

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

Laurenz Strassemeyer

Digital-Omnibus: Kleines Update, (keine) große Folgen?

Seite 325

Stichwort des Monats

Dr. Olaf Koglin

HBDI: „Microsoft 365 kann datenschutzkonform genutzt werden“ – aber was ist dafür erforderlich?

Seite 326

Datenschutz im Fokus

Erdem Durmus

Software-Tests mit Echtdateien – Möglichkeiten, datenschutzfreundliche Alternativen und Pflichten

Seite 333

Jelisaweta Verbizkaja und Sebastian Laoutoumai

Das Verhältnis der datenschutzrechtlichen Regelungen zwischen der DSGVO und DOR-Verordnung

Seite 337

Christian Niemeier

„Emotion as a Service“ als Grenzfall zwischen Kundenorientierung und Persönlichkeitsrecht

Seite 341

Rechtsprechung

Dr. Gernot Fritz

Tatvorwurf, Tatzeitraum und maßgeblicher Jahresumsatz bei DSGVO-Geldbußen

Seite 344

Susan Hillert und Wiebke Reuter

Newsletter-Versand: Der EuGH zum „Verkaufsbegriff“ und Soft Opt-In nach ePrivacy-Richtlinie

Seite 347

Dr. Dominik Sorber und Dr. Christina Knoepffler

Datenschutzrechtlicher Auskunftsanspruch vs. Compliance

Seite 350

▪ **Nachrichten Seite 331**

Dr. Olaf Koglin

HBDI: „Microsoft 365 kann datenschutzkonform genutzt werden“ – aber was ist dafür erforderlich?

Die aufsichtsbehördlichen Einschätzungen hinsichtlich Microsoft 365 (M365) verändern sich langsam, aber stetig. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) hatte 2020 in einer umstrittenen Entscheidung Office 365 noch faktisch abgelehnt und diese Position dann 2022 abgeschwächt. Die niedersächsische Aufsichtsbehörde (LfD Nds) und der Europäische Datenschutzbeauftragte (EDSB) haben den Einsatz von Microsoft 365 zuletzt für akzeptabel gehalten. Nun geht der hessische Datenschutzbeauftragte noch weiter. Er schreibt den Verantwortlichen aber auch eine Reihe von Aufgaben und Hinweisen ins Pflichtenheft.

Der Bericht des HBDI

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit (HBDI) hat Mitte November einen knapp 140-seitigen Bericht veröffentlicht, der einen Paradigmenwechsel bei der aufsichtsbehördlichen Bewertung von M365 enthält ([use365.ms/HBDI](https://www.use365.ms/HBDI)). Bereits die Pressemitteilung titelte: „Microsoft 365 kann datenschutzkonform genutzt werden“ – und provozierte damit natürlich Kritik.

Hintergrund der Untersuchung und des Vorgehens

Hintergrund der Untersuchung des HBDI ist laut dem Bericht eine Anfrage des Hessischen Digitalministeriums zu Nutzungsszenarien von M365 sowie ein aufsichtsbehördliches Verfahren gegen eine nicht-öffentliche Stelle.

Der HBDI hat daraufhin etliche Gespräche mit Microsoft Deutschland geführt. Auf Basis dieser Informationen und weiteren schriftlichen Austauschs wurde der HBDI-Bericht erstellt. Die Themen orientieren sich an der bisherigen aufsichtsbehördlichen Kritik, insbesondere an den sieben zentralen Punkten aus der Feststellung der DSK aus 2022.

Soweit ersichtlich, wurden die von Microsoft gemachten Angaben nicht vertieft überprüft oder hinterfragt; der Bericht beruht sachverhaltsseitig insoweit zu großen Teilen auf den Angaben von Microsoft (z. B. zu dem Vorgehen bei der Pseudonymisierung von Daten auf S. 23 des Berichts). Dies entspricht der Position etlicher Aufsichtsbehörden, dass ein Verantwortlicher den Zusagen von Auftragsverarbeitern grundsätzlich vertrauen darf. Eine technische Überprüfung von M365 erfolgte ausdrücklich nicht.

Einordnung in die aufsichtsbehördlichen Positionen

Zu den zentralen Positionierungen der Aufsichtsbehörden zählten bislang:

- Ein Beschluss der DSK vom September 2020, bei der es zu einer Kampfabstimmung über eine sehr Microsoft-kritische Festlegung kam;

- Eine erneute Festlegung der DSK vom November 2022, deren Tenor im Vergleich dazu moderater ausfiel. Hierin hieß es, „dass der Nachweis von Verantwortlichen, Microsoft 365 datenschutzrechtskonform zu betreiben, auf der Grundlage des von Microsoft bereitgestellten ‚Datenschutznachtrags vom 15. September 2022‘ nicht geführt werden kann.“

Im Kontext der Formulierung des Beschlusses aus 2022 ist die Aussage des HBDI zu lesen, wonach die datenschutzrechtskonforme Nutzung von M365 nunmehr möglich sei. Unter beiden Entscheidungen benötigt der Verantwortliche eigene Dokumentationen und Bewertungen, um M365 einzusetzen. Aber bei der DSK stand 2022 im Vordergrund, dass der Einsatz nicht zulässig sei. Nun wird die Zulässigkeit bejaht – unter bestimmten Voraussetzungen.

Weitere behördliche Bewertungen zu M365

Weitere aufsichtsbehördliche Positionierungen, die letztendlich einen Einsatz von M365 für akzeptabel hielten, erfolgten 2023 und 2024 durch den LfD Nds und 2024 und 2025 durch den EDSB. Beide Aufsichten hatten nach zunächst ausführlichen Kritiken oder Verbesserungsvorschlägen ihre endgültigen und verhalten positiven Stellungnahmen eher karg oder gar nicht begründet. Weitere Positionierungen erschienen insb. zur Corona-Zeit zur Nutzung von Teams als Videokonferenzsystem.

Kohärenz und Abstimmung mit anderen aufsichtsbehördlichen Positionen

Die DSK-Beschlüsse aus 2020 und 2022 wurden selbstverständlich innerhalb der gesamten DSK besprochen und – zumindest im Rahmen der Mehrheiten – von ihren Mitgliedern mitgetragen. Zur Neubewertung des LfD Nds aus 2024 heißt es aus Aufsichtskreisen, dieser sei im Alleingang ohne Abstimmung mit den anderen DSK-Kollegen erfolgt. Der Bericht des HBDI wurde hingegen innerhalb der Aufsichtsbehörden der DSK abgestimmt.

Relevanz von aufsichtsbehördlichen Positionen

Egal ob positiv oder negativ: Fachliche Positionierungen von Datenschutz-Aufsichtsbehörden sollten gekannt und berücksichtigt werden, zumal sie – gerade aus der Feder des HBDI, Prof. Dr. Roßnagel – lesenswert sind und fundierte rechtliche Begründungen liefern.

Im Rahmen der Gewaltenteilung sind die Aufsichtsbehörden aber nur Teil der Exekutive; hier sogar nur im Rahmen einer unverbindlichen Rechtsinformation ohne Verwaltungsakt. Orientierungshilfen oder Berichte wie der des HBDI haben keine rechtliche Bindungswirkung gegenüber Verantwortlichen. Die Frage, ob das HBDI-Dokument nur in Hessen oder auch in anderen Bundesländern „gilt“, stellt sich daher nicht.

Untersuchungsgegenstand: DPA und Sonderfassung für Behörden

Es ist öffentlich bekannt, dass der Datenschutz zur Nutzung von M365 zum großen Teil in einem Microsoft-Dokument mit der Bezeichnung Data Protection Addendum (DPA) geregelt ist, das in der deutschen Fassung als „Datenschutznachtrag“ bezeichnet wird (use365.ms/DPA). Das DPA umfasst nicht nur eine klassische Vereinbarung zur Auftragsvereinbarung (AVV), sondern enthält weitere Regelungsgegenstände (Koglin, DSB 2025, 65). Vom HBDI wurde die aktuelle DPA-Fassung vom 15. September 2025 bewertet, die trotz des ähnlichen Datums nicht mit der von der DSK 2022 betrachteten Fassung vom 15. September 2022 verwechselt werden darf.

Spätestens seit der öffentlichen Bewertung des LfD Nds zu M365 aus 2024 ist bekannt, dass es neben den offiziellen DPA-Fassungen auch weitere, individuell verhandelte und ergänzte Versionen gibt. Der HBDI spricht hier für Hessen von einem „im Zuge der gemeinsamen Gespräche für öffentliche Stellen mit Sitz in Hessen fortentwickelten DPA“ (DPA-ös). Das DPA-ös wurde im Bericht nicht als vollständiges Dokument oder Synopse publiziert. Beim Lesen des HBDI-Berichts lassen sich jedoch etliche Änderungen zusammenfügen.

Ausdrücklich nicht betrachtet hat der HBDI einzelne M365-Dienste. So wird auch auf das KI-Angebot Copilot nicht eingegangen, wohl Microsoft 365 Copilot Chat in M365 enthalten ist und Verantwortliche sich mit dessen Nutzung befassen sollten, um Copilot nicht zur „Schatten-KI“ geraten zu lassen.

Kritik an der Positionierung des HBDI

Wie zu erwarten wurde die Publikation des HBDI in Teilen als praxisnah, pragmatisch und überfällig begrüßt, während sie aus dem Lager der Microsoft-Skeptiker scharf kritisiert wurde.

Kuketz: „Microsoft 365 erhält in Hessen grünes Licht, weil die Aufsicht überfordert ist“

Ein bekannter IT-Sicherheitsblogger kritisiert an der HBDI-Positionierung vor allem, dass behördenseitig keine Überprüfung der Technik oder der tatsächlich übermittelten Daten erfolgte (use365.ms/KUK-HBDI).

Selbstverständlich wäre es immer wünschenswert, eine vollumfängliche Betrachtung aller rechtlichen, technischen und weiteren Aspekte zu haben. Doch zum einen sind Ressourcen stets begrenzt, egal ob in Behörden oder in Unternehmen. Zum anderen haben Mammut-Untersuchungen zu M365, wie von der DSK oder dem EDSB vorgenommen, zu einer langen Projektdauer geführt. Dadurch war bei der Veröffentlichung der Untersuchungsgegenstand bereits wieder veraltet (DPA-Fassung, Drittlandlandtransfer). Insofern ist es aus Sicht des Verfassers sehr erfreulich, eine behördliche Positionierung zu haben, die sich auf ein aktuelles DPA bezieht.

Kritik aus Teilen der konfessionellen Datenschutzaufsicht

In der Datenschutzaufsicht der Kirchen und religiösen Vereinigungen i. S. d. Art. 91 DSGVO lassen sich die Positionen grob dahingehend einteilen, dass sich einige Aufsichten auf Aspekte beschränken, die im konfessionellen Kontext stehen, aber für eher weltliche Fragen wie der Verwendung von Standardsoftware auf die Positionen der allgemeinen „staatlichen“ Aufsicht verweisen.

Andere positionieren sich auch zu M365-Fragen oder stellen diese in einen biblischen Kontext. So hat sich der Datenschutzbeauftragte eines Bistums in sozialen Medien dahingehend geäußert, dass die durch Konzerne wie Microsoft erfolgende „Monetarisierung von Menschen (...) dem Wertekanon der Kirche“ widerspreche und daher Open Source Software „theologisch unterstützt“ werden solle.

Digitale Souveränität

Aspekte der digitalen Souveränität sind keine unmittelbare (datenschutz-)rechtliche Frage. Daher wurden sie zu Recht ausdrücklich nicht vom HBDI geprüft. Gleichwohl gibt er die Empfehlung, vor dem Einsatz von M365 den Betrieb alternativer Produkte in Betracht zu ziehen (S. 93).

Der Inhalt des HBDI-Berichts: Drei mal sieben Themen

Der HBDI hat seine Ausarbeitung an die sieben Hauptkritikpunkte des DSK-Beschlusses von 2022 angelehnt. Diese werden in den Kapiteln Sachverhalt, rechtliche Erwägungen und Handlungsempfehlungen – also je drei Mal – behandelt; die Themen sind:

1. Festlegung der Daten sowie von Art und Zweck ihrer Verarbeitung
2. Eigene Verantwortlichkeit von Microsoft

3. Weisungsbindung und Offenlegung
4. Umsetzung von TOMs
5. Löschung und Rückgabe von Daten
6. Unterauftragsverarbeiter
7. Drittlandübermittlungen

Die wesentlichen Aussagen aus den drei Betrachtungsebenen werden hier thematisch zusammengefasst.

Angaben zur Festlegung der Art der Daten

Die DSK rügte 2022 die fehlende Möglichkeit des Verantwortlichen, personenbezogene Daten und deren Verarbeitungszweck näher zu beschreiben und gegebenenfalls zu konkretisieren. Dies könnte, so die DSK, „durch eine kundenspezifische Konkretisierung“ wie in den Standard-Datenschutzklauseln erfolgen (Punkt 3.1 der Zusammenfassung des Berichts der AG Microsoft-Onlinedienste aus 2022).

Dieser Themenkomplex wurde von Microsoft bereits kurz nach der DSK-Entscheidung mit der DPA-Fassung vom 1. Januar 2023 angepasst. Zudem wurden in der Sonderversion des hessischen DPA-ös zwei Änderungen vorgenommen (S. 20 ff. im HBDI-Bericht): U. a. gelten die sog. „Inhaltsdaten“ nun als „Sammelkategorie“ für all jene Daten, die der Kunde und seine Nutzer in M365 speichern, ohne dass Microsoft weiß und wissen soll, welche Arten von Daten und betroffenen Personen verarbeitet werden. Microsoft verhalte sich zu diesen Daten „agnostisch“. Dies behandelt also das bekannte Problem, dass in Dienstleistungsangeboten mit breiter Verwendungsmöglichkeit der Auftragnehmer keinen Einfluss und keine Kontrollmöglichkeit hat, welche Daten der Kunde hochlädt und verarbeiten lässt.

Der HBDI verweist in seinen rechtlichen Erwägungen zunächst auf die von ihm und die von Microsoft erstellten Erläuterungen und Arbeitshilfen, wie dem M365-Kit (dazu unten) sowie den als Anlagen beigefügten Unterlagen, etwa dem als „Taxonomie“ bezeichneten Dokument zur Begriffserklärung (Anlage 3 zum HBDI-Bericht).

Anders als die DSK 2022 kommt der HBDI nun zu dem Schluss, es sei mit Hilfe der neuen Dokumente „für den Verantwortlichen möglich, den Gegenstand des Auftragsverarbeitungsvertrags (...) hinreichend konkret zu bestimmen und seinen weitergehenden Pflichten nach der DSGVO (etwa Art. 13 ff. DS-GVO und Art. 30 DS-GVO) nachzukommen“ (S. 51). Zudem werden die besonderen Anforderungen im öffentlichen Sektor dargestellt. Nach Ansicht des HBDI wurde das von der DSK monierte Problem der Konkretisierung damit behoben.

Handlungsempfehlung: M365 als Betriebsmittel

Unter den Handlungsempfehlungen wird im HBDI-Bericht nochmals auf die Nutzung der neu zur Verfügung gestell-

ten Dokumente des M365-Kits hingewiesen. Der HBDI übernimmt dabei die auch von anderen Aufsichtsbehörden verwendete Formulierung, dass M365 ein Betriebsmittel sei – so etwa der BayLfD (www.datenschutz-bayern.de/dsfa).

Zutreffend ist, dass Software oder gar die Markennamen von SaaS-Angeboten weder einen Verarbeitungsvorgang i. S. d. Art. 4 Nr. 2 DSGVO noch den Gegenstand einer Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 DSGVO darstellen (so auch Brink/Koglin auf der Datenschutzkonferenz 2025). Gleichwohl können aber für ähnliche Verarbeitungen in gleichartigen Cloud-Angeboten musterartige Dokumente entworfen werden, wie es mit der Unterstützung der Behörden auch durch das M365-Kit erfolgt.

Eigene Verantwortlichkeit von Microsoft

Aufgrund von Formulierungen in früheren Fassungen des DPA war für die DSK unklar, welche Daten des Kunden im Rahmen der Auftragsverarbeitung verarbeitet werden und welche personenbezogenen Daten Microsoft in eigener Verantwortung verarbeitet.

Der HBDI schildert ausführlich die Darstellungen von Microsoft zu deren Verwendung von Daten im Rahmen eigener Verantwortlichkeit (S. 22 ff.). Hiernach werden die zur Verarbeitung für Microsoft-eigene „Geschäftstätigkeiten“ vorgesehenen Daten – soweit sie überhaupt Personenbezug aufweisen – zunächst pseudonymisiert; dies erfolgt von Microsoft noch in der Rolle des Auftragsverarbeiters. Die Daten werden anschließend aggregiert, so dass die sich ergebenden Daten nach Auffassung des HBDI nicht mehr personenbeziehbar sind (S. 23). Soweit diese Daten sodann von Microsoft in eigener Geschäftstätigkeit (vulgo: außerhalb des AVV) verwendet werden, ist dies somit datenschutzrechtlich zulässig. Zudem wurde im DPA-ös die diesbezügliche Passage neu gefasst (S. 26).

Die rechtliche Bewertung dieser Thematik ist ein Schwerpunkt des Gutachtens (S. 54 ff.); sie behandelt verschiedene Unterfälle sowie das DPA-ös und die Rechtsgrundlage zur Pseudonymisierung innerhalb der Auftragsverarbeitung (für Beschäftigte öffentlicher Stellen in Hessen: beachte § 23 Abs. 1 S. 1 HDSIG; für andere Personen § 3 HDSIG).

Anonymisierung zum Zweck der eigenen Nutzung zulässig

Der HBDI kommt zur grundsätzlichen Argumentation, dass die Anonymisierung dem Gebot der Datenminimierung entspricht und daher die Risiken nachfolgender Datenverarbeitungen reduziert. Daher „ist sie nicht mit einem tiefgehenden Grundrechtseingriff verbunden, sondern schließt ihn aus oder minimiert ihn beträchtlich.“

Das Vorgehen sei auch erforderlich, um die „M365-Produkte für die Aufgabenerfüllung der öffentlichen Stelle (der Behörde) nutzen zu können. „Daher sei die Anonymisierung erforderlich und zulässig“ (S. 59 ff.).

Anonymisierung auf Basis der Rechtsgrundlage des „berechtigten Interesses“ – sogar für Behörden

Hilfswise wird auch ausführlich eine „Verarbeitungserlaubnis außerhalb des Auftragsverhältnisses“ geprüft. Diese kann laut HBDI auf die Rechtsgrundlage des berechtigten Interesses gestützt werden – und zwar, was viele überraschen wird, auch bei der Nutzung von M365 durch öffentliche Stellen. Im Bericht wird detailliert vom Zusammenspiel des Gesetzesvorbehaltes für hoheitliches Handeln (Art. 6 Abs. 1 lit. e DSGVO) mit der Ausnahme für das berechnete Interesse bei Behörden bei Datenverarbeitungen in Erfüllung ihrer Aufgaben aus Art. 6 Abs. 1 Satz 2 DSGVO hergeleitet, dass sich eine Behörde für die Nutzung von M365 auf Art. 6 Abs. 1 lit. f DSGVO berufen könne, da der M365-Betrieb nicht im Rahmen ihrer hoheitlichen Aufgaben liegt (S. 62 ff.). Daher gilt laut dem HBDI die dargestellte Interessenabwägung auch für Behörden.

Weisungsbindung und Offenlegung und Drittlandtransfer

Hinter den Begriffen „Weisungsbindung und Offenlegung“ verbarg sich in der DSK-Stellungnahme die Fragestellung, wie mit staatlichen Ersuchen aus den USA zur Herausgabe von Kundendaten umzugehen ist, wenn solche Anfragen in Konflikt zu dem Weisungsrecht des Auftraggebers aus Art. 28 Abs. 3 Satz 2 lit. a DSGVO stehen.

CLOUD Act und FISA 702

Hintergrund waren und sind selbstverständlich Kritikpunkte wie der US-amerikanische CLOUD Act sowie Section 702 des Foreign Intelligence Surveillance Act (FISA 702). Dieses Thema ist eng mit dem Drittlandtransfer und der Frage nach der Rechtsgrundlage zu einem Drittlandtransfer i. S. d. Art. 44 ff. DSGVO verknüpft. Der HBDI geht zur Thematik des Weisungsrechts auf die DPA-Bestimmungen zur Offenlegung, den Anhang C des DPA sowie kleinere Änderungen im DPA-ös ein.

Im Rahmen der rechtlichen Erwägungen könne daher „festgestellt werden, dass der Anforderung des Art. 28 Abs. 3 UAbs. 1 Satz 2 Buchst. a DS-GVO entsprochen werden kann“ (S. 68). Auch dieser große, stark politisierte Kritikpunkt hat sich nach dem Bericht des HBDI somit erledigt.

Drittlandtransfer: Gedeckt vom DPF, den Standard-datenschutzklauseln und Art. 49 Abs. 1 DSGVO

Zum Themenkomplex des Drittlandtransfers werden die Änderungen der Rechts- und Sachlage seit 2022 darge-

stellt, wie dem EU-US Data Privacy Framework (DPF), Änderungen der Drittlandtransfer-Struktur im DPA und Schutzmechanismen wie dem EU Data Boundary-Programm von Microsoft.

Der HBDI verweist auf das DPF, die Latombe-Entscheidung des EuG (EuG, Urt. v. 3.9.2025 – Rs. T-553/23) und darauf, dass „Datenübermittlungen auf der Grundlage des DPF derzeit rechtmäßig“ sind, was rechtlich unstrittig und auch explizite DSK-Meinung ist. Weiter wird auf die ergänzend abgeschlossenen Standarddatenschutzklauseln verwiesen sowie darauf, dass mit der EU Data Boundary (die inzwischen eine „EFTA Data Boundary“ ist) und Zusatzprodukten wie „Customer Lockbox“ ein tatsächlicher Drittlandtransfer nur in sehr wenigen Fällen vorkommen wird (S. 75).

Dies sind zutreffende, aber auch allgemein bekannte Aspekte (vgl. Koglin, Datenschutz bei M365, S. 98). Interessant ist, dass der HBDI zusätzlich darauf hinweist, dass ein Drittlandtransfer zu einem unsicheren Drittstaat zudem auch nach den Einzelfallausnahmen des Art. 49 Abs. 1 DSGVO erfolgen kann.

Unterauftragsverarbeiter seitens Microsoft

Einer der aus Sicht des Verfassers wichtigsten Kritikpunkte der DSK war die Benachrichtigung des Auftraggebers über Änderungen der eingesetzten Unterauftragsverarbeiter nach Art. 28 Abs. 2 DSGVO. Der HBDI erläutert die Vorlaufzeiten von 6 Monaten und 30 Tagen und kommt zu dem Ergebnis, dies „gäbe dem Kunden Zeit, um dem Einsatz des Unterauftragsverarbeiters zu widersprechen oder geeignete Maßnahmen zu ergreifen“ (S. 38). Aus Sicht des Verfassers reicht dies bei weitem nicht für eine „Remigration“ aus M365 in ein anderes System.

HBDI: Keine aktive Information an Kunden erforderlich

Standardmäßig werden Microsoft-Kunden nicht proaktiv (z. B. per E-Mail) über die bevorstehenden Änderungen der Unterauftragnehmer informiert, sondern müssen sich diese Information selbst im Service Trust Portal über die „Online Services Subprocessors List“ heraussuchen (use365.ms/Subs). Der HBDI hält dies für ausreichend, auch wenn der Auftragsverarbeiter den Verantwortlichen nicht aktiv über eine Änderung der Unterauftragsverarbeiter informiert. „Im Ergebnis sind die Anforderungen des Art. 28 Abs. 2 (...) DS-GVO erfüllt, auch wenn der Kunde die Informationen über neue Unterauftragsverarbeiter im Service-Portal von MS einsehen muss“ (S. 73).

Nach Auffassung des Verfassers muss der Verantwortliche oder sein Administrator zumindest die diesbezüglichen Informations-Mails aktivieren, um den Anforderungen des Art. 28 Abs. 2 Satz 2 DSGVO zu genügen („informiert der

Auftragsverarbeiter den Verantwortlichen immer über jede beabsichtigte Änderung“).

Der Praxisteil: Handlungsempfehlungen und weitere Dokumente

Im dritten Hauptteil gibt der HBDI Handlungsempfehlungen für den Einsatz von M365. Hier gibt es zu jedem der sieben DSK-Kritikpunkte Hinweise und Vorschläge. Diese wirken bisweilen etwas allgemein, etwa Ratschläge zur Festlegung von Löschrufen oder zur Datenminimierung. Gleichwohl haben sie ihre Berechtigung und es sollte von einer Aufsichtsbehörde nicht erwartet werden, dass diese ein fertiges Löschkonzept oder konkrete Vorgaben zu den Einstellungen in den Admin-Centern von M365 erstellt.

Unter „Weitere Empfehlungen“ (ab S. 93) folgt der Vorschlag, auch den alternativen Einsatz von Produkten zu prüfen, die dem Trend der digitalen Souveränität folgen. Dies erscheint rechtlich nicht zwingend. Im Rahmen einer unangreifbaren Bewertung sollte dies aber mit in die DSFA und andere Bewertungen aufgenommen werden. Denn indirekt kann dies im Kontext des „berechtigten Interesses“ bei Randthemen wie der Pseudonymisierung relevant werden (siehe oben zur „Eigenen Verantwortlichkeit“): Ist M365 alternativlos, spricht dies eher für eine entsprechende Gewichtung der eigenen Interessen.

In der umfangreichen Anlage 4 werden weitere Hinweise zu datenschutzrechtlichen Anforderungen genannt. Diese beziehen sich auf allgemeine Aspekte ohne spezifischen Bezug zu Cloud-Aspekten oder zu M365, wie die Richtigkeit der Daten, die Erstellung eines Verzeichnisses der Verarbeitungstätigkeiten oder die Durchführung einer DSFA.

Einbindung von Stakeholdern und dauerhafte Überprüfung

Zu Recht weist der HBDI darauf hin, dass Stakeholder wie Datenschutzbeauftragte und Betriebs- und Personalräte eingebunden werden sollten. Elementar ist zudem, einen Prozess zur kontinuierlichen Überprüfung und Bewertung von Änderungen zu implementieren. Denn Software as a Service wie M365 wird laufend neue Funktionen und Tools (wie Copilot) erhalten, Beschäftigte werden M365 für immer neue Use Cases einsetzen und die vertraglichen und rechtlichen Rahmenbedingungen werden sich weiterhin laufend ändern. Dies mit einem wirksamen Prozess abzusichern, ist Compliance-seitig wichtiger als ein Halbsatz im DPA oder ein Meinungsstreit zur Konkretisierung der zu verarbeitenden Daten im AVV.

Weitere Dokumente und Hilfsmittel: Anlagen und M365-Kit

Unter dem Titel „Taxonomie“ hat der HBDI zudem ein ausführliches Dokument beigefügt, in dem Microsoft die eigenen Datenkategorien – wie Inhaltsdaten, Audit-Log-Daten

oder Diagnose-Daten – erläutert (Anlage 3). Leider scheint dies nicht deckungsgleich mit dem sonst oft von Microsoft verwendeten Begriffspaar der Telemetrie- und Diagnose-daten zu sein.

Zusätzlich hat Microsoft unabhängig von den Gesprächen mit dem HBDI, aber in Abstimmung mit dem BayLDA und unter Einbindung des HBDI, u. a. das M365-Kit erstellt (S. 49). Dabei handelt es sich um einen Satz von Mustern u. a. für die Datenschutzzinformation oder etwa auch die DSFA beim Einsatz von M365 (use365.ms/Kit).

Fazit und Auswirkungen auf Beratung und Praxis

Die Bewertungen des HBDI sind eine große, konstruktive Hilfe bei der Nutzung von M365. Bei einigen, von der DSK vielleicht sehr skeptisch bewerteten Punkten, führen die Bewertungen zu sehr praxisnahen, aber rechtlich fundierten Argumentationen – etwa bei der Anonymisierung von Daten zur Überführung in die Nutzung durch Microsoft zu eigenen Geschäftszwecken.

Die Bewertung des HBDI sollte jedoch nicht als Freibrief zur unkontrollierten Nutzung von M365 verstanden werden. Wer nicht nur den Titel der Pressemitteilung, sondern zumindest die Kapitelüberschriften des Inhaltsverzeichnisses liest, wird schnell erkennen, dass der Einsatz von M365 eine individuelle und vor allem laufende datenschutzrechtliche Bewertung erfordert.

Dabei wird es aus der langen Liste der Handlungsempfehlungen und aus den zusätzlich in Anlage 4 genannten Anforderungen etliche Punkte geben, die kleinere und mittelgroße Organisationen überfordern. Auch dürfte die Empfehlung, das nur in teureren Lizenzen enthaltene Zusatzprodukt „Customer Lockbox“ einzusetzen, nicht bei allen Verantwortlichen zwingend zu befolgen sein.

Erfreulich ist, dass die Dauerkritikpunkte CLOUD Act und FISA 702 eindeutig beantwortet wurden. Wünschenswert wäre, wenn das „M365-Recht“ sich den noch weniger betrachteten Themen zuwenden würde, wie etwa der Abgrenzung zum Telekommunikationsrecht bei Videokonferenzen (wie bei Teams) und E-Mail-Infrastruktur (wie bei Exchange).

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.

