RA Jonas Breyer und Anja Hirschel*

Zehn Rechtsverstöße beim DPA für Microsoft 365 vom 2.1.2024 („DPA") – Teil 2

Über die Wertlosigkeit der „Data Boundary" und die Mitverantwortung der Aufsichtsbehörden

Kurz und Knapp

Es ist nicht ernsthaft zu bestreiten, dass Microsoft 365 von Unternehmen nicht DSGVO-konform eingesetzt werden kann. Die Aufsichtsbehörden haben dies offiziell bestätigt,[1] ebenso aus ähnlichen Gründen jüngst der Europäische Datenschutzbeauftragte.[2] Und doch wird Microsoft 365 zu Lasten unzähliger Beschäftigter, minderjähriger Schüler und anderer betroffenen Personen breitflächig eingesetzt. Der Beitrag knüpft an den im vergangenen Heft erschienenen ersten Teil an.

IX. Risiko „Aushöhlung des Weisungsrechts"

Es liegt in der Natur der Auftragsverarbeitung, dass der Auftragnehmer Daten nur „auf Weisung des Verantwortlichen" verarbeiten darf (Art. 28 Abs. 3 lit. a DSGVO, Art. 29 DSGVO).[3] Zweck dieser Vorschrift ist es, sicherzustellen, dass der Verantwortliche über die Verarbeitung der Daten disponieren kann.[4] Dieses Weisungsrecht reduziert Microsoft jedoch nahezu auf Null, indem das Abschließen des vorformulierten DPA als einzig mögliche Weisung an Microsoft definiert wird:

„Der Kunde stimmt zu, dass der Kundenvertrag (einschließlich der DPA-Bestimmungen und aller anwendbaren Aktualisierungen) zusammen mit der Produktdokumentation und der Verwendung und Konfiguration der Features der Produkte durch den Kunden die vollständigen und dokumentierten Anweisungen des Kunden gegenüber Microsoft in Bezug auf die Verarbeitung personenbezogener Daten darstellen, oder die Dokumentation der Professional Services und die Nutzung der Professional Services durch den Kunden. Informationen zur Verwendung und Konfiguration der Produkte sind unter https://docs.microsoft.com (oder einer entsprechenden, dieser nachfolgenden Stelle) oder in einem anderen Vertrag, der dieses DPA einbezieht, zu finden. Zusätzliche oder andere Weisungen bedürfen einer Einigung nach Maßgabe des Verfahrens zur Änderung des Vertrags des Kunden. In allen Fällen, in denen die DSGVO gilt und der Kunde der Auftragsverarbeiter ist, sichert der Kunde Microsoft zu, dass die Anweisungen des Kunden einschließlich der Benennung von Microsoft zum Auftragsverarbeiter oder Unterauftragsverarbeiter vom jeweiligen Verantwortlichen autorisiert wurden."[5]

Zwar spricht nichts gegen eine automatisierte Bearbeitung von Weisungen, zumal es sich um ein Massenprodukt handelt. Ein zu starkes Beschneiden des Weisungsrechts i. V. m. einem wenig konturierten Vertrag (Umfang ersetzt keine Substanz) bewirkt aber, dass der Verantwortliche die Kontrolle über die Verarbeitung seiner Daten verliert.[6] So liegt es hier, da Microsofts DPA Microsoft erhebliche Ermessensspielräume belässt. So sind die Datenarten wenig konturiert, die Speicherfristen bleiben unklar, die Maßnahmen zur Datensicherheit sind, gemessen an den beliebig sensiblen Daten, schwammig und Microsoft behält sich nach Belieben Exporte in alle Länder der Welt[7] vor.

Für bestimmte Fälle, etwa für die „Schaffung einer erhöhten Transparenz für Kunden" oder „regulatorische Anforderungen, insoweit dies von der DSGVO gefordert wird", bezeichnet sich Microsoft in Abgrenzung zur Auftragsverarbeitung sogar ausdrücklich als „unabhängigen Datenverantwortlichen".[8] Dafür, dass tatsächlich die Microsoft Corp., Redmond, die Zwecke und Mittel bestimmt, spricht auch, dass diese im DPA als zentraler Ansprechpartner für Datenschutzfragen genannt ist, obwohl sie nicht Vertragspartner ist.[9] Es stellt sich die Frage, inwieweit die Auftragsverarbeitung überhaupt wirksam ist und in Wahrheit eine gemeinsame Verantwortlichkeit gemäß Art. 26 DSGVO vorliegt. Eine solche zeichnet sich dadurch aus, dass die Zwecke und Mittel der Verarbeitung durch mehrere Akteure bestimmt werden (Art. 4 Nr. 7 DSGVO). Im Fall Facebook, in dem Kunden ebenfalls wenig Einfluss auf die Datenverarbeitung hatten, bestätigte der EuGH eine solche gemeinsame Verantwortlichkeit, obwohl die nominelle Vertragslage dem nicht entsprach.[10] In einer späteren Entscheidung bestätigte der EuGH erneut, dass ein nomineller Auftragsverarbeiter, der Daten für eigene Zwecke verwendet, dadurch zum Verantwortlichen wird,[11] auch wenn eine förmliche Vereinbarung zur gemeinsamen Verantwortlichkeit nicht besteht.[12] Diese Frage beschäftigte „kursorisch" auch die DSK.[13] Im Fall einer gemeinsamen Verantwortlichkeit wäre die Datenverarbeitung ebenfalls rechtswidrig, da eine Vereinbarung gemäß Art. 26 DSGVO fehlt. Auch soweit Microsoft alleiniger Verantwortlicher wäre, wäre insbesondere die Weitergabe nach Art. 5, 6, 9, 44 ff. DSGVO seitens des Kunden weiterhin rechtfertigungs- und rechenschaftspflichtig.

X. Risiko „Auditierung"

Gesetzlich muss der Auftragsverarbeiter verpflichtet werden, dem Verantwortlichen Überprüfungen zu ermöglichen, ob alle Vorgaben der DSGVO eingehalten werden (Art. 28 Abs. 3 lit. h DSGVO). Dies umfasst beispielsweise die Funktionsweise der

* Mehr über den Autor und die Autorin erfahren Sie am Ende des Beitrags. Alle zitierten Internetquellen wurden zuletzt abgerufen am 9. 8. 2024.
1 DSK, Festlegung vom 24. 11. 2022 zu Microsoft 365.
2 EDSB, Pressemeldung vom 11. 3. 2024, https://www.edps.europa.eu/system/files/2024-03/EDPS-2024-05-European-Commission_s-use-of-M365-infringes-data-protection-rules-for-EU-institutions-and-bodies_EN.pdf.
3 EDSA, Leitlinien 7/2020 zur Auftragsverarbeitung, Rn. 116.
4 Vgl. *Spoerr*, in: Wolff/Brink/v. Ungern-Sternberg, BeckOK Datenschutzrecht, 46. Ed. 1. 5. 2022, DSGVO, Art. 29 Rn. 2.
5 DPA, S. 7, „Auftragsverarbeiter und Verantwortlicher – Rollen und Verantwortlichkeit", https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=14.
6 Vgl. *Spoerr*, in: Wolff/Brink/v. Ungern-Sternberg, (Fn. 4), Art. 29 Rn. 3.
7 DPA, S. 10, „Datenübermittlungen"; ebenso die nur Kunden zugänglichen Microsoft-SCC v. 13. 9. 2021, S. 17.
8 DPA, S. 7, „Auftragsverarbeiter und Verantwortlicher – Rollen und Verantwortlichkeit".
9 DPA, S. 13, „Kontaktaufnahme mit Microsoft".
10 EuGH, 29. 7. 2019 – C-40/17, K&R 2019, 562 ff. – Facebook.
11 EuGH, 5. 12. 2023 – C-807/21, K&R 2024, 30 ff., Rn. 85 – Deutsche Wohnen.
12 EuGH, 5. 12. 2023 – C-807/21, K&R 2024, 30 ff., Rn. 44, 46 – Deutsche Wohnen.
13 DSK, Festlegung vom 24. 11. 2022 zu Microsoft 365, Anlage, S. 6, 25.

Systeme, den Speicherort, Übermittlungen, Empfänger, Subunternehmer und zugriffsberechtigte Personen.[14] Die Entscheidung über die Person des Prüfers muss dem Verantwortlichen vorbehalten werden.[15] Microsoft behält sich jedoch vor, auf Prüfforderungen des Kunden überhaupt nur zu „reagieren", soweit diese nicht schon durch „Prüfberichte, Dokumentationen oder Informationen … angemessen erfüllt werden können".[16] Dies erfolgt durch Microsoft. Es bleibt auch unklar, was „angemessen" ist. Die Beweislast für das Vorliegen der Voraussetzungen für weitere Audits liegt der Formulierung nach beim Kunden. Außerdem macht Microsoft eine Prüfung davon abhängig, dass Kunden eine separate, nicht näher bestimmte Vereinbarung über Umfang, Zeit, Dauer, Kontroll- und Nachweisanforderungen sowie insbesondere Gebühren abschließen.[17] Microsoft ist aber zum Abschluss einer solchen Vereinbarung nie verpflichtet. Die Aufsichtsbehörden meinen zwar, dass Auditkosten an sich rechtmäßig seien,[18] obwohl es sich dabei um eine gesetzliche Pflicht des Auftragnehmers handelt. Nach deutschem Recht muss grundsätzlich jeder gesetzliche Pflichten auf eigene Kosten erfüllen.[19] Teleologisch spricht viel dafür, dies bei Audits nicht anders zu handhaben. Selbst nach Auffassung der Behörden dürfen die Kosten jedenfalls keine abschreckenden Ausmaße annehmen, da sie sonst das Auditrecht konterkarieren.[20] Das ist hier der Fall, da der Vertrag keine Begrenzung enthält. Dies gilt umso mehr, als sich die Daten nach dem Belieben Microsofts in sämtlichen Ländern der Welt befinden können, sodass allein Auslagen in beträchtlicher Höhe zu erwarten sind. Microsoft erlegt dem Kunden zudem alle eigenen Kosten „im Zusammenhang mit dieser Prüfung" auf, wie auch immer diese zu berechnen sein mögen. Eine solche Beschneidung des Auditrechts des Kunden entzieht ihm der Intention der Art. 28, 29 DSGVO zuwider die Kontrolle über seiner Daten[21] und verstößt gegen Art. 28 Abs. 3 lit. h DSGVO.

XI. Risiko „Löschfristen"

Nach Art. 17 DSGVO sind personenbezogene Daten zu löschen, wenn sie für den Zweck der Erhebung nicht mehr erforderlich sind. Dies setzt voraus, dass sie im Einzelnen überhaupt rechtmäßig erhoben wurden; fehlt es daran, sind sie ebenfalls zu löschen (Art. 17 Abs. 1 lit. d DSGVO). Eine Ausnahme gilt, soweit gesetzliche Aufbewahrungspflichten einer Löschung entgegenstehen (Art. 17 Abs. 1 lit. e DSGVO). Ein relevantes Beispiel ist die sechsjährige Aufbewahrung von Handelskorrespondenz gemäß § 257 Abs. 1 Nr. 2, 3 HGB.

Mangels abweichender, rechtfertigender Regelungen ist die Löschpflicht unverzüglich zu erfüllen.[22] Dies ergibt sich auch aus Art. 6 Abs. 1 DSGVO. Microsoft behält sich vor, personenbezogene Daten pauschal 180 Tage „nach Ablauf oder Beendigung des Abonnements des Kunden" zu löschen.[23] Somit können Beschäftigtendaten noch über den Tod des Beschäftigten hinaus gespeichert werden, je nachdem, wie lange sein Arbeitgeber seinen Microsoft-Vertrag unterhält, auch wenn der Beschäftigte längst ausgeschieden ist und die gesetzlichen Löschvoraussetzungen gegeben sind. Dies kann prinzipiell auch höchst sensible Daten wie Videomitschnitte betreffen, wobei aufgrund des Speicherplatzbedarfs unklar ist, ob Microsoft diese speichert. Das Beispiel legt nahe, dass die pauschale Frist wahrscheinlich schon unwahr ist, in jedem Fall aber für zahlreiche Datenarten in ihrer Länge nicht zu rechtfertigen ist. Der BGH hat etwa für die Deutsche Telekom als Internet-Zugangsprovider entschieden, dass Metadaten einer Internetverbindung bis zu sieben Tage gespeichert werden dürften[24] und dies auch nur, weil eine damalige Spezialvorschrift des Telekommunikationsgesetzes (heute: § 12 TDDDG) dies zur Störungsbeseitigung erlaubte.

Aufwendige Löschkonzepte von Unternehmen müssen ins Leere laufen, wenn Microsoft an diese nicht vertraglich gebunden ist und der Kunde diese Fristen auch technisch nicht zur Geltung bringen kann. Dies betrifft beispielsweise den gesamten E-Mail-Verkehr nebst Inhalten auf den Exchange-Servern Microsofts, selbst wenn für die E-Mails keine Aufbewahrungspflichten mehr greifen.

Etwaige punktuelle technische Einstellungsmöglichkeiten Microsofts zur Datenlöschung sind nach dem Vertragswerk nicht verpflichtend und allenfalls eine freiwillige Leistung Microsofts.

XII. Risiko „Subunternehmer"

Nach dem Gesetz setzt der Auftragnehmer keine weiteren Subunternehmer ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen ein. Im Fall einer allgemeinen Genehmigung informiert der Auftragsverarbeiter den Verantwortlichen stets über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Auftragsverarbeitern, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (Art. 28 Abs. 2 DSGVO). Die Information muss insbesondere Angaben des Subunternehmers zu Standort, seiner Aufgabe und der Datensicherheit enthalten.[25] Beim Standort ist nicht nur die Angabe des rechtlichen Sitzes (lokale Gesetze), sondern auch der Verarbeitungsort (Art. 44 ff. DSGVO) zur Prüfung erforderlich. Klauseln, wonach der Auftragnehmer das Schweigen des Auftraggebers als Zustimmung zu einer Änderung werten darf, sollen zulässig sein, auch wenn die Rechtsprechung des EuGH jedenfalls bei der Erklärung von Einwilligungen in die gegensätzliche Richtung weist,[26] jedoch muss vorher eine Information erfolgen und es muss ein Widerspruchsrecht bestehen.[27]

In Microsofts DPA fällt auf, dass Microsoft alle „Microsoft-Gesellschaften" für „unterstützende Dienstleistungen" zu Subunternehmern deklariert.[28] Microsoft verpflichtet sich, eine Liste aller Subunternehmer auf „einer Microsoft-Website" bereitzustellen,[29] nähere Angaben fehlen. Der Kunde muss sich seinen Vertragsinhalt „zusammengoogeln". Dies stellt gemessen an Art. 28 Abs. 2 DSGVO keine zumutbare Möglichkeit der Kenntnisnahme dar. Eine Verpflichtung, dass bei Änderungen die URL mitgeteilt wird, fehlt ebenfalls. Ebenso fehlt die Verpflichtung zu einer synoptischen Gegenüberstellung im Fall von Änderungen.[30] Eine Suche nach „Online Services Subprocessors" auf der Microsoft-Website führte vorliegend

14 EDSA, Leitlinien 7/2020 zur Auftragsverarbeitung, Rn. 143.
15 EDSA, Leitlinien 7/2020 zur Auftragsverarbeitung, Rn. 144.
16 DPA, S. 9, „Prüfung und Einhaltung".
17 DPA, S. 9, „Prüfung der Einhaltung".
18 EDSA, Leitlinien 7/2020 zur Auftragsverarbeitung, Rn. 145.
19 BGH, 18. 4. 2002 – III ZR 199/01, K&R 2002, 368 ff. – Deaktivierungsgebühr.
20 EDSA, Leitlinien 7/2020 zur Auftragsverarbeitung, Rn. 145.
21 Vgl. *Spoerr*, in: Wolff/Brink/v. Ungern-Sternberg (Fn. 4), Art. 29 Rn. 3.
22 *Worms*, in: Wolff/Brink/v. Ungern-Sternberg, BeckOK Datenschutzrecht, 46. Ed. 1. 8. 2023, DSGVO, Art. 17 Rn. 54.
23 DPA, S. 11, „Speicherung und Löschung von Daten".
24 BGH, 3. 7. 2014 – III ZR 391/13, K&R 2014, 593 ff. – T-Online.
25 EDSA, Leitlinien 7/2020 zur Auftragsverarbeitung, Rn. 152.
26 EuGH, 1. 10. 2019 – C-673/17, K&R 2019, 705 ff., Rn. 44 ff. – Planet49.
27 EDSA, Leitlinien 7/2020 zur Auftragsverarbeitung, Rn. 156.
28 DPA, S. 11, „Hinweise und Kontrollen beim Einsatz von Unterauftragsverarbeitern".
29 DPA, S. 11, „Hinweise und Kontrollen beim Einsatz von Unterauftragsverarbeitern".
30 DSK, Festlegung vom 24. 11. 2022 zu Microsoft 365, Anlage, S. 51.

zu einer aktuellen Version in englischer Sprache.[31] Diese Liste enthält indes nicht alle Microsoft-Gesellschaften, die „Dienstleistungen" erbringen können, sondern nur solche, die „data center" betreiben.[32] Im Übrigen bleibt unklar, welche Microsoft-Gesellschaften in Frage kommen. Es bleibt auch im Dunkeln, ab welchen Eigentumsquoten, Stimmrechten oder sonstigen Merkmale eine Microsoft-Gesellschaft als solche gilt.

Beispiel: Ist die SAP AG eine Microsoft-Gesellschaft in diesem Sinne, wenn Microsoft eine SAP-Aktie erwirbt?

In der Liste fehlen die Anschriften der Gesellschaften, ihrer Aufgabe und bei der Angabe „Country" ist unklar, ob dies den Geschäftssitz oder den Verarbeitungsort bezeichnen soll. Ein Link in der Liste führt zu einer Website Microsofts über verschiedene Rechenzentren,[33] bei denen unklar bleibt, von welcher Gesellschaft sie betrieben werden und welche Daten sie verarbeiten. Bemerkenswert ist weiter, dass die Liste zahlreiche Subunternehmer in Drittländern aufführt, für die kein Angemessenheitsbeschluss besteht, etwa China, Indien, Australien, Singapur – sowie Standorte des Amazon-Diensts AWS. Wenn der Kunde auch diese Liste „ergooglet",[34] ergeben sich unter anderem die möglichen Verarbeitungsorte Bahrain, Kolumbien, Vereinigte Arabische Emirate, Hong Kong, Malaysia, Oman, Mexiko, Nigeria, Panama, Philippinen, Thailand, Vietnam, Indonesien und Peru. Dort müsste ein rechtstreuer Kunde zumindest gelegentlich auditieren. Die Notwendigkeit all dieser Subunternehmer erschließt sich nicht. Für jedes Drittland muss eine Abwägung der dort bestehenden, insbesondere rechtlichen Risiken erfolgen.[35] Eine solche Evaluation fehlt bei Microsoft völlig.[36] Je nach Gefahr, etwa der vom EuGH beleuchteten Gesetzgebung örtlicher Nachrichtendienste, eignen sich Maßnahmen für Land X keineswegs automatisch für Land Y. Die Einhaltung der Art. 44 ff. DSGVO kann somit vom Kunden nicht gemäß Art. 5 Abs. 2, Art. 24 DSGVO nachgewiesen werden und eine effektive Auditierung ist in praxi unmöglich.

Ein weiteres Risiko liegt im fehlenden Widerspruchsrecht des Kunden, wenn Microsoft die Subunternehmer ändern möchte, was grundsätzlich jederzeit möglich ist.[37] Dem Kunden muss dabei das Recht eingeräumt werden, gegen jede „Änderung Einspruch zu erheben" (Art. 28 Abs. 2 DSGVO). Statt den Vertrag bis zu einer ordentlichen Beendigung unverändert fortzuführen, räumt Microsoft lediglich ein außerordentliches Kündigungsrecht ein. Microsoft stellt den Kunden damit gemäß dem Prinzip „take it or leave it" vor die Wahl, beliebige Änderungen der Subunternehmer zu akzeptieren oder kurzfristig gänzlich auf Microsoft 365 zu verzichten. Dies entspricht nicht dem unionsrechtlichen Effektivitätsgrundsatz (Art. 4 Abs. 3 EUV), da das Ziel ausgehöhlt wird, dem Verantwortlichen auch im Fall der Auftragsverarbeitung die Kontrolle über seine Daten zu bewahren.[38] Auch der BGH hat entschieden, dass ein vertragliches Preisänderungsrecht nicht dadurch wirksam werde, dass dem Kunden jeweils ein außerordentliches Kündigungsrecht eingeräumt werde; die Ausweitung wichtiger Kündigungsgründe auf unwichtige Fälle sei unwirksam, weil das Vertrauen des Kunden auf den vertraglichen Bestandsschutz vorgehe.[39] Derartige Klauseln stellten eine unzulässige Verschiebung des vertragsrechtlichen Äquivalenzverhältnisses dar.[40] Nicht anders liegt es hier.

XIII. Risiko „biometrische Daten"

Nach dem Gesetz dürfen biometrische Daten als sogenannte besondere Kategorien personenbezogener Daten gemäß Art. 9 DSGVO unter bestimmten Voraussetzungen verarbeitet werden, etwa wenn dies sozial- oder arbeitsrechtlich erforderlich ist (Art. 9 Abs. 2 lit. b DSGVO). Biometrische Daten sind unter anderem identifizierende Gesichtsfotos und Fingerabdruckdaten.[41] Zu denken ist – im Hinblick auf die Datenarten – etwa an Zweifaktor-Authentifizierungen. Der Einsatz von biometrischen Gesichtserkennungskameras in mehreren Bundesländern zeigt, dass heute schon gewöhnliche Gesichtsfotos biometrisch auswertbar sind, sodass gewöhnliche Fotos biometrische Daten darstellen können. Hiergegen wird eingewandt, dass EG 51 Fotos nur dann als biometrische Daten verstanden wissen will, wenn sie „mit speziellen technischen Mitteln verarbeitet werden, die die eindeutige Identifizierung oder Authentifizierung einer natürlichen Person ermöglichen".[42] Jedoch dürfen Erwägungsgründe nicht dahin ausgelegt werden, dass sie dem Wortlaut der DSGVO widersprechen.[43] Vielmehr erscheint die Voraussetzung erfüllt, zumal bekannt ist, dass Microsoft zum Zweck der Bekämpfung von Kindesmissbrauch[44] routinemäßig Fotodaten von Kunden gegen inkriminiertes Material KI-basiert abgleicht und im Verdachtsfall Strafanzeige gegen seine Kunden erstattet, wobei schon entsprechende Ermittlungsverfahren regelmäßig zu Hausdurchsuchungen und sozialen Existenzvernichtungen führen, auch wenn sich der Verdacht nicht bestätigt. Solche Screenings können zulässig sein.[45] Microsofts Verfahren ist allerdings besonders fehleranfällig; so führten im Jahr 2020 nur 52 % der Treffer zu einem Anfangsverdacht.[46] Dieses Beispiel verdeutlicht den hohen Schutzbedarf von Fotos. Diesen bejaht auch der EuGH, indem er ausführt, dass Art. 9 DSGVO unabhängig davon greift, ob der Verantwortliche in der Absicht handelt, besondere Kategorien personenbezogener Daten als solche zu verarbeiten, und ob die Daten eine dritte Person betreffen.[47]

Die Erhebungsvoraussetzungen des Art. 9 DSGVO mögen streng sein, ein grundsätzlicher Einwilligungsvorbehalt existiert jedoch nicht. Hingegen stellt Microsoft im DPA jede Verarbeitung biometrischer Daten unter Einwilligungsvorbehalt („er muss die Einwilligung der betroffenen Person einholen").[48] Die Einhaltung dessen wird dem Kunden vielfach rechtlich unmöglich sein und er wird werden wegen gesetzlicher Erlaubnistatbestände keinen Anspruch auf Einwilligungen haben, sodass Microsoft die eigenen Kunden in Vertragsverstöße treibt. Erzwungene Einwilligungen wären unwirksam (Art. 4 Nr. 11 DSGVO). Unternehmen werden so regelmäßig von Microsoft vor die Wahl gestellt, entweder Microsoft 365 nicht zu nutzen oder gegen das DPA zu verstoßen.

31 https://api.servicetrust.microsoft.com/api/v2/downloadDocuments/6471c92a-d274-4188-914a-033aa3efb296.
32 https://api.servicetrust.microsoft.com/api/v2/downloadDocuments/6471c92a-d274-4188-914a-033aa3efb296, S. 10-11.
33 https://go.microsoft.com/fwlink/?linkid=2274321&clcid=0x409.
34 https://aws.amazon.com/compliance/sub-processors.
35 EDSA, Recommendation 1/2020 zur Ergänzung von Übermittlungstools; DSK, Festlegung vom 24. 11. 2022 zu Microsoft 365, Anlage, S. 55.
36 DSK, Festlegung vom 24. 11. 2022 zu Microsoft 365, Anlage, S. 55.
37 DPA, S. 2, „Hinweise und Kontrollen beim Einsatz von Unterauftragsverarbeitern".
38 Vgl. *Spoerr*, in: Wolff/Brink/v. Ungern-Sternberg (Fn. 4), Art. 29 Rn. 3.
39 BGH, 15. 11. 2007 – III ZR 247/06, K&R 2008, 246 ff. = NJW 2008, 360, 364.
40 BGH, 15. 11. 2007 – III ZR 247/06, K&R 2008, 246 ff. = NJW 2008, 360, 363.
41 *Albers/Veit* in: Wolff/Brink/v. Ungern-Sternberg (Fn. 20), Art. 9 Rn. 44.
42 *Albers/Veit*, in: Wolff/Brink/v. Ungern-Sternberg (Fn. 20), Art. 9 Rn. 44.
43 EuGH, 26. 10. 2023 – C-307/22, K&R 2023, 793 ff., Rn. 52 – U.F.
44 Sog. CSAM-Material, d. h. child sexual abuse material.
45 Vgl. VO (EU) 2021/1232 zur Bekämpfung des sexuellen Missbrauchs von Kindern im Internet.
46 *Gundermann/Trinkwalder*, c't 2/2022, S. 50 ff.
47 EuGH, 4. 7. 2023 – C-252/21, K&R 2023, 492 ff., Rn. 68 f. – Meta.
48 DPA, S. 13, „Biometrische Daten".