Microsoft

11. August 2022

Stellungnahme von Microsoft Deutschland zur Datenschutzkonformität von Microsoft 365 und Microsoft Teams

Stellungnahmen öffentlicher Stellen, insbesondere die einiger Datenschutzbehörden, erwecken bereits seit längerem möglicherweise den Eindruck, Microsoft 365 und Microsoft Teams für Unternehmen und die öffentliche Hand (insb. den Bildungssektor) könnten nicht datenschutzkonform eingesetzt werden oder seien gar selbst nicht datenschutzkonform. Derartige Aussagen sind nicht richtig, wie wir nachfolgend erläutern möchten:

RICHTIG IST:	
1	Microsoft bietet **zukunftsweisende Technologien mit branchenführendem Sicherheitsstandard,** auf die Deutschland sich auch in Krisenzeiten **verlassen kann**. Unsere Technologien **stärken Deutschland**. Nur konsequente Digitalisierung mit Technik auf dem Stand der Zeit wird es Deutschland ermöglichen, seinen **Wohlstand** zu wahren, seine **Werte** zu verteidigen und seinen gesellschaftlichen Aufgaben erfolgreich nachzukommen (etwa dem **Bildungsauftrag**).
2	Microsoft ist ein **zuverlässiger und verantwortungsbewusster Partner**.[1] Unser **Unternehmensziel** ist es, jede Person und jede Organisation zu befähigen, mehr zu erreichen. Unser **Geschäftsmodell** besteht darin, durch produktive Technologie **zum Erfolg unserer Kunden beizutragen**.
3	Alle Microsoft Produkte und Dienste können in der Privatwirtschaft und im öffentlichen Sektor (z. B. an Schulen) **datenschutzkonform eingesetzt werden** und sind auch **selbst datenschutzkonform**. Microsoft hält die Anforderungen des geltenden Datenschutzrechts ein.
4	Microsoft bietet Kunden **vertragliche Zusagen und technische Mittel**, um Microsoft Produkte und Dienste datenschutzkonform nutzen zu können, insbesondere: ➢ vertragliche Zusagen, dass Microsoft: ➢ Kundendaten nicht für sachfremde Zwecke wie Werbung verwendet; ➢ rechtliche Schutzmaßnahmen gegen unrechtmäßige Herausgabeverlangen von Behörden oder Dritten ergreift;[2] ➢ Dritten, falls überhaupt, nur im vertraglich vorgesehenen Umfang Zugriff auf Kundendaten gewährt; ➢ für die Verschlüsselung von Kundendaten verwendete Plattform-Schlüssel nicht preisgibt und Dritten auch nicht die Möglichkeit einräumt, die Verschlüsselung zu überwinden; und ➢ keinen Grund zur Annahme hat, durch anwendbare Gesetze an der Einhaltung der Verpflichtungen unter den Standardvertragsklauseln gehindert zu sein; und ➢ Möglichkeiten zur technischen Absicherung von Daten (z. B. Verschlüsselung, Pseudonymisierung, differenzierte Zugriffsberechtigungen und die Automatisierung von sicherheitsrelevanten Prozessen) nach dem aktuellen Stand der Technik.
5	Bereits jetzt speichert Microsoft Daten weitgehend regional in **Rechenzentren in der EU**. Zusätzlich – obwohl es keine gesetzliche Verpflichtung dazu gibt – wird die Microsoft **EU Data Boundary** es künftig in der EU ansässigen Kunden aus dem öffentlichen Sektor und Unternehmenskunden ermöglichen, **ihre Daten innerhalb der EU zu verarbeiten und zu speichern**.[3] [4]
6	**Microsoft ist im Bereich der Cybersecurity führend** und hat eine Vielzahl technischer Maßnahmen implementiert, um **Kundendaten vor Cyberattacken zu schützen**. Hierzu gehören unter anderem Technologien zur Erkennung und Vereitelung von Attacken und unberechtigten Datenzugriffen. Microsoft wird zwischen 2021 und 2025 **$20 Milliarden in Cybersecurity investieren**.[5]

[1] https://news.microsoft.com/wp-content/uploads/prod/sites/358/2022/08/RPC-Framework-2.pdf
[2] https://blogs.microsoft.com/on-the-issues/2020/11/19/defending-your-data-edpb-gdpr/
[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/
[5] https://cloudblogs.microsoft.com/industry-blog/microsoft-in-business/security/2021/09/23/microsoft-expands-on-cybersecurity-commitments-for-u-s-government-agencies/

7	Microsoft unterzieht sich mindestens einmal im Jahr **Überprüfungen von international anerkannten unabhängigen Auditoren**. Diese überprüfen auf Grundlage des **ISO/IEC 27001-Standards**, ob Microsoft die Richtlinien und Verfahren für Sicherheit, Datenschutz, Kontinuität und Konformität gewährleistet. Weiterhin erfüllt Microsoft den **Anforderungskatalog Cloud Computing (C5)** des BSI[6] und verfügt über eine Vielzahl weiterer relevanter Zertifizierungen und Attestierungen wie z. B. den **ISO/IEC 27018-Standard für Datenschutz in der Cloud** und den **ISO/IEC 27701-Standard zum Datenschutz-Risikomanagement**.[7] [8]
UNRICHTIG SIND FOLGENDE AUSSAGEN:	
1	***„Die Cloud ist unsicher."***
	Richtig ist vielmehr: ➢ Die Cloud-Nutzung führt zu einer **erhöhten Sicherheit und Verfügbarkeit von Daten** im Vergleich zu on-premises Lösungen. Der aktuelle Krieg in der Ukraine zeigt, dass Länder, die eine Cloud-Strategie verfolgen, **weniger von Cyber-Angriffen betroffen** sind.[9] ➢ Vorschriften zum technologischen Schutz von Daten (z. B. Art. 32 DS-GVO) machen es erforderlich, den Schutz an die technischen Gegebenheiten fortwährend anzupassen und weiterzuentwickeln. Cloud-Lösungen bilden fortlaufend die **aktuellen Sicherheits-anforderungen** ab.
2	***„Die US-Regierung liest alles mit."***
	Richtig ist vielmehr: ➢ Ein Interesse von US-Behörden z. B. an **Daten aus einem Schulunterricht** in Deutschland **kann nicht ernsthaft behauptet werden.** ➢ Eine umfangreiche Auswertung öffentlich verfügbarer Dokumente von US-Regierungs-Behörden zur Nutzung von **§702 des Foreign Intelligence Surveillance Act (FISA) in der Praxis**[10] belegt dagegen: ➢ Es gibt **keinen Anhaltspunkt** dafür, dass die US-Regierung §702 FISA nutzt, um (i) Industriespionage zu betreiben oder US-amerikanische wirtschaftliche Interessen zu verfolgen oder (ii) Regierungen im Europäischen Wirtschaftsraum ins Visier zu nehmen; und ➢ Die US-Regierung nutzt §702 FISA im Wesentlichen zur Sammlung von Informationen für Ermittlungen zu **schwerwiegenden Bedrohungen der nationalen Sicherheit**, wie Terrorismus, Cybersecurity-Angriffe und Waffen-proliferation. ➢ Microsoft hat die **US-Regierung mehrmals erfolgreich verklagt,** um die Datenschutz-Rechte seiner Kunden zu verteidigen.[11] Microsoft bezieht auch weiterhin Stellung, um Kundendaten zu verteidigen.[12] ➢ Microsofts „Transparency Reporting" zeigt, dass eine erzwungene Herausgabe von außerhalb der USA befindlichen Unternehmensdaten an amerikanische Strafver-folgungsbehörden in nur **sehr wenigen Fällen** erfolgt ist.[13] ➢ Die pauschale Empfehlung seitens einzelner Behörden, nur Anbieter aus der EU zu nutzen, verkennt im Übrigen, dass auch Anbieter mit Stammsitz innerhalb der EU US-Überwachungsgesetzen unterliegen können, z. B. durch eine Präsenz in oder minimalen Kontakt mit den USA. Behörden dürfen nicht mit **zweierlei Maß** messen und unterliegen dem **Objektivitätsgebot**.
3	***„Datentransfers in Drittstaaten wie die USA sind unzulässig."***

[6] https://docs.microsoft.com/de-de/compliance/regulatory/offering-c5-germany
[7] https://news.microsoft.com/de-de/im-daten-dschungel-zertifizierungen-der-microsoft-cloud/
[8] https://docs.microsoft.com/de-de/compliance/regulatory/offering-home
[9] https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/
[10] https://www.microsoft.com/en-us/trust-center/privacy (auf "Learn about Compliance with the EU transfer Requirements" klicken)
[11] 2014: https://blogs.microsoft.com/on-the-issues/2014/02/03/providing-additional-transparency-on-us-government-requests-for-customer-data/#sm.00059ylyl10cvctusyt1n87pf9egh; und https://blogs.microsoft.com/on-the-issues/2014/05/22/new-success-in-protecting-customer-rights-unsealed-today; 2016: https://blogs.microsoft.com/eupolicy/2016/09/05/our-search-warrant-case-microsofts-commitment-to-protecting-your-privacy; 2017: https://blogs.microsoft.com/on-the-issues/2017/10/23/doj-acts-curb-overuse-secrecy-orders-now-congress-turn
[12] https://www.washingtonpost.com/opinions/2021/06/13/microsoft-brad-smith-trump-justice-department-gag-orders/
[13] https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report und https://www.microsoft.com/en-us/corporate-responsibility/us-national-security-orders-report

	Richtig ist vielmehr: ➢ Die **DS-GVO erlaubt Übermittlungen in Drittstaaten, einschließlich in die USA,** unter Nutzung von geeigneten Garantien (z. B. Standardvertragsklauseln 2021/914 und zusätzliche Maßnahmen). ➢ Dabei ist eine Risikoanalyse im Lichte der Schrems II-Rechtsprechung des EuGH durchzuführen und es sind ggf. zusätzliche Maßnahmen zu implementieren. ➢ Microsoft bietet für Datenübermittlungen in Drittstaaten **zusätzliche, rechtlich anerkannte Schutzmechanismen**, wie zusätzliche vertragliche Klauseln. ➢ Es ist rechtlich nicht geboten, jedes theoretische Restrisiko, etwa eines behördlichen Zugriffs im Drittstaat, im Zusammenhang mit einer internationalen Datenübermittlung auszuschließen.[14] Einen **„Null-Risiko-Ansatz"** zu fordern, ist **unverhältnismäßig** und steht weder im Einklang mit der DS-GVO noch mit den Regelungen der Standardvertragsklauseln[15], der Schrems II-Rechtsprechung und den Empfehlungen des Europäischen Datenschutzausschusses für Maßnahmen zu Datenübermittlungen in Drittstaaten[16].
4	***„Diagnosedaten sind nicht notwendig und schädlich."***
	Richtig ist vielmehr: ➢ **Diagnosedaten sind notwendig, um Produkte und Dienste sicher und stabil zu betreiben**. Unsere Kunden erwarten zurecht, dass sie unsere Produkte und Dienste vertragsgemäß und sicher nutzen können. Die verantwortungsvolle Nutzung von Diagnosedaten trägt dazu bei. ➢ Kunden nutzen viele verschiedene technische Infrastrukturen. Die Verarbeitung von Diagnosedaten ist daher sehr nützlich, um **die Anfälligkeit für Fehler und die Wahrscheinlichkeit von Sicherheitsrisiken zu verringern**. ➢ Diagnosedaten werden oft falsch verstanden und **mit Funktionsdaten verwechselt**, z. B., weil entsprechende (Fehl-)Einordnungen außer Acht lassen, dass für die vertraglich vereinbarte und daher vom Kunden auch zurecht erwartete Stabilität und Sicherheit der jeweiligen Anwendung (und damit für deren ordnungsgemäßes Funktionieren) bestimmte Daten erfasst werden müssen, um die gewünschte Aktion des Nutzers auszuführen.
5	***„Microsoft überwacht die Nutzer seiner Produkte und Dienste."***
	Richtig ist vielmehr: ➢ Die technische Verbindung zwischen Nutzer und Microsoft (z. B. über Server und Rechenzentren) ist in vielen Fällen **zwingende Voraussetzung für die vertraglich geschuldete Diensterbringung.** Nichts davon kann als ein Ausspähen von Kunden angesehen werden. ➢ Cloud-Dienste funktionieren nur, wenn Nutzeraktionen übermittelt werden, damit die jeweilige Reaktion der Applikation ausgeführt werden kann (z. B. eine Übersetzung). **Das ist technisch mit Verarbeitungen bei on-premises Lösungen vergleichbar.**
6	***„Einen Dienst darf nur einsetzen, wer die technische Funktionsweise des Dienstes voll versteht."***

[14] Vgl. Stefan Brink et al.: "Auf der anderen Seite geht der EuGH zu weit, wenn er etwa die nur abstrakte und hypothetische Möglichkeit des Zugriffs nicht-europäischer Sicherheitsbehörden ohne konkretes und reales Risiko für persönliche Daten von Europäern als Killerkriterium für globalen Datenaustausch begreift." (https://www.faz.net/aktuell/wirtschaft/digitec/so-war-die-dsgvo-nicht-gemeint-was-bei-ihrer-anwendung-schieflaeuft-18179521.html; veröffentlicht am 18.07.2022)

[15] Siehe insbesondere auch Fußnote 12 der EU Standardvertragsklauseln 2021/914.

[16] Siehe Empfehlungen 01/2020 des Europäischen Datenschutzausschusses zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten, Rn. 47.

Richtig ist vielmehr:

- Eine Analyse jedes einzelnen Prozesses eines Diensts durch den Verantwortlichen/Nutzer ist **datenschutzrechtlich weder erforderlich noch geboten** und geht weit über die Rechenschaftspflichten unter Art. 5 (2) DS-GVO hinaus. Entscheidend ist, dass die verantwortliche Stelle die notwendigen Informationen besitzt, um seinen Rechenschaftspflichten nachzukommen.
- Das Errichten einer solchen Hürde würde das Ende vieler Hyperscaling Technologien im Cloud-Umfeld bedeuten, denen ein Wissensgefälle zwischen dem Anbieter der Technologie und dem Nutzer inhärent ist. Dies zu fordern wäre **unrealistisch und technologiefeindlich.** Entsprechende Anforderungen können in kaum einem maßgeblich von Technik beeinflussten Lebensbereich eingehalten werden.
- Es ist anerkannt, dass die reine **technische Umsetzung** durch den Auftragsverarbeiter selbst in gewissem Rahmen bestimmt werden kann.[17]

[17] Siehe z. B. der Europäische Datenschutzausschuss in seinen „Guidelines 07/2020 on the concepts of controller andprocessor 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.*").