

DATENSCHUTZ- BERATER

» Ihr zuverlässiger Partner für Datenschutz und Datensicherheit

Chefredakteur: Dr. Carlo Piltz

Schriftleitung: Prof. Dr. Alexander Golland, Tilman Herbrich, Philipp Quiel, Laurenz Strassemeyer

Editorial

Philipp Quiel

Die Zeit für den datenschutzrechtlichen Frühjahrsputz

Seite 101

Stichwort des Monats

Dr. habil. Silke Jandt

Wer kontrolliert die Einhaltung der KI-VO? Gesetzentwurf zum KI-MIG vorgelegt

Seite 102

Datenschutz im Fokus

Dr. Carlo Piltz und Ilia Kukin

Werbung mit „DSGVO-konform“: Wo liegen die Grenzen des Zulässigen?

Seite 106

Tilman Herbrich und David Wagner

KI-Agenten im E-Commerce: Ein früher Blick auf datenschutzrechtliche Herausforderungen

Seite 110

Laurenz Strassemeyer

Sensible Daten beim KI-Training und KI-Testing – Das Verbot gilt. Die Rechtfertigung auch.

Seite 114

Aktuelles aus den Aufsichtsbehörden

Alexandra Rath und Tom Vincent Kuhnert

Europäischer Datenschutzausschuss zieht Bilanz zum Umsetzungsstand des Rechts auf Löschung

Seite 120

Dr. Nina Herbort

Gastzugang reloaded: EDSA Empfehlungen zur Einrichtung von Nutzerkonten

Seite 124

Dr. Olaf Koglin

HmbBfDI: Einsatz von Microsoft 365 ist bei nichtsensiblen Daten vertretbar

Seite 129

Rechtsprechung

Guido Aßhoff

Wenn Löschen zum DSGVO-Verstoß wird: Warum man bei Art.-15-Anfragen klare Löschroutinen definieren sollte

Seite 131

Dr. Dominik Sorber und Dr. Christina Knoepffler

Entgelttransparenz und Datenschutz – Gegner oder Team?

Seite 133

Service

Jan Spittka

Faßner: Der datenschutzrechtliche Schadenersatzanspruch nach Art. 82 DS-GVO

Seite 135

▪ **Nachrichten** Seite 104

Dr. Olaf Koglin

HmbBfDI: Einsatz von Microsoft 365 ist bei nicht-sensiblen Daten vertretbar

Im Frühjahr ist Hochsaison für Tätigkeitsberichte der Aufsichtsbehörden. Damit werden auch Informationen zu Prüfungen bei konkreten Produkten – wie denen von Microsoft – veröffentlicht. Der Bericht des BayLDA gab einzelne Hinweise zu Outlook und Exchange. Der Bericht aus Sachsen enthielt keine konkreten Punkte zu Microsoft 365 (M365). Der Tätigkeitsbericht aus Hamburg enthält hingegen eine ausführliche Beschreibung einer Projektprüfung und der individuellen Vereinbarungen mit Microsoft.

Der Tätigkeitsbericht des HmbBfDI

In seinem Tätigkeitsbericht 2025 hat der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) ausführlich die datenschutzrechtlichen Fragestellungen bei der Nutzung von M365 in der hamburgischen Verwaltung geschildert (use365.ms/HHTB). Hiernach „ist der Einsatz bei nichtsensiblen Daten vertretbar.“

Damit setzt sich ein Wandel bei den Aufsichtsbehörden fort, der 2024 mit einer Darstellung des niedersächsischen Landesbeauftragten für Datenschutz (LfD-NI) begonnen hatte und auch jüngst bei dem ausführlichen Gutachten des Hessischen Beauftragten für Datenschutz und Informationsfreiheit (HBDI) zu beobachten war: Im Gegensatz zu u. a. den früheren Entscheidungen der Datenschutzkonferenz des Bundes und der Länder lautet der Tenor nicht mehr, dass ein datenschutzkonformer Einsatz nicht möglich sei. Vielmehr lauten die Überschriften „Microsoft 365 kann datenschutzkonform genutzt werden“ (so der HBDI) oder „ist bei nichtsensiblen Daten vertretbar“ (so der HmbBfDI).

Zu beachten ist dabei, dass der Einsatz einer Software oder eines Software-as-Service-Dienstes niemals pauschal rechtskonform oder unzulässig ist. Vielmehr kommt es auf die zu verarbeitenden Daten, technische und organisatorische Maßnahmen (darunter die Einstellungen in den Admin-Centern von M365), vertragliche Regelungen und weitere Aspekte an, zB der Stellung des Verantwortlichen als Behörde.

Zu Recht setzt sich immer mehr die Erkenntnis durch, dass M365 lediglich ein Betriebsmittel, aber nicht die Datenverarbeitung selbst darstellt. Zu bewerten ist also nicht das Produkt M365, sondern die damit jeweils durchgeführte Datenverarbeitung.

M365-Projekt in Hamburg: „BestCloudBasis“

Ein umfangreiches Kapitel des Tätigkeitsberichts widmet sich dem Einsatz von „M365 in der Verwaltung“ (Kap. III.5, S. 52 ff.). Konkret geht es um das Projekt „BestCloudBasis“ der Hamburger Senatskanzlei, bei dem die Einführung von M365 für die Verarbeitung von Daten mit normalem

Schutzbedarf geprüft wurde. Hierbei hat der HmbBfDI die Senatskanzlei seit mehreren Jahren begleitet.

Besonderheiten im „Hamburger Modell“

Anders als die meisten anderen Verantwortlichen haben manche Bundesländer und Konzerne die Möglichkeit, ihre Verträge mit Microsoft individuell nachzuverhandeln. Ähnlich wie bei den Bewertungen vom HBDI und dem Europäischen Datenschutzbeauftragten (EDSB) existieren auch bei der Senatskanzlei Zusatzvereinbarungen zum Vertragswerk, insbesondere zum „Data Protection Addendum“ von Microsoft. Dies ist das zentrale Datenschutzschutz-Dokument, das für die Nutzung von M365 unter anderem eine Vereinbarung über die Auftragsverarbeitung i. S. d. Art. 28 Abs. 3 Satz 1 DSGVO enthält und Standarddatenschutzklauseln i. S. d. Art. 46 Abs. 2 lit. c DSGVO einbindet.

Einige der von der Hamburger Senatskanzlei individuell ausgehandelten Punkte (vgl. S. 54 des Tätigkeitsberichts) sind bereits aus anderen Zusatzvereinbarungen bekannt:

- Stärkung der Weisungsbefugnis des Auftraggebers und
- Zusicherungen zur Einhaltung der DSGVO sowie
- Vorrang des EU-Rechts bei Drittstaatenübermittlungen

Zudem wurden „umfangreiche Dokumentationen“ bereitgestellt; neben der Datenschutz-Folgenabschätzung werden u. a. Feinkonzepte zu den M365-Diensten und „Sicherheits- und Governancekonzepte“ genannt.

EU Data Boundary: Wieder EU statt EFTA

Eine interessante Individualvereinbarung modifiziert das Microsoft-Konzept der „EU Data Boundary“. Hierbei handelte es sich um eine Zusage von Microsoft, den Großteil der Kundendaten nur in der EU zu verarbeiten. Im Rahmen der letzten Änderungen wurde dies jedoch auf die Europäische Freihandelszone (EFTA) erweitert und schließt somit neben den EWR-Ländern auch die Schweiz als möglichen Datenspeicherort mit ein. Damit wurde das „EU Data Boundary“-Programm sozusagen zu einer „EFTA Data Boundary“ gelockert. Mit einer Zusatzklausel hat die Senatskanzlei die Grenzen des Programms wieder auf die EU beschränkt.

Telemetrie- und Diagnosedaten

Der HmbBfDI hat sich auch ausführlich mit den von Microsoft erhobenen Telemetrie- und Diagnosedaten und der Nutzung von (Kunden-)Daten für eigene Zwecke des Anbieters befasst. Dies ist seit Jahren ein zentraler Kritikpunkt an M365. Der HmbBfDI bewertet verbleibende Risiken bei diesen pseudonymisierten Daten als gering, hält Details u. a. zu Reports und zu Anonymisierungsverfahren aber noch für klärungsbedürftig.

Drittlandtransfers

Ein „Dauerbrenner“ bei der Kritik an US-Dienstleistern ist die Frage des etwaigen Transfers von Daten in Drittländer, insbesondere die USA. Auch dieses Thema wurde vom HmbBfDI ausführlich behandelt. Mit dem Konzept der EU Data Boundary (s.o.), vertraglichen Vereinbarungen und dem EU-US Data Privacy Framework wird die Problematik laut HmbBfDI „zumindest derzeit ausreichend adressiert.“ Als Maßnahme soll nicht nur die weitere Entwicklung beobachtet werden: Auf Aufforderung der Aufsichtsbehörde wurde zusätzlich eine Exit-Strategie entwickelt.

Einsatz von M365 für sensible Daten

Ausdrücklich außen vor gelassen war die Bewertung von Daten mit hohem Schutzbedarf. Als Beispiele werden hierfür Rechner der Polizei oder von Sozialträgern genannt. Gemeint sind mit „sensiblen Daten“ also wohl nicht schon Daten der normalen Verwaltung, die nur gelegentlich Daten i. S. v. Art. 9 Abs. 1 DSGVO enthalten. Auch für die genannten Bereiche mit hohem Schutzbedarf scheint der Einsatz von M365 möglich zu sein, wenn sie besonders gegen die missbräuchliche Einsichtnahme oder Verwendung durch Unberechtigte etc. geschützt werden. Entsprechende Voreinstellungen und Multi-Faktor-Authentifizierung bleiben Gegenstand weiterer Prüfungen (S. 53, 56 und 57 des Tätigkeitsberichts).

Nutzung von AI und Copilot

Der Tätigkeitsbericht geht auch auf die KI-Nutzung in M365 ein. Zu den individuell mit Microsoft vereinbarten Klauseln gehört der „Ausschluss der Nutzung von Kundendaten für das Training von Künstlicher Intelligenz, um eine unautorisierte Weiterverwendung der Daten zu verhindern“ (S. 54).

Entsprechende Zusagen gibt es von Microsoft zwar bereits in „Committments“ und anderen Stellen. Hier erscheint es aber sehr gut nachvollziehbar, eine solche wichtige Regelung individuell, eindeutig und unveränderbar zu vereinbaren. Denn gerade bei Copilot ändert Microsoft Produktumfang und -bezeichnungen in sehr hoher Frequenz. Dies ist bei innovativen Produkten verständlich, begründet aber auf der Kundenseite auch ein Bedürfnis nach zusätzlicher Klarheit.

So hat Microsoft jüngst angekündigt, die erst Anfang 2025 eingeführte Nomenklatur von „Microsoft 365 Copilot“ und „Microsoft 365 Copilot Chat“ erneut zu verändern und bestimmte Anwendungen unter „M365 Copilot Basic“ bzw. „M365 Copilot Premium“ firmieren zu lassen (use365.ms/CopilotBasic). Dies zeigt gerade für den Copilot-Bereich, dass – abhängig von der Sensibilität der Daten und Anwendungsfälle – eine engmaschige datenschutzseitige Betreuung nötig sein kann.

Folgen für die Praxis

Wie schon bei den vorangegangenen aufsichtsbehördlichen Stellungnahmen ist die positive Positionierung des HmbBfDI natürlich für diejenigen Verantwortlichen erfreulich, die M365 einsetzen wollen. Auf den zweiten Blick zeigen sich dann jedoch arbeitsintensive Details: Selbstverständlich ergibt sich aus der Prüfung des HmbBfDI keine pauschale „Freigabe“ für andere Verantwortliche. Erforderlich ist eine Bewertung am konkreten Fall, wobei der HmbBfDI zu Recht aufzeigt, dass dabei nach der Sensibilität der Daten zu differenzieren ist. Der HmbBfDI weist auch auf weitere Aktivitäten bzgl. Telemetriedaten und Drittlandtransfer hin (s.o.).

Wie schon bei den Bewertungen von LfD-NI, EDSB und HBfDI setzt sich der Trend zur „Geheimwissenschaft“ über die individuellen Microsoft-Verträge der öffentlichen Stellen fort: Aus einem Statement von Aufsichtsbehörden über die Zulässigkeit der Datenverarbeitung in M365 kann für diejenigen, die die vertraulichen Verträge der öffentlichen Hand nicht kennen, nie rechtssicher herausgelesen werden, ob die Aussagen auch für die Nutzung unter Standard-Verträgen von Microsoft gelten soll. Abhängig von Umfang der Nutzung und Sensibilität der Daten kann der Einsatz von M365 also viel Aufwand erfordern; der HmbBfDI nennt für die Senatskanzlei eine Menge an Dokumenten und Konzepten. Für Standardnutzungen gibt es hierzu jedoch etliche – auch kostenlose – Muster, an denen sich Verantwortliche und ihre Datenschutzbeauftragten orientieren können. Wie auch bei anderen komplexen und ständigen Änderungen unterworfenen Software-as-a-Service-Angeboten muss der Verantwortliche sich jedoch laufend informieren und die Details seiner Nutzung und seiner Dokumentation anpassen. Mit entsprechenden Maßnahmen ist der Einsatz von M365 gut vertretbar, wie die Aufsichtsbehörden bestätigen.

Autor: Rechtsanwalt Dr. Olaf Koglin ist Geschäftsführer des Datenschutzdienstleisters LegalCheck 365 GmbH, der standardisierte Lösungen zum Einsatz von M365 bereitstellt. Er berät vornehmlich zu Fragen des Einsatzes von Cloud-Diensten und künstlicher Intelligenz aus rechtlicher und Compliance-Sicht.

