Kommunikation & Recht

K&R
12 | Dezember 2025
28. Jahrgang
Seiten 749 - 820

Verlies Navidad
Philipp Schröder-Ringe

749 EU Digital Services Act und Digitale-Dienste-Gesetz
István Fancsik

755 Zwischen Cloud und Kontrolle – Datenschutz und digitale Souveränität bei Microsoft 365
Stefan Hessel, Christina Ziegler-Kiefer und Moritz Schneider

761 Private Nutzung betrieblicher E-Mail-Postfächer
Dr. Carlo Piltz und Ilia Kukin

765 Wem gehört das Glasfasernetz?
Dr. Stephan Rippert, Anne-Sophie Fischer und Maximilian Issels

772 Länderreport Österreich
Prof. Dr. Clemens Thiele

775 **BGH:** Schadensersatzanspruch bei vorsätzlicher Herbeiführung eines DSGVO-Verstoßes?
mit Kommentar von **Dr. Stefanie Hellmich**

781 **BGH:** Kostenlose Registrierung auch bei Preisgabe personenbezogener Daten zu Werbezwecken?

783 **BGH:** Bequemer Kauf auf Rechnung II: Irreführende Werbung mit Zahlungsmodalitäten

793 **OLG München:** Vertragszusammenfassung: Unterlassungsansprüche beim Vertrieb von Internet- und TV-Kabelverträgen

801 **OLG Köln:** Orthopädische Matratze: Gerichtsstand bei irreführender Werbung im Onlinehandel

803 **LG Hamburg:** Haftung für KI-generierte falsche Tatsachenbehauptungen
mit Kommentar von **Dr. Louis Rolfes und Dr. Malte Engeler**

806 **LG Bonn:** Keine Verpflichtung zur Auskunft bei entgegenstehendem US-amerikanischem Recht

809 **BVerwG:** Compact: Presse- und Medienunternehmen können grundsätzlich unter Vereinsverbot fallen
mit Kommentar von **Dr. Sandra Lukosek**

Chefredakteur
RA Torsten Kutschke

Stellvertretende Chefredakteurin
RAin Dr. Anja Keller

Redakteur
Dr. Maximilian Leicht

Redaktionsassistentin
Stefanie Lichtenberg

www.kommunikationundrecht.de

dfv Mediengruppe
Frankfurt am Main

RA Stefan Hessel, LL.M., RAin Christina Ziegler-Kiefer, LL.M. und RA Moritz Schneider*

Zwischen Cloud und Kontrolle – Datenschutz und digitale Souveränität bei Microsoft 365

Kurz und Knapp

Die Diskussion um digitale Souveränität hat neue Dynamik gewonnen. Im Mittelpunkt steht dabei die Nutzung von Cloud-Diensten amerikanischer Anbieter. Der Beitrag untersucht die rechtlich umstrittenen Fragen rund um Microsoft 365 und zeigt, dass ein datenschutzkonformer Einsatz grundsätzlich möglich ist. Neben den bekannten Kritikpunkten der Aufsichtsbehörden werden auch die Auswirkungen aktueller Entwicklungen in den USA und Europa analysiert.

I. Einleitung

Die Debatte um den datenschutzkonformen Einsatz von Microsoft 365 im Lichte der Datenschutz-Grundverordnung (DSGVO) währt inzwischen seit Jahren. Zwar haben sich zahlreiche Kritikpunkte der Datenschutzaufsichtsbehörden durch fortlaufende Anpassungen und Präzisierungen der Datenschutzbestimmungen von Microsoft – insbesondere im Microsoft Product and Services Data Protection Addendum (DPA)[1] – inzwischen deutlich relativiert.[2] Gleichwohl bleibt das Thema Gegenstand intensiver Diskussionen. Aktuelle politische Entwicklungen in den USA verleihen der Debatte neue Dynamik. Unter Schlagworten wie „digitaler Souveränität" wird der Einsatz amerikanischer Diensteanbieter teils pauschal infrage gestellt. Ereignisse wie die zu Beginn des Jahres erfolgte Abberufung demokratischer Mitglieder des Privacy and Civil Liberties Oversight Board (PCLOB),[3] das eine zentrale Rolle bei der unabhängigen Kontrolle von US-Überwachungsmaßnahmen im Hinblick auf den Schutz der Privatsphäre und Bürgerrechte spielt, haben die Diskussion um die Voraussetzungen des Angemessenheitsbeschlusses für die USA weiter verstärkt.

Gleichzeitig hat der Europäische Datenschutzbeauftragte sein Verfahren gegen die EU-Kommission wegen des Einsatzes von Microsoft 365 eingestellt, nachdem die Kommission die zuvor angemahnten technischen und organisatorischen Maßnahmen ergriffen hat.[4] Zudem hat der Angemessenheitsbeschluss der EU-Kommission für Datenübermittlungen in die USA seine erste gerichtliche Überprüfung überstanden: Das Europäische Gericht (EuG) hat mit Entscheidung vom 3. 9. 2025 eine Nichtigkeitsklage gegen den Beschluss abgewiesen.[5] Des Weiteren hat Microsoft zu Beginn des Jahres den vollständigen Rollout der sogenannten EU Data Boundary bekannt gegeben, die Kunden innerhalb der EU mehr Kontrolle über ihre Daten geben soll.[6]

Der Beitrag gibt einen Überblick über den datenschutzrechtlichen Stand der aktuellen Debatte zum Einsatz von Microsoft 365. Dabei werden zunächst aktuelle Entwicklungen unter dem Schlagwort digitale Souveränität rechtlich eingeordnet (II.). Danach werden die bereits bekannten, aber nach wie vor anzutreffenden, Kritikpunkte an den Regelungen des Microsoft DPA durch die Datenschutzaufsichtsbehörden einer kritischen Bewertung unterzogen (III.), um die datenschutzrechtliche Debatte zur Nutzung von Microsoft 365 umfassend abzubilden.

II. Digitale Souveränität

Der Begriff der digitalen Souveränität ist derzeit ein zentrales Schlagwort in der politischen Debatte. Oftmals ist die Stoßrichtung dieser Debatte gegen den Einsatz von Cloud-Lösungen amerikanischer Anbieter durch europäische Unternehmen und öffentliche Stellen gerichtet. Auf diese Stimmung reagieren auch große US-Anbieter: Neben der bereits angesprochenen EU Data Boundary von Microsoft, arbeitet etwa Amazon Web Services an der European Sovereign Cloud, die entsprechende Bedenken ausräumen soll.[7]

Stein des Anstoßes der Kritiker sind dabei Zugriffsbefugnisse amerikanischer Sicherheitsbehörden. Bei der rechtlichen Bewertung wird jedoch häufig nicht präzise zwischen unterschiedlichen Konstellationen unterschieden: Rechtlich ist die Frage des Datenschutzniveaus von Daten, die in die USA übermittelt werden, von der Frage der Nutzung europäischer Tochtergesellschaften amerikanischer Anbieter in Europa zu trennen. Die erste Frage betrifft rechtlich die Voraussetzungen der Übertragung von Daten aus dem Geltungsbereich der DSGVO in ein Drittland. Eine solche Übermittlung kann, sofern vorhanden, auf einen Angemessenheitsbeschluss der Europäischen Kommission für das Empfängerland gestützt werden. Nach Art. 45 Abs. 1 S. 2 DSGVO setzt die Rechtmäßigkeit eines solchen Beschlusses voraus, dass in dem betreffenden Drittland ein angemessenes Schutzniveau gewährleistet ist.

Die zweite Frage betrifft die Rechtskonformität des Einsatzes europäischer Tochtergesellschaften amerikanischer Unternehmen in Europa, wenn diese Daten in Europa speichern. In diesem Zusammenhang wird häufig auf die tatsächliche oder vermeintliche extraterritoriale Wirkung amerikanischer Sicherheitsgesetze verwiesen, die zu einer abstrakten Gefahr eines Datenzugriffs durch US-Behörden begründeten. Diese Zugriffsmöglichkeiten allein begründen jedoch keine Drittlandübermittlung im Sinne der DSGVO. Vielmehr sind sie als Aspekt der Zuverlässigkeit des Auftragsverarbeiters zu würdigen. Dass diese Gefahr allein keine Drittlandübermittlung begründet, sondern als rechtliches Problem im Rahmen der Zuverlässigkeit des Auftragsverarbeiters zu berücksichtigen ist, hat auch die deutsche Datenschutzkonferenz (DSK) zutreffend festgestellt.[8]

---

* Mehr über die Autoren und die Autorin erfahren Sie am Ende des Beitrags. Alle zitierten Internetquellen wurden zuletzt abgerufen am 18. 10. 2025.

1 Microsoft, Datenschutznachtrag für Produkte und Services von Microsoft, Stand: 1. 9. 2025, unter: https://ruw.link/2025/174 (microsoft.com).

2 *Hessel/Kiefer*, RDi 2023, 282.

3 Bloomberg Law, Trump Fires Democrats from Privacy Oversight Board, unter: https://ruw.link/2025/175 (news.bloomberglaw.com).

4 EDPS, Closure of enforcement proceedings in the Commission's use of Microsoft 365, unter: https://ruw.link/2025/176 (edps.europa.eu).

5 EuG, 3. 9. 2025 – T-553/23, unter: https://ruw.link/2025/177 (eur-lex.europa.eu).

6 Microsoft, Microsoft completes landmark EU Data Boundary, offering enhanced data residency and transparency, unter: https://ruw.link/2025/178 (blogs.microsoft.com).

7 Amazon News, Multimilliarden AWS Cloud-Projekt in Brandenburg erhält eigenständige Governance, unter: https://ruw.link/2025/200 (aboutamazon.de).

8 DSK, Zur datenschutzrechtlichen Bewertung von Zugriffsmöglichkeiten, S. 1, unter: https://ruw.link/2025/199 (datenschutzkonferenz-online.de).

Dieser Unterscheidung Rechnung tragend werden im Folgenden der Angemessenheitsbeschluss für die USA sowie die Effektivität des EU Data Boundary von Microsoft (II.1.) und die Zuverlässigkeit des Auftragsverarbeiters im Hinblick auf Zugriffsmöglichkeiten von US-Sicherheitsbehörden (II.2.) getrennt dargestellt.

1. Angemessenheitsbeschluss und EU Data Boundary

a) Drittlandübermittlungen bei Microsoft 365

Microsoft hat bereits im Januar 2023 mit der Umsetzung der sogenannten EU Data Boundary begonnen.[9] Mit der Einführung der EU Data Boundary wurde schrittweise die Verarbeitung personenbezogener Daten (zunächst die Kundendaten aus den Core Online Services, dann die Diagnosedaten und schließlich der gesamte Supportbereich) in den europäischen Raum verlagert. Microsoft hat angekündigt, dass europäische Kunden automatisch und ohne weiteres Zutun von den Regelungen und technischen Vorkehrungen der EU Data Boundary erfasst werden. Bezüglich Microsoft 365 fallen Kunden, deren Anmeldeort in einem Land oder einer Region der EU oder der EFTA liegt, in den Geltungsbereich der EU Data Boundary.[10]

Inzwischen hat Microsoft bekannt gegeben, dass die letzte Phase der Einführung der EU Data Boundary abgeschlossen ist. Mit dem Abschluss der letzten Projektphase sollen nun auch Professional-Services-Daten, etwa Protokolle und Support-Daten, innerhalb der EU und der Europäischen Freihandelszone (EFTA) verbleiben.[11] Auch wenn dies eine deutliche Risikominimierung mit sich bringt, kann nach wie vor nicht ausgeschlossen werden, dass es zu vereinzelten Übermittlungen personenbezogener Daten in Drittländer wie die USA kommt. So ist es nach Angaben von Microsoft möglich, dass es im Rahmen von Untersuchungen zur Cybersicherheit auch zu Übertragungen personenbezogener Daten in andere Weltregionen kommen kann.[12] Dies soll zwar primär pseudonymisierte personenbezogene Daten und Professional-Services-Daten betreffen. In seltenen Fällen können dabei eingeschränkt Kundendaten übermittelt werden. Insoweit sind Drittlandübermittlungen in die USA auch dann nicht ausgeschlossen, wenn der Einsatz von Microsoft 365 unter die Regeln der EU Data Boundary fällt. Die Regelungen bringen jedoch eine erhebliche Risikoreduktion mit sich. Auch der Europäische Datenschutzbeauftragte sieht die EU Data Boundary als wesentlichen Fortschritt an, der dazu beigetragen hat, dass seine Bedenken gegen den Einsatz von Microsoft 365 durch die EU-Kommission ausgeräumt wurden.[13]

b) Angemessenheitsbeschluss für die USA

Für Drittlandübermittlungen in die USA besteht zurzeit eine rechtssichere Grundlage nach Art. 45 Abs. 1 S. 1 DSGVO: Die EU-Kommission hat am 10. 7. 2023 einen nach wie vor gültigen Angemessenheitsbeschluss für Datenübermittlungen in die USA erlassen.[14] Vorausgegangen war dem Beschluss eine politische Einigung zwischen der EU und den USA, die im EU-U.S. Data Privacy Framework (DPF) gipfelte. Streng genommen handelt es sich dabei um kein Abkommen, wie etwa ein völkerrechtlich bindender Vertrag, sondern lediglich um Zusagen und Entscheidungen der US-Regierung, auf denen der neue Angemessenheitsbeschluss beruht.[15] Dem DPF liegt das Prinzip der Selbstzertifizierung zugrunde. Daher gilt auch der Angemessenheitsbeschluss für die USA nur für Organisationen in den USA, die in die „Data Privacy Framework List" des U.S. Department of Commerce eingetragen sind.[16] Nach aktuellem Stand ist die Microsoft Corporation sowohl für HR Data als auch für Non-HR Data zertifiziert. Eine Datenübermittlung an die Microsoft Corporation unterfällt daher grundsätzlich dem geltenden Angemessenheitsbeschluss. Solange der Angemessenheitsbeschluss weder vom EuGH oder EuG noch von der EU-Kommission selbst aufgehoben wurde, bleibt er gültig und Datentransfers an zertifizierte Empfänger in den USA bleiben rechtmäßig. Das ergibt sich auch daraus, dass sogar eine mögliche Aufhebung des Angemessenheitsbeschlusses nach Art. 45 Abs. 5 S. 1 DSGVO ausdrücklich ohne rückwirkende Kraft erfolgt. Selbst im Falle einer Aufhebung blieben die bis dahin vorgenommenen Übermittlungen daher rechtmäßig.

c) EuG-Entscheidung

Bereits unmittelbar nach Erlass des neuen Angemessenheitsbeschlusses der Europäischen Kommission wurden Stimmen laut, die bezweifelten, dass die Voraussetzungen für dessen Erlass vorlagen. Der Verein NOYB um den Datenschutzaktivisten Max Schrems kündigte umgehend an, gegen den Beschluss juristisch vorgehen zu wollen.[17] Die DSK äußerte in ihren Anwendungshinweisen zum Angemessenheitsbeschluss für die USA die Einschätzung, Verantwortliche müssten sich auf eine mögliche künftige Aufhebung einstellen.[18] Entgegen dieser Befürchtungen hat der Angemessenheitsbeschluss seine erste rechtliche Bewährungsprobe bestanden: Das EuG wies eine Nichtigkeitsklage gegen ihn ab.[19] Dies verschafft Unternehmen weiterhin eine rechtssichere Grundlage für Datentransfers in die USA. Dabei bleibt jedoch unklar, wie lange die Entscheidung Bestand haben wird. In seinem Urteil stellte das Gericht klar, dass für die Beurteilung der Zeitpunkt des Erlasses des Angemessenheitsbeschlusses durch die EU-Kommission maßgeblich gewesen sei.[20] Nicht berücksichtigt wurden hingegen nachträgliche Entwicklungen innerhalb der USA, wie etwa die Abberufung eines Teils der Mitglieder des PCLOB.

2. Zuverlässigkeit des Auftragsverarbeiters und CLOUD-Act

Von den Voraussetzungen rechtskonformer Drittlandübermittlungen zu unterscheiden ist die Bewertung abstrakter Risiken, die aus dem Einsatz europäischer Tochtergesellschaften amerikanischer Anbieter entstehen, wenn die Daten innerhalb des Geltungsbereichs der DSGVO gespeichert werden. Hintergrund sind die weitreichenden Befugnisse amerikanischer Sicherheitsbehörden nach Gesetzen wie dem Clarifying Lawful Overseas Use of Data Act (CLOUD-Act) und dem Foreign Intelligence Surveillance Act (FISA). Es besteht die Befürchtung, dass diese Vorschriften zu einer nach europäischem

9 Siehe https://ruw.link/2025/181 (blogs.microsoft.com).
10 Microsoft, What is the EU Data Boundary, unter: https://ruw.link/2025/201 (learn.microsoft.com).
11 Microsoft, Was ist die EU-Datengrenze, unter: https://ruw.link/2025/202 (learn.microsoft.com).
12 Microsoft, Fortlaufende Datenübertragungen, unter: https://ruw.link/2025/184 (learn.microsoft.com).
13 EDPS, Closure of enforcement proceedings in the Commission's use of Microsoft 365, unter: https://ruw.link/2025/176 (edps.europa.eu).
14 Kommission, 10. 7. 2023 – C(2023) 4745 final.
15 *Hessel*, NJW 2023, 2970.
16 https://www.dataprivacyframework.gov/list.
17 NOYB, European Commission gives EU-US data transfers third round, unter: https://ruw.link/2025/203 (noyb.eu).
18 DSK, Anwendungshinweise, S. 31, unter: https://ruw.link/2025/204 (datenschutzkonferenz-online.de).
19 EuG, 3. 9. 2025 – T-553/23, unter: https://ruw.link/2025/177 (eur-lex.europa.eu).
20 EuG, 3. 9. 2025 – T-553/23, Rn. 22, unter: https://ruw.link/2025/177 (eur-lex.europa.de).

Recht unzulässigen Offenlegung von in der Europäischen Union gespeicherten personenbezogenen Daten gegenüber US-Behörden führen könnten. Rechtlicher Anknüpfungspunkt dieser Bedenken ist Art. 28 Abs. 1 DSGVO,[21] wonach Verantwortliche nur solche Auftragsverarbeiter einsetzen dürfen, die hinreichende Garantien für eine DSGVO-konforme Verarbeitung bieten.

Der CLOUD-Act wurde vor dem Hintergrund erlassen, dass umstritten war, ob sich Herausgabeverpflichtungen nach dem Stored Communications Act amerikanischer Unternehmen in den USA auch auf im Ausland gespeicherte Daten beziehen. Nach dem Stored Communications Act können Electronic Communication Service Provider (ECSP) und Anbieter von Remote-Computing-Diensten (RCS) von amerikanischen Ermittlungsbehörden angewiesen werden, Informationen und Daten über Nutzer herauszugeben. Dabei dürfen aktuelle Kommunikationsinhalte nur auf Grundlage eines gerichtlichen Beschlusses herausgegeben werden. Für den Erlass eines solchen Beschlusses ist der hinreichende Verdacht einer Straftat erforderlich.[22] Die Besonderheit des CLOUD-Act besteht nun darin, dass sich diese Herausgabeverpflichtung auch auf Daten und Informationen bezieht, die sich im Ausland befinden, sofern der verpflichtete Diensteanbieter Besitz, Gewahrsam oder Kontrolle an den Daten hat.[23] Sec. 702 FISA ist demgegenüber eine Befugnisnorm im Bereich der Auslandsaufklärung, die ebenfalls zu einer Herausgabepflicht für ECSP und RCS führen kann.[24]

Aus diesem Grund bestehen Befürchtungen, europäische Tochtergesellschaften könnten, z. B. auf Anweisung der Muttergesellschaft kraft deren gesellschaftsrechtlichen Weisungsrechte, personenbezogene Daten an Behörden in den USA übermitteln. Nach Art. 48 DSGVO dürfen Entscheidungen von Gerichten oder Behörden in Drittländern, mit denen von einem Verantwortlichen oder einem Auftragsverarbeiter die Übermittlung oder Offenlegung personenbezogener Daten verlangt wird, jedoch nur dann anerkannt oder vollstreckbar werden, wenn sie auf Übereinkünfte wie Rechtshilfeabkommen gestützt werden können. Im Ergebnis sind Datenübermittlungen an ausländische Stellen rechtswidrig, wenn sie nicht aufgrund etablierter Mechanismen für Rechtshilfeersuchen ergehen.[25] Für die Annahme, Anbieter wie Microsoft verstießen systematisch gegen europäisches Datenschutzrecht, fehlen jedoch tragfähige Anhaltspunkte. Die Datenschutzaufsichtsbehörden verfügen zudem über ein umfassendes Instrumentarium an Eingriffsbefugnissen, um im Zweifelsfall ein rechtskonformes Verhalten durchzusetzen. Es wirkt daher befremdlich, wenn bereits im Voraus die Wirksamkeit des Unionsrechts und die Fähigkeit der deutschen sowie europäischen Aufsichtsbehörden zu dessen effektiver Umsetzung in Zweifel gezogen werden. Der Chefjustiziar von Microsoft France erklärte in diesem Zusammenhang vor einem französischen Untersuchungsausschuss, er könne zwar nicht unter Eid ausschließen, dass es niemals zu einer entsprechenden Übermittlung ohne Zustimmung europäischer Behörden kommen könnte; ein solcher Fall sei bislang jedoch nicht vorgekommen.[26] Microsoft verpflichtet sich zudem in Anhang C des DPA zu zusätzlichen Schutzmaßnahmen.[27] Dazu gehört insbesondere, dass Microsoft alle rechtlich zulässigen Schritte unternimmt, um eine behördliche Aufforderung zur Offenlegung von Daten anzufechten, sofern diese auf Rechtsmängeln im Recht der anfragenden Partei oder auf Konflikten mit dem anwendbaren Recht der Europäischen Union beziehungsweise der Mitgliedstaaten beruht. Ohne weitere Anhaltspunkte wird sich, nur gestützt auf diese amerikanischen Befugnisse, eine pauschale Unzuverlässigkeit von Auftragsverarbeitern innerhalb der Europäischen Union nicht begründen lassen.

III. Das Microsoft DPA

Neben aktuellen Diskussionen um digitale Souveränität werden in der Praxis weiterhin Kritikpunkte am Einsatz von Microsoft 365 aufgegriffen, die die deutschen Datenschutzaufsichtsbehörden bereits 2022 und in den Jahren zuvor vor allem am DPA von Microsoft geäußert haben. Die zentralen Argumente wurden dabei in einer Festlegung der DSK vom 24. 11. 2022 vorgebracht.[28] Daneben veröffentlichten sieben der achtzehn in der DSK vertretenen Aufsichtsbehörden eine „Handreichung für die Verantwortlichen zum Abschluss einer Auftragsverarbeitungsvereinbarung gem. Art. 28 Abs. 3 DSGVO mit Microsoft für den Einsatz von Microsoft 365“[29] (Handreichung). Im Folgenden werden die zentralen Kritikpunkte aufgegriffen und kritisch gewürdigt.

1. Microsoft als Auftragsverarbeiter

Microsoft 365 wird als „Software as a Service“ zur Verfügung gestellt. Dies bedeutet, die Software wird nicht ausschließlich auf IT-Systemen der Kunden betrieben, sondern von Microsoft als webfähige Software zur Verfügung gestellt. In datenschutzrechtlicher Hinsicht wird Microsoft dabei für Unternehmen und öffentliche Stellen, die Software einsetzen, als Auftragsverarbeiter tätig. Verantwortliche müssen mit Auftragsverarbeitern nach Art. 28 Abs. 3 DSGVO einen Auftragsverarbeitungsvertrag schließen, der auch bestimmte Mindestinhalte umfassen muss. Dazu gehört nach Art. 28 Abs. 3 S. 2 lit. a DSGVO, dass der Auftragsverarbeiter personenbezogene Daten, die das Unternehmen im Rahmen der Auftragsverarbeitung erhält, nur auf dokumentierte Weisung des Kunden verarbeiten darf.

Die deutschen Datenschutzaufsichtsbehörden haben in der Vergangenheit am Microsoft DPA vermeintliche Widersprüche in den Bestimmungen zur Weisungsbindung gerügt.[30] Dabei stellt Microsoft in seinem DPA klar, dass Microsoft, soweit das Unternehmen als Auftragsverarbeiter oder Unterauftragsverarbeiter handelt, personenbezogene Daten nur nach dokumentierter Weisung des Kunden verarbeitet.[31] Eine Weisung enthält eine Festlegung des Verantwortlichen über die vom Auftragsverarbeiter zu erbringenden Leistungen einschließlich technischer und organisatorischer Schutzmaßnahmen. Charakteristisch für eine Weisung ist daher, dass diese die Zwecke und die wesentlichen Mittel der Datenverarbeitung durch den

21 DSK, Zur datenschutzrechtlichen Bewertung von Zugriffsmöglichkeiten, S. 1, unter: https://ruw.link/2025/199 (datenschutzkonferenz-online.de).
22 *Anheier/Nau*, ZD 2025, 559 f.
23 Wissenschaftlicher Dienst des Bundestages, Zu den Auswirkungen auf die Nutzung von Cloud-Diensten durch Behörden, S. 7, unter: https://ruw.link/2025/205 (bundestag.de).
24 *Anheier/Nau*, ZD 2025, 558.
25 *Jungkind*, in: Wolff/Brink/v. Ungern-Sternberg (Hrsg.), BeckOK DatenschutzR, 53. Ed. 1. 5. 2025, DSGVO Art. 48 Rn. 19.
26 *Förster*, Keine Garantien: Microsoft muss EU-Daten an USA übermitteln, unter: https://ruw.link/2025/206 (heise.de).
27 Microsoft, Datenschutznachtrag zu den Produkten und Services von Microsoft, 1. 9. 2025, S. 39, unter: https://ruw.link/2025/191 (microsoft.com).
28 AG DSK, Microsoft-Onlinedienste, unter: https://ruw.link/2025/197 (datenschutzkonferenz-online.de).
29 LfD Niedersachsen, Handreichung zur Auftragsverarbeitungs-Vereinbarung für Microsoft 365, unter: https://www.lfd.niedersachsen.de/download/199434.
30 AG DSK, Microsoft-Onlinedienste, S. 31, unter: https://ruw.link/2025/197 (datenschutzkonferenz-online.de).
31 Microsoft, Datenschutznachtrag zu den Produkten und Services von Microsoft, 1. 9. 2025, S. 13, unter: https://ruw.link/2025/191 (microsoft.com).

Verantwortlichen inhaltlich festlegt. Hinsichtlich der Mittel der Verarbeitung verbleibt dem Auftragsverarbeiter entsprechend der Leitlinien 07/2020 des Europäischen Datenschutzausschusses (EDSA) ein Gestaltungsspielraum.[32] Es ist nicht notwendig, jede Klausel eines Standardvertrags individuell zu verhandeln. Ermessensspielräume bei der konkreten Umsetzung der Maßnahmen sind der Delegation technischer Prozesse an fachkundigere Dienstleister und den offenen Formulierungen des Art. 28 DSGVO inhärent.[33] Nach der Handreichung soll das Erfordernis einer Vertragsänderung für zusätzliche oder abweichende Weisungen dem einseitigen Weisungsrecht des Verantwortlichen (Art. 29 DSGVO) widersprechen.[34] Vereinzelt wird in der Literatur in dem Erfordernis einer Vertragsänderung für zusätzliche oder abweichende Weisungen sogar ein „auf Null"[35] reduziertes Weisungsrecht des Kunden gesehen. Dabei ist jedoch nicht klar, woher in diesen Fällen der Widerspruch zu den Anforderungen der DSGVO bestehen soll. Insbesondere erschließt sich die Unvereinbarkeit zwischen dem einseitigen Weisungsrecht und der Vereinbarung, dass diesbezügliche Erweiterungen einer Vertragsanpassung bedürfen, nicht. Ein einseitiges Weisungsrecht ist kein einseitiges Leistungsbestimmungsrecht. Es liegt in der Natur des Massengeschäfts, dass die Weisungen des Kunden vertraglich vorweggenommen werden und zusätzliche Weisungen individuell vereinbart werden müssen.

2. Microsofts Verarbeitung zu eigenen Geschäftszwecken

Ein weiterer Kritikpunkt der Datenschutzaufsichtsbehörden ist die Verarbeitung personenbezogener Daten durch Microsoft für eigene Geschäftstätigkeiten. Das DPA ist kein reiner Auftragsverarbeitungsvertrag, sondern eine umfassende datenschutzrechtliche Rahmenvereinbarung für die Nutzung entsprechender Microsoft-Produkte und -Dienste. Insoweit enthält er auch Regelungen zu Verarbeitungsvorgängen, die Microsoft nicht im Auftrag des Kunden, sondern in eigener Verantwortlichkeit ausübt. Auch das aktuelle DPA vom September 2025 sieht die Möglichkeit der Verarbeitung durch Microsoft für eigene Zwecke vor.[36] Kritisiert wurde, dass die Verarbeitungen für eigene Geschäftszwecke nicht konkret genug beschrieben seien.[37] Die Bewertungen der Datenschutzaufsichtsbehörden bezogen sich auf veraltete Versionen des DPA. Inzwischen enthalten die DPA von Microsoft bereits seit mehreren Jahren detaillierte Vorgaben zu den Zwecken. Dort werden Zwecke wie etwa Abrechnungs- und Kontoverwaltung, Finanzberichterstattung und Geschäftsmodellierung wie Kapazitätsplanung genannt.[38]

Soweit personenbezogene Daten nicht im Rahmen der Auftragsverarbeitung, sondern zu eigenen Zwecken von Microsoft verarbeitet werden, handelt es sich nach Ansicht der deutschen Datenschutzaufsichtsbehörden um eine Offenlegung personenbezogener Daten des Kunden gegenüber Microsoft, für die der Verantwortliche einer Rechtsgrundlage bedarf.[39] Es erscheint bereits zweifelhaft, ob die bloße Gelegenheit zu einer Datenverarbeitung durch Microsoft in Folge der Nutzung von Microsoft 365 eine Offenlegung durch den Verantwortlichen darstellt. Der Begriff der Offenlegung wird in der DSGVO „als Oberbegriff für alle Vorgänge verwendet, durch die der Verantwortliche personenbezogene Daten anderen Stellen in einer Weise zugänglich macht, dass diese vom Informationsgehalt der betreffenden Daten Kenntnis erlangen können".[40] Für eine Verarbeitung bedarf es einer menschlichen Handlung, auf die der Verarbeitungsvorgang zurückzuführen ist und die dem Verantwortlichen zugerechnet werden kann.[41] Dass der Kunde durch die Nutzung von Microsoft 365 die Gelegenheit schafft, dass Microsoft die personenbezogenen Daten entsprechend verarbeiten kann, ist nicht ausreichend, um ihm dies als Offenlegung der Daten gegenüber Microsoft auszulegen. Damit fehlt es an einer Verarbeitungstätigkeit in Bezug auf den konkreten Verarbeitungsvorgang. Verarbeitungstätigkeiten nach der DSGVO setzen eine menschliche Handlung bzw. Zustandsveränderung voraus.[42] Aber auch wenn man der Ansicht der Datenschutzaufsichtsbehörden folgt und eine Offenlegung annimmt, stehen Rechtsgrundlagen zur Verfügung, auf die sich eine Übermittlung stützen lässt. Soweit nichtöffentliche Stellen Microsoft einsetzen, kommt insbesondere ein berechtigtes Interesse nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO in Betracht. Soweit öffentliche Stellen Verarbeitungen im Rahmen ihrer Aufgabenerfüllung vornehmen, können sie sich nach Art. 6 Abs. 1 UAbs. 2 DSGVO auf kein berechtigtes Interesse berufen. Ob eine Offenlegung der Daten, die in eigener Verantwortlichkeit von Microsoft etwa zu Abrechnungszwecken oder zur Planung von Kapazitäten verarbeitet werden, überhaupt in behördlicher Aufgabenerfüllung erfolgt, ist fraglich. Selbst wenn, kommen regelmäßig andere Rechtsgrundlagen wie etwa § 25 Abs. 2 Nr. 2 BDSG, wonach eine Übermittlung personenbezogener Daten durch öffentliche Stellen an nichtöffentliche Stellen zulässig ist, oder vergleichbare landesrechtliche Vorschriften in Betracht. Nach § 25 Abs. 2 Nr. 2 BDSG bedarf es für die Zulässigkeit der Übermittlung an eine nichtöffentliche Stelle eines berechtigten Interesses des Dritten an der Kenntnis der zu übermittelnden Daten, welches der Dritte hinreichend glaubhaft dargelegt haben muss. Zudem darf die betroffene Person kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung haben. Ähnliche Regelungen finden sich in Datenschutzgesetzen der Länder. Das berechtigte Interesse an der Verarbeitung der Daten für eigene Zwecke hat Microsoft mit den Ausführungen zu den Geschäftszwecken im Rahmen des DPA hinreichend glaubhaft dargelegt. Microsoft sichert ausdrücklich zu, Daten nicht zu anderen als den im DPA aufgeführten Zwecken zu verarbeiten. Angesichts des Umstandes, dass die zu übermittelnden Daten zunächst aggregiert und pseudonymisiert werden, ist ein überwiegendes schutzwürdiges Interesse der Betroffenen am Ausschluss der Offenlegung nicht ersichtlich.

3. Rechenschaftspflicht

Auch die sogenannte Rechenschaftspflicht dient seit Jahren als argumentativer Ansatzpunkt für die Kritik am Einsatz von

32 Europäischer Datenschutzausschuss, Leitlinien 07/2020 zu den Begriffen „Verantwortlicher" und „Auftragsverarbeiter" in der DSGVO, 7. 11. 2021, S. 4, unter: https://ruw.link/2025/207 (edpb.europa.eu).

33 Europäischer Datenschutzausschuss, Leitlinien 07/2020 zu den Begriffen „Verantwortlicher" und „Auftragsverarbeiter" in der DSGVO, 7. 11. 2021, 12, S. 4, 15, 38, unter: https://ruw.link/2025/207 (edpb.europa.eu).

34 LfD Niedersachsen, Handreichung zur Auftragsverarbeitungs-Vereinbarung für Microsoft 365, S. 13, unter: https://www.lfd.niedersachsen.de/download/199434.

35 *Breyer/Hirschel*, K&R 2024, 644.

36 Microsoft, Datenschutznachtrag zu den Produkten und Services von Microsoft, 1. 9. 2025, S. 10 f., unter: https://ruw.link/2025/191 (microsoft.com).

37 LfD Niedersachsen, Handreichung zur Auftragsverarbeitungs-Vereinbarung für Microsoft 365, S. 10, unter: https://www.lfd.niedersachsen.de/download/199434.

38 Microsoft, Datenschutznachtrag zu den Produkten und Services von Microsoft, 1. 9. 2025, S. 11, unter: https://ruw.link/2025/194 (microsoft.com).

39 AG DSK, Microsoft-Onlinedienste, S. 15, unter: https://ruw.link/2025/197 (datenschutzkonferenz-online.de).

40 *Herbst*, in: Kühling/Buchner (Hrsg.), DSGVO BDSG, 4. Aufl. 2024, Art. 4 Nr. 2 DSGVO Rn. 29.

41 *Herbst*, in: Kühling/Buchner (Fn. 40), Art. 4 Nr. 2 DSGVO Rn. 14, 21.

42 OVG Hamburg, 15. 10. 2020 – 5 Bs 152/20, openJur 2020, 78365, Rn. 29.

Microsoft 365. Nach Art. 5 Abs. 2, 24 Abs. 1 S. 1 DSGVO muss der Verantwortliche nachweisen können, dass er personenbezogene Daten im Einklang mit DSGVO verarbeitet. Den Umfang dieser Rechenschaftspflicht legen die Datenschutzaufsichtsbehörden sehr weit aus und fordern eine vollständige Kontrolle über das System.[43] Solch strenge Anforderungen ergeben sich jedoch nicht aus der DSGVO. Dieser Interpretation liegen technische Vorstellungen zugrunde, die mit der Komplexität moderner Cloud-Dienste, die hohen Anforderungen an Skalierbarkeit, Cybersicherheit und teils globaler Verfügbarkeit genügen müssen, nicht zu vereinbaren sind. Im Hinblick auf den Handlungsspielraum des Auftragsverarbeiters muss der Verantwortliche tatsächlich nicht alle Details eines Verarbeitungsvorgangs kennen, sondern nur so weit, wie dies für den Nachweis der Datenschutzkonformität erforderlich ist. Die Rechenschaftspflicht ist kein Ersatz für die Amtsermittlungspflicht der Datenschutzaufsichtsbehörden. Zumindest im Verwaltungs- und Strafverfahren darf die Rechenschaftspflicht nicht zu einer Beweislastumkehr zu Lasten des Verantwortlichen führen.[44] Da die DSGVO keine weiteren Anforderungen an den Nachweis stellt, genügt es, die Verträge und sonstigen Informationen des Auftragsverarbeiters zu prüfen und zu dokumentieren. Der Sinn und Zweck der Rechenschaftspflicht, eine ausreichende Transparenz über die Verarbeitungsprozesse zu schaffen und die Behörden bei ihrer Kontrolle zu unterstützen, ist damit regelmäßig erreicht.[45] Zudem bezieht sich die Rechenschaftspflicht nur auf Verarbeitungen, die im Rahmen der Auftragsverarbeitung erfolgen. Verarbeitet Microsoft personenbezogene Daten zu eigenen Zwecken, ist Microsoft für die Verarbeitungsvorgänge selbst verantwortlich und muss die Rechenschaftspflicht erfüllen. In Anlage 1 des aktuellen DPA verpflichtet sich Microsoft ausdrücklich, den Kunden während der gesamten Vertragslaufzeit bei der Erfüllung seiner Rechenschaftspflicht zu unterstützen.[46] Damit räumt Microsoft seinem Vertragspartner neben den gesetzlichen Ansprüchen nach der DSGVO einen vertraglichen Anspruch auf Überlassung der zur Erfüllung der Rechenschaftspflicht erforderlichen Informationen ein.

4. Festlegung der Art und des Umfangs der Verarbeitung

Der Verantwortliche muss im Auftragsverarbeitungsvertrag Angaben zu Art und Umfang der Verarbeitung machen. Wie weitgehend der Verantwortliche dem Auftragsverarbeiter dabei Vorgaben machen muss, ist umstritten. Hinsichtlich des erforderlichen Detailgrades der Angaben weichen die Auffassungen der Datenschutzbehörden mitunter von den gesetzlichen Anforderungen ab. Die Handreichung fordert etwa akribisch geführte Verarbeitungsverzeichnisse,[47] ohne die Gestaltungsspielräume der Auftragsverarbeitung zu berücksichtigen. In der Literatur werden zum Teil „situationsbezogene Formulierungen“ als ausreichend erachtet.[48] Dies schließt nicht aus, dass sowohl die Verarbeitungszwecke als auch die Art der personenbezogenen Daten in allgemeiner Form umschrieben werden. Erforderlich soll jedoch eine hinreichende Differenzierung der Verarbeitungszwecke sein.[49] Die Regelungstiefe muss in einem angemessenen Verhältnis zur Bedeutung der Auftragsverarbeitung stehen. Diese ergibt sich aus einer Abwägung zwischen dem Schutzbedarf und der Zumutbarkeit der Detailtiefe.[50] Nicht gefordert ist eine Darstellung aller Datenarten und Betroffenenkategorien für jeden Einzelfall. Sogar die Berliner Beauftragte für Datenschutz und Informationsfreiheit bezeichnet bis ins kleinste Detail ausgestaltete Verarbeitungsverzeichnisse als „Förmelei“, solange Art und Zweck der Verarbeitung und die betroffenen Daten genannt werden.[51] Microsoft unterteilt die erhobenen personenbezogenen Daten in drei Kategorien: Kundendaten, Professional-Services-Daten oder von Microsoft generierte, abgeleitete oder gesammelte Daten.[52] Welche Gestalt diese Kategorien an personenbezogenen Daten annehmen können, wird in Anhang B des DPA hinreichend aufgeführt. Der Bewertung, dass die verarbeiteten Daten in dem aktuellen DPA von Microsoft „nur kursorisch definiert“[53] seien, kann daher nicht gefolgt werden.

5. Technische und organisatorische Maßnahmen

Nach Art. 32 DSGVO sind geeignete technische und organisatorische Maßnahmen (TOM) zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Art. 32 DSGVO listet Maßnahmen auf und rekurriert dabei auf den Stand der Technik. Dieser ausfüllungsbedürftige Rechtsbegriff wird durch aktuelle Standards und Normen geprägt. In Zusammenschau mit der Rechenschaftspflicht kritisieren die Datenschutzaufsichtsbehörden unzureichende Angaben bezüglich der ergriffenen TOM.[54] Microsoft hat auf diese Kritik reagiert und verpflichtet sich in dem aktuellen DPA ausdrücklich, alle erforderlichen Maßnahmen nach Art. 32 DSGVO für alle Dienste und Services zu ergreifen. Dies beinhaltet die Verpflichtung zur Einhaltung der Normen ISO 27001, ISO 27002 und ISO 27018 sowie der in Anhang II der Standardvertragsklauseln der EU-Kommission von 2021 festgelegten Sicherheitsmaßnahmen zum Schutz personenbezogener Daten.[55]

6. Löschung personenbezogener Daten

Die Datenschutzaufsichtsbehörden haben zudem Bedenken hinsichtlich der im DPA festgelegten Löschfristen geäußert.[56] Argumentativer Anknüpfungspunkt ist dabei die Verpflichtung des Verantwortlichen, den Auftragsverarbeiter gemäß Art. 28 Abs. 3 S. 2 lit. g DSGVO vertraglich zu verpflichten, alle personenbezogenen Daten des Verantwortlichen nach Abschluss der Erbringung der Verarbeitungsleistungen entweder zu löschen oder zurückzugeben. Microsoft bewahrt gespeicherte Kundendaten für einen Zeitraum von 90 Tagen nach Ablauf oder Kündigung des Abonnements auf. Nach Ablauf dieser Aufbewahrungsfrist wird das Kundenkonto deaktiviert und die Kundendaten inklusive personenbezogener Daten innerhalb weiterer 90 Tage gelöscht. Zudem verpflichtet sich Microsoft, die personenbezogenen Daten nach Abschluss der Erbringung

43 AG DSK, Microsoft-Onlinedienste, S. 27 ff., unter: https://ruw.link/2025/197 (datenschutzkonferenz-online.de).
44 *Veil*, ZD 2018, 11 f.
45 *Veil*, ZD 2018, 12.
46 Microsoft, Datenschutznachtrag zu den Produkten und Services von Microsoft, 1. 9. 2025, S. 43, unter: https://ruw.link/2025/194 (microsoft.com).
47 LfD Niedersachsen, Handreichung zur Auftragsverarbeitungs-Vereinbarung für Microsoft 365, S. 9, unter: https://www.lfd.niedersachsen.de/download/199434.
48 *Spoerr*, in: Wolff/Brink/v. Ungern-Sternberg (Fn. 25), Art. 28 DSGVO Rn. 51.
49 *Borges*, in: Borges/Hilber (Hrsg.), BeckOK IT-Recht, 16. Aufl. 2022, Art. 28 DSGVO Rn. 50, 51.
50 *Borges*, in: Borges/Hilber (Fn. 49), Art. 28 DSGVO Rn. 46.
51 BlnBDI, Checkliste Prüfung AVV, 30. 6. 2022, S. 4, unter: https://ruw.link/2025/208 (datenschutz-berlin.de).
52 AG DSK, Microsoft-Onlinedienste, S. 7., unter: https://ruw.link/2025/197 (datenschutzkonferenz-online.de).
53 *Breyer/Hirschel*, K&R 2024, 556.
54 AG DSK, Microsoft-Onlinedienste, S. 15, unter: https://ruw.link/2025/197 (datenschutzkonferenz-online.de).
55 Microsoft, Datenschutznachtrag zu den Produkten und Services von Microsoft, 1. 9. 2025, S. 15 f., unter: https://ruw.link/2025/194 (microsoft.com).
56 AG DSK, Microsoft-Onlinedienste, S. 18, unter: https://ruw.link/2025/197 (datenschutzkonferenz-online.de).

der Verarbeitungsleistungen dem Verantwortlichen nach dessen Wahl zurückzugeben oder zu löschen.[57] Kritisiert wird, dass es für die Datenaufbewahrung nach Vertragskündigung in der Regel keine Rechtsgrundlage mehr gäbe.[58] In der Praxis gibt es jedoch gute Gründe, personenbezogene Daten über das Vertragsende hinaus aufzubewahren. Hierzu zählt z. B. der Schutz vor unbeabsichtigtem Datenverlust. Wie die Löschfristen für den Verantwortlichen zu bemessen sind, kann nicht abstrakt festgelegt werden, sondern muss im Einzelfall betrachtet werden.[59] Art. 28 Abs. 3 UAbs. 1 S. 2 lit. g DSGVO verlangt die Löschung bzw. Datenrückgabe nach „Abschluss der Erbringung der Verarbeitungsleistungen". Das Gesetz bezieht sich mit gutem Grund nicht auf den Zeitpunkt der Vertragsbeendigung. Die im DPA festgelegte maximale Löschfrist von 180 Tagen nach Vertragskündigung ist dabei Teil der vertraglich vereinbarten Verarbeitungsleistung und bewegt sich grundsätzlich im Rahmen zulässiger privatautonomer Vertragsgestaltung. Die Auslegung der Datenschutzaufsichtsbehörden widerspricht den Gegebenheiten bei der Nutzung moderner Cloud-Dienste und ist mit dem Ziel der DSGVO, den freien Verkehr personenbezogener Daten zu ermöglichen, nicht vereinbar.[60]

7. Einsatz von Unterauftragsverarbeitern

Ein weiterer Kritikpunkt betrifft den Einsatz von Unterauftragsverarbeitern durch Microsoft, insbesondere die Transparenz hinsichtlich der hierzu bereitgestellten Informationen.[61] Inzwischen hat Microsoft diesbezüglich umfassende Änderungen vorgenommen: Die Liste der Unterauftragsverarbeiter enthält nun detaillierte Angaben, darunter die Kontaktdaten des jeweiligen Unterauftragnehmers, das betroffene Microsoft-Produkt, die konkret durchgeführten Verarbeitungstätigkeiten, den Verarbeitungsort sowie die Unternehmensadresse.[62] Darüber hinaus wurde das DPA dahingehend angepasst, dass Microsoft die Verantwortlichen proaktiv über die Einbindung neuer Unterauftragsverarbeiter informiert – und zwar mindestens sechs Monate vor dem erstmaligen Zugriff auf Kundendaten sowie mindestens 30 Tage vor dem Zugriff auf Daten im Rahmen von Professional Services oder auf personenbezogene Daten, die nicht in den Kundendaten enthalten sind.[63] Die Liste der Unterauftragsverarbeiter wird zudem regelmäßig aktualisiert.

IV. Fazit

Ein datenschutzkonformer Einsatz von Microsoft 365 bleibt weiterhin möglich. Weder die politischen Entwicklungen in den USA noch die aktuellen Debatten um digitale Souveränität ändern diese rechtliche Bewertung. Der Angemessenheitsbeschluss für die USA ist weiter in Kraft und legitimiert Drittlandübermittlungen in die USA, sofern die Empfänger nach dem DPF zertifiziert sind. Das abstrakte Risiko, basierend auf der Unterstellung, europäische Tochtergesellschaften amerikanischer Unternehmen würden europäisches Recht brechen, vermag keine pauschale Unzuverlässigkeit von Auftragsverarbeitern zu begründen, die deren Einsatz rechtswidrig machen würde. Auch den in der Vergangenheit geäußerten Kritikpunkten deutscher Datenschutzaufsichtsbehörden am Microsoft DPA lassen sich, nicht zuletzt auch im Hinblick auf Verbesserungen am DPA von Microsoft, überzeugende rechtliche Argumente entgegensetzen.

Unternehmen und andere Stellen, die Microsoft 365 einsetzen, sollten sich daher weniger um das „Ob" als um das „Wie" eines datenschutzkonformen Einsatzes von Microsoft 365 Gedanken machen. Sofern der Einsatz von Microsoft 365 voraussichtlich mit einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen verbunden ist, ist gemäß Art. 35 DSGVO eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen. Ziel einer DSFA ist es, die Risiken, die sich aus bestimmten Verarbeitungstätigkeiten ergeben, systematisch zu identifizieren, zu bewerten und geeignete Abhilfemaßnahmen zu ermitteln, um die Risiken auf ein akzeptables Maß zu reduzieren. Ob eine DSFA im konkreten Fall erforderlich ist, hängt von der Art, dem Umfang, den Umständen und den Zwecken der jeweiligen Datenverarbeitung ab. Eine Verpflichtung besteht nicht bei jeder Nutzung von Microsoft 365. Aufgrund der Komplexität des Dienstes, der Vielzahl möglicher Verarbeitungsvorgänge, der regelmäßig umfangreichen Verarbeitung personenbezogener Daten sowie der potenziellen Einbindung schutzbedürftiger Personengruppen kann jedoch in vielen Fällen ein hohes Risiko im Sinne von Art. 35 Abs. 1 DSGVO nicht ausgeschlossen werden. Neben der DSFA bestehen weitere datenschutzrechtliche Anforderungen, die unabhängig vom Risikoniveau zu erfüllen sind. Insbesondere sind den betroffenen Personen die gesetzlich vorgeschriebenen Informationen gemäß Art. 13 und 14 DSGVO in präziser, transparenter, verständlicher und leicht zugänglicher Form bereitzustellen. Darüber hinaus sind – je nach konkretem Anwendungsfall – weitere Dokumentations- und Nachweispflichten zu beachten, etwa im Rahmen des Verzeichnisses von Verarbeitungstätigkeiten (Art. 30 DSGVO) sowie der technischen und organisatorischen Maßnahmen (Art. 32 DSGVO). Soweit diese Vorgaben eingehalten werden, kann Microsoft 365 datenschutzkonform eingesetzt werden.

Stefan Hessel
ist Rechtsanwalt, Salary Partner und Head of Digital Business bei reuschlaw in Saarbrücken.

Christina Ziegler-Kiefer
ist Rechtsanwältin und Senior Associate in der Digital Business Unit bei reuschlaw in Saarbrücken.

Moritz Schneider
ist Rechtsanwalt und Associate in der Digital Business Unit bei reuschlaw in Saarbrücken.

57 Microsoft, Datenaufbewahrung, Löschung und Vernichtung in Microsoft 365, unter: https://ruw.link/2025/209 (learn.microsoft.com).
58 AG DSK, Microsoft-Onlinedienste, S. 18, unter: https://ruw.link/2025/197 (datenschutzkonferenz-online.de).
59 *Worms*, in: Wolff/Brink/v. Ungern-Sternberg (Fn. 25), Art. 17 DSGVO Rn. 26.
60 *Hessel/Kiefer*, RDi 2023, 288.
61 AG DSK, Microsoft-Onlinedienste, S. 46 f., unter: https://ruw.link/2025/197 (datenschutzkonferenz-online.de).
62 Microsoft, Online Services Subprocessors List, 23. 6. 2025, unter: https://ruw.link/2025/198 (servicetrust.microsoft.com).
63 Microsoft, Datenschutznachtrag zu den Produkten und Services von Microsoft, 1. 9. 2025, S. 23., unter: https://ruw.link/2025/194 (microsoft.com).