert. Auf Grundlage des EU-US-Data Privacy Framework sind Übermittlungen an zertifizierte US-Unternehmen wie Microsoft seit 2023 zulässig. Zudem hat Microsoft seine Datenverarbeitung technisch so umgestellt, dass sie ganz überwiegend innerhalb des Europäischen Wirtschaftsraums stattfindet und bietet sog. EU-Boundaries an.

Der HBDI kommt daher zu dem Ergebnis, dass der Drittlandtransfer nur noch einen äußerst geringen Teil der Verarbeitung betrifft und durch geeignete Schutzinstrumente abgesichert ist. Auch der EDSB hat seine Untersuchung des M365-Einsatzes bei der EU-Kommission im Juli 2025 abgeschlossen und keine Verstöße gegen die Datenschutzverordnung der EU-Organe festgestellt – u.a. deshalb, weil Microsoft umfangreiche Korrekturmaßnahmen umgesetzt hat.

Vollständig gelöst ist das Risiko allerdings nicht: Microsoft hat in einer öffentlichen Anhörung vor dem französischen Senat im Juni 2025 eingeräumt, dass eine Offenlegung personenbezogener Daten auf Anordnung der US-Regierung ohne Zustimmung des Verantwortlichen für die Zukunft nicht vollständig ausgeschlossen werden könne – auch wenn dies in der Vergangenheit noch nie vorgekommen sei. Der HBDI empfiehlt Verantwortlichen daher, zu evaluieren, welche Datenkategorien von einer solchen Offenlegung betroffen sein könnten, und technische sowie organisatorische Maßnahmen zur Risikominimierung zu ergreifen.

Der HmbBfDI geht einen Schritt weiter: Er hat die Senatskanzlei zur Entwicklung einer **Exit-Strategie** aufgefordert. Diese setzt sich mit dem Szenario auseinander, dass die Daten kurzfristig aus der Microsoft-Cloud zurückgeholt werden müssen.

Handlungsempfehlungen des HBDI

Der Bericht des HBDI stellt fest, dass ein datenschutzkonformer Einsatz möglich ist – allerdings nur, wenn auch die Kunden als Verantwortliche ihre Pflichten erfüllen. Die wichtigsten Empfehlungen:

- **Microsoft 365 als Betriebsmittel einordnen**: Die Software selbst ist ein technisches Hilfs- oder Betriebsmittel, mit dem unterschiedliche Verarbeitungstätigkeiten durchgeführt werden. Für die konkreten Verarbeitungen, die mit der Software vorgenommen werden, ist jeweils eine eigene datenschutzrechtliche Bewertung im Kontext des jeweiligen Einsatzzwecks erforderlich. Es empfiehlt sich, eine Beschreibung von Microsoft 365 als Betriebsmittel vorzuhalten und im Verzeichnis der Verarbeitungstätigkeiten darauf zu verweisen.

- **Dokumentation und Nachweispflichten erfüllen**: Verantwortliche müssen ein vollständiges Verzeichnis der Verarbeitungstätigkeiten anlegen und aktualisieren. Soweit erforderlich, ist eine Datenschutz-Folgenabschätzung für die konkreten Verarbeitungen durchzuführen. Dabei sollten die von Microsoft bereitgestellten Materialien – insbesondere die Interpretationshilfe zum DPA, die Taxonomie und das M365-Kit – als Grundlage herangezogen werden.

- **Customer Lockbox und technische Konfiguration nutzen**: Im Kontext der Weisungsbindung und Offenlegung (Kritikpunkt 3 der DSK) empfiehlt der HBDI, den Einsatz des Zusatzprodukts „Customer Lockbox" zu prüfen, mit dem Kunden den Zugriff von Microsoft-Mitarbeitern auf Inhaltsdaten kontrollieren und genehmigen können. Das Tool ist mit höheren Lizenzgebühren verbunden. Unabhängig davon sollte die Software so konfiguriert werden, dass insbesondere Diagnose-Daten nur im erforderlichen Umfang erhoben und nur in pseudonymisierter Form an Microsoft übermittelt werden. Die konkrete Konfiguration ist sauber zu dokumentieren.

- **Kontinuierliche Überprüfung etablieren**: Microsoft 365 wird laufend um neue Funktionen erweitert – etwa jüngst das KI-Tool Copilot. Der HBDI empfiehlt, einen definierten Prüfprozess vor Einführung neuer Produkte sowie eine laufende Überwachung bestehender Dienste einzurichten, um Änderungen

an Diensten (Updates, Funktionsänderungen, Anbieterwechsel) systematisch auf ihre datenschutzrechtlichen Auswirkungen hin zu bewerten.

- **Alternativen prüfen – digitale Souveränität stärken:** Der HBDI empfiehlt, stets auch alternative, möglichst europäische und datenschutzfreundliche Lösungen als Bestandteil einer nachhaltigen IT-Strategie zu evaluieren. Der Bericht begründet dies ausdrücklich mit der Notwendigkeit, die Abhängigkeit von einzelnen Herstellern zu verringern und – angesichts geopolitischer Entwicklungen – die Fähigkeiten von Drittstaatenakteuren, politischen Druck auszuüben, zu minimieren. Verwiesen wird unter anderem auf die Delos Cloud für den öffentlichen Dienst.

Einordnung

Der Bericht des HBDI sendet ein klares Signal, das dem Arbeitsalltag vieler Behörden und Unternehmen entgegenkommt und der Praxis in vielen, datenschutzrechtlich fundiert aufgestellten Unternehmen entspricht. Mit einer differenzierten Konfiguration und Dokumentation können die Risiken erheblich verringert werden.

Auch wenn die Einschätzung der DSK von 2022, wonach ein datenschutzkonformer Betrieb auf Grundlage des damaligen DPA nicht nachgewiesen werden könne, nicht formal aufgehoben worden ist, kommt dem Bericht des HBDI erhebliches Gewicht zu: Der HBDI argumentiert umfassend und plausibel und stützt seine abweichende Bewertung auf die zwischenzeitlichen Veränderungen – insbesondere die Fortentwicklung des DPA, den EU-US-Data Privacy Framework und die EU-Datengrenze von Microsoft. Und auch die DSK hat eine Neubewertung der Zulässigkeit von Microsoft 365 in Auftrag gegeben. Das Ergebnis dieser Neubewertung wurde aber bislang nicht veröffentlicht.

Wer die empfohlenen Maßnahmen umsetzt, verfügt über eine deutlich verbesserte Argumentationsgrundlage für den datenschutzkonformen Einsatz von Microsoft 365 – jedenfalls Bußgeldrisiken reduzieren sich dadurch enorm.

Für alle weiteren Fragen rund um das Datenschutzrecht stehen Ihnen gerne zur Verfügung

Dr. Kristina Schreiber
+49 221 65065-337
kristina.schreiber@loschelder.de

Dr. Simon Kohm
+49 221 65065-200
simon.kohm@loschelder.de

Dennis Pethke, LL.M.
+49 221 65065-337
dennis.pethke@loschelder.de

Rebecca Moßner
+49 221 65065-465
rebecca.mossner@loschelder.de

Impressum

LOSCHELDER RECHTSANWÄLTE
Partnerschaftsgesellschaft mbB
Konrad-Adenauer-Ufer 11
50668 Köln

Tel. +49 (0)221 65065-0, Fax +49 (0)221 65065-110
info@loschelder.de
www.loschelder.de