Stellungnahme von Microsoft Deutschland zur datenschutzrechtlichen Bewertung von Microsoft 365 durch die DSK

Mit ihrem am 25.11.2022 veröffentlichten Bericht haben die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) Bedenken in Bezug auf die Datenschutzkonformität von Microsoft 365 geäußert. Wir nehmen die Bedenken der DSK ernst. Jedoch halten wir viele der datenschutzrechtlichen Einschätzungen sowie die Schlussfolgerungen der DSK für grundlegend falsch.

EINE VERANTWORTUNGSBEWUSSTE CLOUD FÜR EUROPA

Microsoft 365 ist datenschutzkonform einsetzbar

Bereits mit unserer Stellungnahme vom 17.08.2022 haben wir auf Bedenken von Datenschutzbehörden reagiert und erläutert, warum Microsoft Produkte und Dienste in der Privatwirtschaft und im öffentlichen Sektor (z. B. an Schulen) datenschutzkonform eingesetzt werden können. Wir haben Anregungen der DSK aufgenommen und am 15.09.2022 Verbesserungen an unserem Auftragsverarbeitungsvertrag (DPA) umgesetzt.

Dies unterstreicht, dass Microsoft auch weiterhin an einem konstruktiven und lösungsorientierten Austausch mit Datenschutzbehörden interessiert ist. Im Interesse der Transparenz befürwortet Microsoft die Veröffentlichung des detaillierten Berichts der DSK zum DPA vom 19.09.2022 (abzüglich gezielter Auslassungen zur Wahrung von Geschäftsgeheimnissen) zusammen mit den damaligen detaillierten Anmerkungen von Microsoft.

Technologie für Europa

Microsoft ist sich seiner Verantwortung als globaler Technologieanbieter mit mehr als einer Milliarde Nutzern in 140 Ländern bewusst. Die Cloud muss sicher sein und Datenschutz und digitale Souveränität respektieren. Dazu gehört, Europa bei der Umsetzung seiner digitalen Ambitionen zu unterstützen. Deshalb bieten wir Technologielösungen an, die europäischen Gesetzen und Erwartungen (in Bezug auf Sicherheit und Datenlokalisierung) entsprechen.[1] [2]

Bereits jetzt speichert Microsoft Kundendaten weitgehend regional in Rechenzentren in der EU. Zusätzlich – über die gesetzlichen Anforderungen hinaus – wird die Microsoft EU-Datengrenze bald in der EU ansässigen Kunden aus dem öffentlichen Sektor und Unternehmenskunden ermöglichen, ihre Daten innerhalb der EU zu speichern und auch zu verarbeiten.[3] [4] Die EU-Datengrenze wird Datenflüsse nach außerhalb der EU maßgeblich reduzieren und noch größere Transparenz mit detaillierter Dokumentation zu verbleibenden, notwendigen Datenflüsse herstellen.

[1] https://blogs.microsoft.com/eupolicy/2020/09/25/its-time-to-make-tech-fit-for-europe/
[2] https://blogs.microsoft.com/on-the-issues/2022/08/06/microsoft-adopts-european-cloud-principles/
[3] https://news.microsoft.com/de-de/unsere-antwort-an-europa-microsoft-ermoeglicht-speicherung-und-verarbeitung-von-daten-ausschliesslich-in-der-eu/
[4] https://blogs.microsoft.com/eupolicy/2021/12/16/eu-data-boundary-for-the-microsoft-cloud-a-progress-report/

MICROSOFTS ANTWORTEN AUF DIE BEDENKEN DER DSK

(1) Welcher Auslegungsmaßstab für die DS-GVO?

- Der Bericht der DSK wirft zunächst die grundsätzliche Frage auf, mit welchem Maßstab die DS-GVO auf konkrete, praktische Fragen anzuwenden ist.
- Einige Datenschutzbehörden in Deutschland scheinen die DS-GVO übermäßig risikoscheu und die Pflichten von Verantwortlichen ausufernd auszulegen.
- Verantwortliche agieren jedoch nicht in einer isolierten oder akademischen Datenschutzwelt. Die Ziele des Datenschutzes wollen sie praxisgerecht und regelkonform erreichen und gleichzeitig ihre dringlichen Aufgaben zum Wohle von Bürgern, Verbrauchern, Schülern etc. erfolgreich meistern.
- Ein ausufernder Aufsichtsansatz, der keinen Betroffenenschutz mehr verfolgt, macht Datenschutz zum dogmatischen Selbstzweck. Er überfordert und lähmt Verantwortliche (z. B. Schulleiter bei der Erstellung einer Datenschutz-Folgenabschätzung).
- Auch bremst er die erfolgreiche Digitalisierung Deutschlands und die Strategie für einen digitalen Aufbruch der Bundesregierung. Es drohen ein nicht zu verantwortender Rückstand des deutschen Bildungssystems und der Digitalisierung der deutschen Verwaltung.

(2) Anforderungen an die Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO

Bedenken der DSK: Microsoft legt nicht vollumfänglich offen, welche Verarbeitungen im Einzelnen stattfinden. Verantwortliche können auf dieser Grundlage ihren Rechenschaftspflichten nach Art. 5 Abs. 2 DS-GVO nur schwer nachkommen.

Antwort von Microsoft:

(a) Ausufernde Erwartungen an die Rechenschaftspflicht

- An die Rechenschaftspflicht der Verantwortlichen dürfen keine übermäßigen Anforderungen gestellt werden: Kunden müssen die technische Funktionsweise von Microsoft 365 nicht vollständig verstehen. Die reine technische Umsetzung kann durch den Auftragsverarbeiter selbst in gewissem Rahmen bestimmt werden.[5]
- Eine ausufernde Erwartung an Verantwortliche ist praxisfern und blockiert technischen Fortschritt, selbst wenn dieser der Verbesserung der eingesetzten Technologie oder ihrer Sicherheit dient.
- Microsoft 365 ist eine leistungsstarke Produktfamilie mit einer Vielzahl an Funktionalitäten (Microsoft Teams, Word, Excel, PowerPoint und mehr). Als Gesamtlösung ist Microsoft 365 notwendigerweise technisch komplexer als eine Teillösung (z. B. nur Videotelefonie).

(b) Detailgrad der von Microsoft bereitgestellten Dokumentation

[5] siehe z.B. den Europäische Datenschutzausschuss und seine „Guidelines 07/2020 on the concepts of controller and processor in the GDPR", Rn. 40: „*Essential means" are traditionally and inherently reserved to the controller. While non-essential means can also be determined by the processor, essential means are to be determined by the controller. […] "Non-essential means" concern more practical aspects of implementation, such as the choice for a particular type of hard- or software or the detailed security measures which may be left to the processor to decide on.*").

- Microsoft stellt die nötige Transparenz über Verarbeitungstätigkeiten durch umfangreiche Dokumentation her. Diese ist teils für die Öffentlichkeit[6] und teils nur für Kunden[7] zugänglich. Noch mehr technische Details über die bereitgestellte Dokumentation hinaus schaffen keine größere Klarheit für Verantwortliche.

- Die DSK hat nach unserem Eindruck im Rahmen ihrer Untersuchung den vollen Umfang dieser Kunden zur Verfügung stehenden Dokumentation nicht beachtet. Es bleibt unklar, in welchem Detailgrad Verantwortliche die technische Funktionsweise von Microsoft 365 nach Auffassung der DSK verstehen müssen, um ihren Rechenschaftspflichten nachzukommen.

(3) Festlegen des Vertragsgegenstandes

Bedenken der DSK: Microsoft sieht programmatisch im DPA keine ausreichende Konkretisierung der durch den Kunden intendierten Verarbeitungstätigkeiten vor, und dies genügt nicht Art. 28 Abs. 3 Satz 1 DS-GVO.

Antwort von Microsoft:

- Microsoft teilt diese Einschätzung der DSK nicht. Das DPA enthält Informationen gemäß Art. 28 Abs. 3 Satz 1 DS-GVO im Abschnitt „Verarbeitungsdetails“ (welcher auf das Verarbeitungsverzeichnis des Kunden gemäß Art. 30 DS-GVO verweist) und in Anhang B. Dies entspricht den Anforderungen des unabhängigen ISO/IEC 19944 Standards an die Darstellung von Datenerhebungskategorien und Nutzungszwecken im Kontext der Cloud.

- Die Kontrolle über diese Verarbeitungsdetails liegt beim Kunden. Er bestimmt, welche Daten er wie lange für welchen Zweck in der Microsoft Cloud verarbeiten möchte.

- Das DPA und die standardisierte Leistungserbringung der Microsoft Cloud sind darauf ausgerichtet, alle legalen vertragsgemäßen Verarbeitungen durch Kunden zu ermöglichen. Deshalb würde eine weitere Konkretisierung der „Verarbeitungsdetails“ keine Änderung der Leistungserbringung durch Microsoft zur Folge haben. Microsoft erfüllt unabhängig von den Datenkategorien den gleichen hohen Standard an Sicherung, Sicherheit und Funktionalität.

- Eine weitere Konkretisierung im DPA würde in der Praxis dazu führen, dass die gemachten Angaben regelmäßig veralten und somit unrichtig würden.

(4) Verarbeitungen für Geschäftstätigkeiten von Microsoft

Bedenken der DSK: Das DPA enthält unzureichend eingegrenzte Verarbeitungsbefugnisse der möglichen Geschäftstätigkeiten, und dies stellt öffentliche Stellen bei der Erfüllung ihrer Rechenschaftspflichten vor erhebliche Hindernisse.

Antwort von Microsoft:

(a) Widersprüchliche Auslegung der DS-GVO seitens der Behörden in Europa

- Wie die DSK anerkennt, beurteilen europäische Aufsichtsbehörden unterschiedlich, in welcher Position (Verantwortlicher oder Auftragsverarbeiter) Cloud-Anbieter im Zusammenhang mit der Diensterbringung personenbezogene Daten verarbeiten dürfen.

[6] https://www.microsoft.com/de-de/microsoft-365/business/data-security-privacy-germany; https://www.microsoft.com/licensing/terms/productoffering/Microsoft365/all; https://learn.microsoft.com/de-de/microsoft-365/?view=o365-worldwide

[7] https://servicetrust.microsoft.com

- Dieser unaufgelöste Dissens der nationalen Behörden stellt international agierende Unternehmen vor eine faktisch unüberwindbare Hürde.

(b) Rechtsgrundlage

- Microsoft aggregiert lediglich pseudonymisierte, personenbezogene Daten und berechnet Statistiken bezogen auf Kundendaten. Dies resultiert in nicht-personenbezogenen Daten, welche Microsoft dann für folgende Geschäftstätigkeiten nutzt: (i) Abrechnungs- und Kontoverwaltung, (ii) Vergütung, (iii) interne Berichterstattung und Geschäftsmodellierung und (iv) Finanzberichterstattung. Die Rechtsgrundlagen, die bereits den Einsatz von Microsoft 365 durch den Verantwortlichen (Kunden) rechtfertigen, decken auch diese Vorgänge ab. Microsoft wird seine Kunden durch geeignete Unterlagen und Dokumentation zu dieser Auffassung unterstützen.

- Die DSK übersieht auch, dass der Auftragsverarbeiter selbst Adressat der Verpflichtungen gemäß Art. 32 DS-GVO ist und für deren Durchführung nicht von einer Rechtsgrundlage des Verantwortlichen abhängig sein kann. Dies betrifft mindestens Aspekte der Weiterentwicklung, Produktstrategie und Kapazitätsplanung. Es ist daher widersprüchlich und nicht im Einklang mit der Systematik der DS-GVO, (i) Verantwortlichen Verarbeitungen und Maßnahmen zuzurechnen, zu deren Erbringung Auftragsverarbeiter verpflichtet und durch eine eigenständige Bußgeldnorm bedroht sind und (ii) für diese falsch zugeordneten Verarbeitungen und Maßnahmen dann eine fehlende Rechtsgrundlage anzumahnen.

(c) Keine „eigenen Zwecke“ losgelöst von Kundeninteressen

- Von „eigenen Zwecken“ Microsofts zu sprechen ist irreführend. Die Verarbeitung für Geschäftstätigkeiten ist durch die Bereitstellung der Produkte und Dienste an den Kunden veranlasst und erfolgt auch im Interesse der Kunden.

- Die vorgesehenen Geschäftstätigkeiten sind notwendiger Teil der Bereitstellung, Abrechnung und Planung jedes komplexen Cloud-Produktes, nicht nur bei Microsoft. Microsoft hebt sich durch seine Transparenz in dieser Frage hervor.

- Die DSK hat Bedenken geäußert, dass der Text des DPA (Stand 15.09.2021) Microsoft zu weitgehende Rechte einräume. Daraufhin hat Microsoft die Formulierungen im DPA (Stand 15.09.2022) eingeschränkt. Die genaueren Formulierungen entsprachen ohnehin der tatsächlichen, eingeschränkten Praxis Microsofts in Bezug auf diese Verarbeitungen.

(d) Rein akademische Diskussion

- Die datenschutzrechtliche Relevanz der Geschäftstätigkeiten ist minimal:
    - Microsoft greift nicht auf Inhaltsdaten von Kunden zu;
    - Wie oben dargestellt, ist zum Zeitpunkt der Nutzung der nicht-personenbezogenen Daten für die Geschäftstätigkeiten von Microsoft der Anwendungsbereich der DS-GVO bereits verlassen; und
    - Microsoft sagt Kunden im DPA zu, dass (i) die Datennutzung minimiert wird (etwa durch die Pseudonymisierung bereits bei der Erhebung) und (ii) keine Nutzung für sonstige (etwas Werbe- oder Profilierungszwecke) erfolgt.

- Bei vernünftiger Betrachtung handelt es sich hier um eine rein akademische, den Interessen der Betroffenen und Kunden in keiner Weise dienende Diskussion um hoch standardisierte, industrietypische und datenschutzrechtlich neutrale Verarbeitungen.

- Die Aussage, ein Anbieter für die öffentliche Hand dürfe keine eigenen Zwecke verfolgen, ist jedenfalls in Bezug auf Microsofts Geschäftstätigkeiten rechtlich nicht haltbar. Sie steht

zumindest in dieser Pauschalität diametral im Gegensatz zur gesellschaftlich und politisch geforderten Digitalisierung der öffentlichen Hand.

(5) Mutmaßlicher Konflikt zwischen Weisungsbindung des Auftragsverarbeiters und Offenlegungs-Verpflichtungen drittstaatlichen Rechts (CLOUD Act, FISA 702)

Bedenken der DSK: Das DPA schränkt das Weisungsrecht des Kunden in Bezug auf Offenlegungen der im Auftrag verarbeiteten Daten ein.

Antwort von Microsoft:

(a) Weisungen an Auftragsverarbeiter bei Cloud-Diensten

- Das DPA wird zwischen Kunden und Microsoft vereinbart. Es enthält die allgemeinen Weisungen sowie Modalitäten für weitere Weisungen des Kunden an Microsoft.
- Bei Cloud-Diensten ist es Industriestandard, dass (i) sich der Kunde die Erbringung der Dienste wie vertraglich und in der Produktdokumentation beschrieben als Weisung zu eigen macht; (ii) laufende Weisungen des Kunden über die Konfiguration und Nutzung des Dienstes durch den Kunden erfolgen; und (iii) darüber hinaus die Möglichkeit einer einvernehmlichen Vertragsanpassung besteht.
- Diese Art Weisungen zu erteilen ist nötig, damit Kunden die gewünschten Vorteile der Cloud nutzen können: Kunden wollen Teile des Betriebs ihrer IT an einen Anbieter von Multi-Tenant-Lösungen auslagern, um an Skaleneffekten (Kostenersparnis, Innovation etc.) Teil zu haben.

(b) CLOUD Act, FISA 702 etc.

- Es zeichnet sich bereits eine datenschutzrechtliche Lösung des gesamten Themenkomplexes nach Art. 45 DS-GVO ab: Die Europäische Kommission arbeitet zurzeit an einem Angemessenheitsbeschluss, wonach das Datenschutzniveau in den USA als angemessen bewertet werden soll. Grundlage dafür ist, dass die USA mit Wirkung ab dem 7. Oktober 2022 bedeutende Änderungen an ihren Rechtsvorschriften vorgenommen haben und noch vornehmen werden, welche das Schrems-II-Urteil in vollem Umfang berücksichtigen.
- Herausgabeverlangen von Behörden außerhalb der EU betreffen nicht nur Microsoft: Neben anderen amerikanischen Technologieanbietern können auch Anbieter mit Stammsitz innerhalb der EU (z. B. Unternehmen des DAX-Index) US-Überwachungsgesetzen unterliegen, etwa durch eine Präsenz in oder minimalen Kontakt mit den USA.

(6) Umsetzung technischer und organisatorischer Maßnahmen nach Art. 32 DS-GVO

Bedenken der DSK: Es bleiben Rechtsunsicherheiten, da die Garantien über „Sicherheitsmaßnahmen“ formal nur eine Teilmenge der vertragsgegenständlichen personenbezogenen Daten erfassen.

Antwort von Microsoft:

- Microsoft teilt diese Einschätzung der DSK nicht. Microsoft verpflichtet sich zur Einhaltung von TOMs für alle verarbeiteten Daten und dass die Maßnahmen den Anforderungen von ISO 27001, ISO 27002 und ISO 27018 entsprechen. Dies gilt für alle Services, insbesondere auch die sogenannten Non-Core Services, die im Übrigen in der

Gesamtschau der vom DPA abgedeckten Leistungen eine sehr kleine Teilmenge bilden. Weitere Details dazu finden Kunden im Service Trust Portal.[8]

- Zusätzlich enthalten das DPA und die Dokumentation im Service Trust Portal weitergehende Verpflichtungen zu TOMs für die wesentlichen Leistungsgegenstände: Core Online Services und Professional Services.
- Als Teil von Microsofts Bekenntnis dazu, die Vertragsbedingungen mit Hinblick auf Feedback von Aufsichtsbehörden und Kunden weiter zu verbessern, wird Microsoft untersuchen, ob weitere organisatorische Maßnahmen in die Vertragsbedingungen aufgenommen werden können, welche Microsoft in der Praxis bereits für personenbezogene Daten außerhalb von Kundendaten in Core Online Services und Professional Services anwendet.

(7) Löschung und Rückgabe personenbezogener Daten

Bedenken der DSK: Rückgabe- und Löschverpflichtung entsprechen nicht in jedem Fall den gesetzlichen Anforderungen aus Art. 28 Abs. 3 UAbs. 1 Satz 2 Buchstabe g DS-GVO.

Antwort von Microsoft: Das DPA ermöglicht dem Kunden sehr wohl in datenschutzkonformer Weise die Löschung sowie die Extraktion von Daten (die bei Cloud-Diensten die einzige einer Rückgabe entsprechende sinnvolle Option ist).[9]

(8) Informationen über Unterauftragsverarbeiter

Bedenken der DSK: Microsoft informiert nur darüber, dass Änderungen an Unterauftragsverarbeitern geplant sind, nicht jedoch welche Änderungen konkret beabsichtigt sind. Die bereitgestellten Informationen sind nicht detailliert genug.

Antwort von Microsoft:

- Microsoft teilt diese Einschätzung der DSK nicht. Microsoft stellt Kunden jederzeit eine Übersicht der von Microsoft eingesetzten Unterauftragsverarbeiter zur Verfügung.[10]
- Bereits in der Vergangenheit konnten Kunden Updates per E-Mail abonnieren.
- Darüber hinaus ist Microsoft dem Wunsch der DSK nachgekommen, ein Benachrichtigungsverfahren per E-Mail einzuführen, welches alle Kunden von Microsoft 365 aktiv über Aktualisierungen informiert. Diese Benachrichtigung verweist auf die online verfügbare Liste der Unterauftragsverarbeiter, welche Änderungen konkret und leicht nachvollziehbar benennt.
- Microsoft arbeitet bereits an einer detaillierteren Liste von Unterauftragsverarbeitern.

[8] https://servicetrust.microsoft.com
[9] https://learn.microsoft.com/en-us/compliance/assurance/assurance-data-retention-deletion-and-destruction-overview
[10] https://go.microsoft.com/fwlink/?linkid=2208809

(9) Datenübermittlungen in Drittstaaten: Zusätzliche Schutzmaßnahmen entsprechend der Schrems II-Rechtsprechung

Bedenken der DSK: Die zusätzlichen Schutzmaßnahmen im DPA mit Bezug auf Datentransfers reichen nicht aus.

Antwort von Microsoft:

- Microsoft teilt diese Einschätzung der DSK nicht. Es ist rechtlich nicht geboten, jedes theoretische Restrisiko, etwa eines behördlichen Zugriffs im Drittstaat, im Zusammenhang mit einer internationalen Datenübermittlung auszuschließen.
- Microsofts EU-Datengrenze wird das aktuell bestehende Restrisiko durch maßgeblich reduzierte Datenflüsse (von Kundendaten und personenbezogenen Daten) nach außerhalb der EU weiter mindern.
- Der erwartete Angemessenheitsbeschluss der EU-Kommission wird die Notwendigkeit von zusätzlichen Schutzmaßnahmen für Datentransfers in die USA komplett entfallen lassen.
- Microsoft setzt gemäß Art. 32 DS-GVO und dem aktuellen Stand der Technik umfangreiche, differenzierte und wirkungsvolle technische und organisatorische Maßnahmen ein.
- Mit den vertraglichen Zusagen im DPA (vgl. insbesondere Anhang C) geht Microsoft über die rechtlichen Anforderungen hinaus, um die Daten seiner Kunden zu schützen.