Digitales Lernen möglich machen – Datenschutz & Co.

Cornelia Schneider-Pungs
Industry Advisor
Microsoft Deutschland GmbH

Datenschutz ist ein Grundrecht

Unser Ansatz zum Schutz der Privatsphäre beruht darauf, **Nutzer*innen die Kontrolle und Transparenz über die Erfassung, Nutzung und Verarbeitung der eigenen Daten** zu geben.

Microsoft war eines der ersten Unternehmen, die die grundlegenden Rechte der DSGVO allen Kunden weltweit bereitgestellt hat.

Mythen gegen Realität

Wir gewähren keiner staatlichen Stelle direkten, ungehinderten Zugang zu den Daten unserer Kunden.

Falls eine Regierung Kundendaten von uns verlangt, muss sie den geltenden rechtlichen Verfahren folgen.

Wir werden Forderungen nur dann nachkommen, wenn wir rechtlich eindeutig dazu gezwungen sind. Unser erster Schritt besteht immer in dem Versuch, unsere Kunden darüber zu informieren oder die Anfragen an sie weiterzuleiten.

Bildung ist wichtig, Datenschutz auch.

Lernen mit Laptop und Tablet: Der digitale Unterricht ist in die direkte Umsetzung gekommen. Digitale Konzepte erweitern die Gestaltungsmöglichkeiten im Unterricht und Studium und fördern den Erwerb von Skills für das digitale Zeitalter.

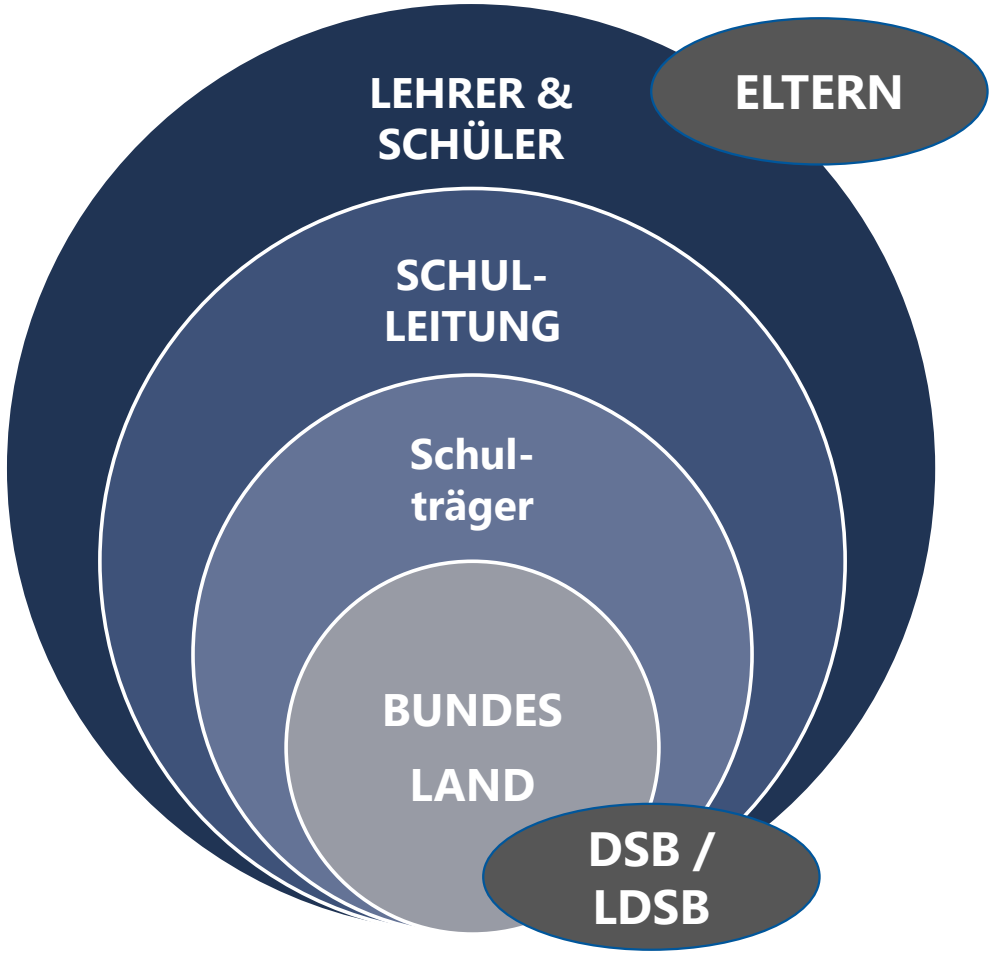
Wir sind davon überzeugt, dass unsere Angebote im Einklang mit den bestehenden Anforderungen an Datensicherheit und -schutz genutzt werden können.

Microsoft Teams ist zukunftsorientiert, zuverlässig und sicher. Aus unserer Sicht ist es auch in Bildungseinrichtungen DSGVO-konform einsetzbar. Die Übertragung von Daten erfolgt verschlüsselt.

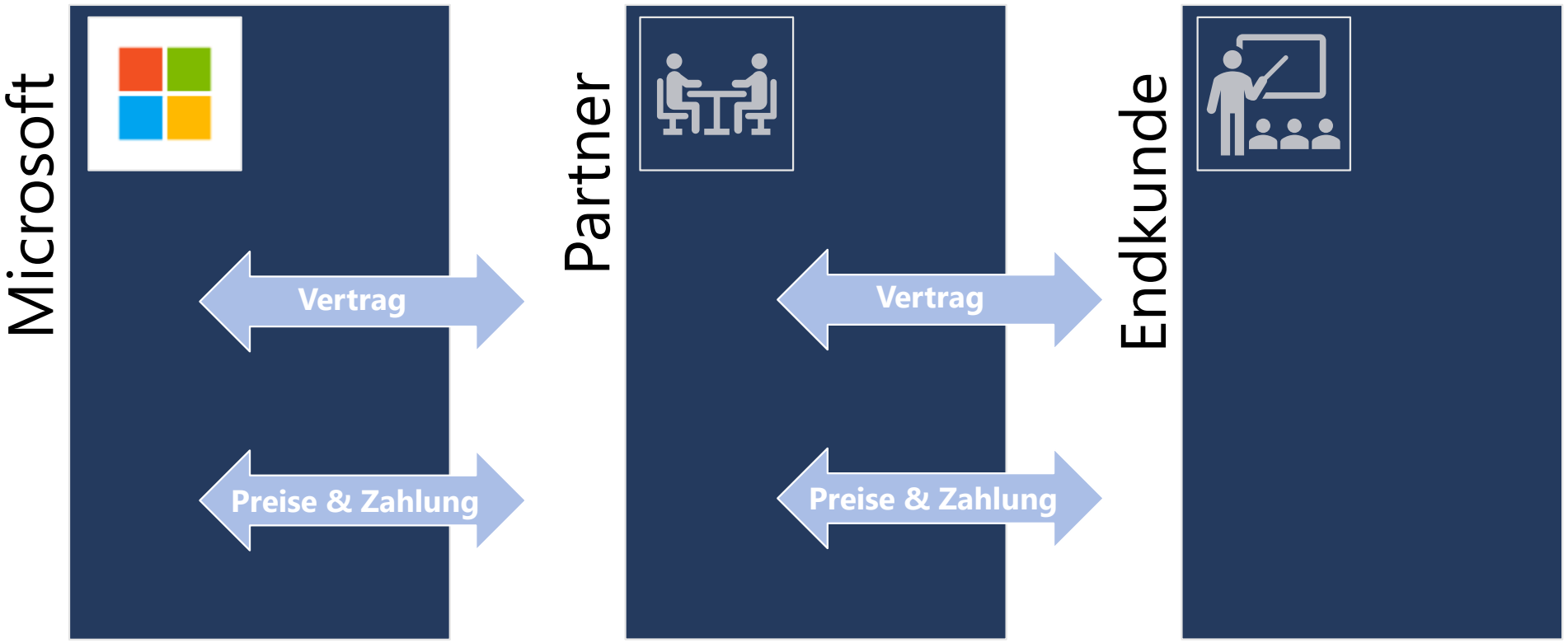
Jede Schule sollte in der Lage sein, ihren Lehrer*innen und Schüler*innen sichere digitale Lösungen zur Verfügung zu stellen. Bildungseinrichtungen sind Schutzräume, die auch Schutz vor Cyberattacken und Cyberkriminalität bieten müssen. Unsere Rechenzentren erfüllen die hohen Standards des Bundesamts für Sicherheit in der Informationstechnik (BSI).

Unsicherheiten beim Umgang mit Datenschutz-Regeln dürfen nicht auf dem Rücken der Lehrer*innen und Schüler*innen ausgetragen werden. Bildung ist wertvoll, Datenschutz auch – beides ist kein Widerspruch.

Wer ist verantwortlich?



Was ist vertragsrechtlich relevant?



Product Terms (PT), Online Services Terms (OST), Datenschutz-Addendum (DPA)

Licensing Terms | Microsoft Volume Licensing

Geteilte Verantwortung / Shared Responsibility

- Volumenlizenzverträge (bspw. EES)
- OST + DPA (inkl. TOM)
- Zusätzliche technische Garantien und Möglichkeiten (Datenspeicherung in der Region / Georedundanz, *Verschlüsselung*, etc.)
- Trust Center
- Zertifizierungen & Audits
- Zusätzlicher *Rechtsschutz*

- Bestimmen des Einsatzszenarios
- Beschluss der Schulkonferenz
- EDV-Nutzungsordnung
- Verzeichnis der Verarbeitstätigkeiten
- Nutzungsvereinbarung/en Dienstvereinbarung/en
- Datenschutzfolgeabschätzung
- (Zusätzliche) technische und organisatorische Maßnahmen (TOM)

Datenschutz: Möglicher Prozess

- Sicherstellung der Rechtmäßigkeit (Vertrag, Einwilligung etc.)
- Definition der technischen und organisatorischen Maßnahmen (TOM) incl. Schulungen (!)
- Dokumentation und Nachweisführung (VVT, DSFA etc.)

Bestimmungen für Onlinedienste (OST)

OST
aka.ms/ost

Definitionen

Core-Onlinedienste, Kundendaten, Datenschutznachtrag, Externer Nutzer, Instanz, Lizenzierungswebsite, Lizenziertes Gerät, Netzwerkserver, Nicht von Microsoft stammendes Produkt, Onlinedienste, Betriebssystemumgebung, OST, Personenbezogene Daten, Vorschauversionen, Professional Services, Daten zu Professionellen Dienstleistungen, SL, Unterauftragsverarbeiter, Supportdaten

Geschäftsbedingungen

- Lizenzierung der Onlinedienste
- Nutzung der Onlinedienste
- **Datenschutz und Sicherheit**
- Verwendung von Software mit dem Onlinedienste
- Technische Beschränkungen
- Import-/Exportdienste
- Schriftartkomponenten
- Änderungen und Verfügbarkeit der Onlinedienste
- Sonstige

Spezifische Bestimmungen

- Azure
- Dynamics 365
- Office 365
- Sonstige Online Dienste

Anhang zum Datenschutz (DPA)

DPA
aka.ms/dpa

Definitionen

Kundendaten, Diagnosedaten, Datenschutzvorschriften, DSGVO, Lokale EU-/EWR-Datenschutzgesetze, DSGVO-Bestimmungen, Personenbezogene Daten, Daten zu Professionellen Dienstleistungen, Dienstgenerierte Daten, Standardvertragsklauseln, Unterauftragsverarbeiter, Supportdaten,

Datenschutzbestimmungen

- Umfang
- Art der Verarbeitung; Eigentumsverhältnisse
- Offenlegung verarbeiteter Daten
- Verarbeitung personenbezogener Daten; DSGVO
- Datensicherheit
- Meldung von Sicherheitsvorfällen
- Datenübermittlungen und Speicherstelle
- Speicherung und Löschung von Daten
- Vertraulichkeitsverpflichtung des Auftragsverarbeiters
- Hinweise und Kontrollen beim Einsatz von Unterauftragsverarbeitern
- Bildungseinrichtungen
- CJIS-Kundenvertrag
- HIPAA-Geschäftspartner
- Bestimmungen des kalifornischen Datenschutzgesetzes (California Consumer Privacy Act, CCPA)
- Kontaktaufnahme mit Microsoft
- Anhang A – Sicherheitsmaßnahmen

Datentypen

Kundendaten
(„zur Verfügung gestellt“ durch den Kunden)

Diagnosedaten
(„erhoben“ oder „erlangt“ aus Software, die vom Kunden installiert wurde)

Dienstgenerierte Daten
(„generiert“ oder „abgeleitet“ durch Microsoft)

Professional Services Daten
(„zur Verfügung gestellt“ durch den Kunden im Zusammenhang mit „Professional Services“)

Supportdaten
(„zur Verfügung gestellt“ durch den Kunden im Zusammenhang mit technischem Support)

Personenbezogene Daten

(„Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen“)

Auszug aus dem DPA

Privacy Shield aufgehoben - sind die Standard-vertragsklauseln noch gültig?

Ja, das hat der EuGH bestätigt.

Es werden aber *case-by-case assessments* gefordert hinsichtlich der Umstände des Transfers, einschließlich vorhandener *supplementary measures* (gesetzlich, technisch oder organisatorisch).

Was macht Microsoft?

- Vertragliche Zusicherungen (Defending your data)
- Kein direkter Zugriff auf Daten durch Regierungen
- Least Priviledge Access Mechanismen für Mitarbeiter
- Zertifizierungen (ISO, SOC, C5 etc)
- Verschlüsselung („at rest“ und „in transit“)
- Prüfung aller Forderungen der Regierung nach Rechtsgültigkeit und Angemessenheit
- Transparenz bei Anfragen durch Strafverfolgungs-behörden (Law Enforcement Request Reports)

Law Enforcement National Security (LENS) Team

Das LENS Team

- arbeitet 24/7
- überprüft alle Anfragen und widerspricht ggf.
- prüft Zulässigkeit (individualisierter Beschluss)
- verweist an Unternehmenskunden
- benachrichtigt und informiert den Kunden (sofern nicht untersagt)

Microsoft wird Dritten Folgendes <u>nicht</u> bereitstellen:

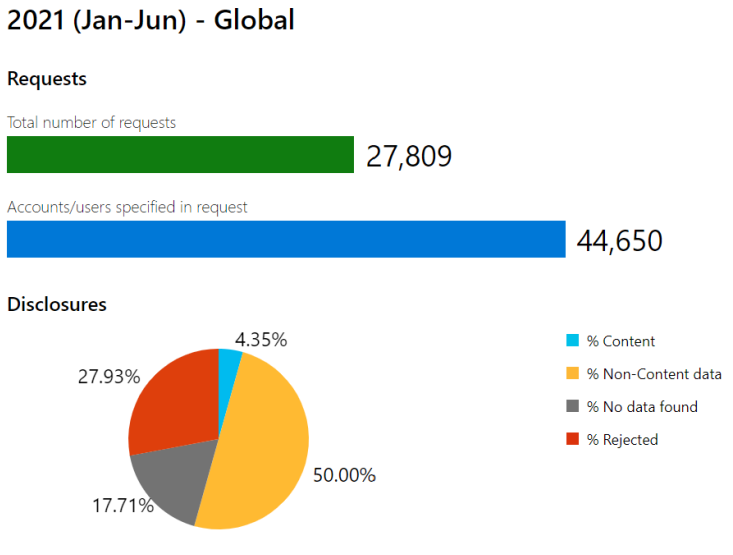
(a) einen direkten, indirekten, pauschalen oder uneingeschränkten Zugriff auf verarbeitete Daten;

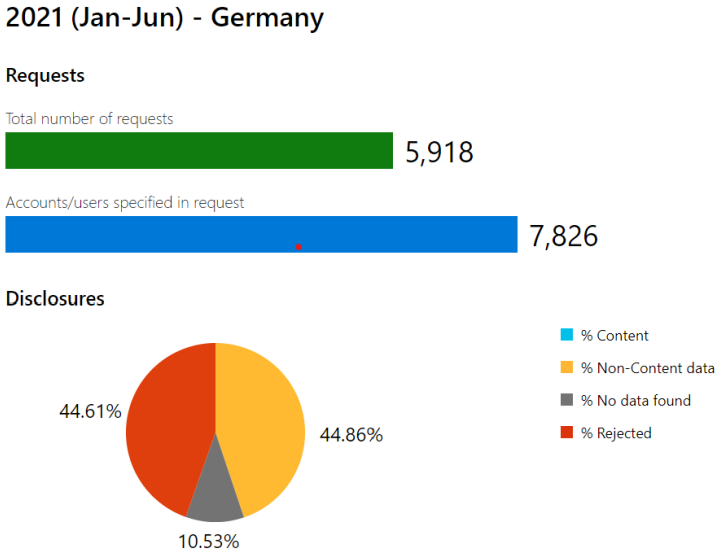
(b) für die Sicherung der verarbeiteten Daten verwendete Verschlüsselungsschlüssel für die Plattform, oder die Möglichkeit, eine solche Verschlüsselung zu umgehen; oder

(c) den Zugang zu verarbeiteten Daten, wenn Microsoft bekannt ist, dass diese Daten für andere als die in der betreffenden Anfrage Dritter angegebenen Zwecke verwendet werden sollen.

Law Enforcement Request Report

- halbjährliche Statistik
- zeigt Auskunftsersuchen aus allen Ländern für alle Kunden (Consumer und Enterprise)





Defending Your Data

Erstens verpflichten wir uns, dass wir jede Anfrage einer staatlichen Stelle – egal von welcher Regierung – nach Daten unserer Unternehmenskunden oder unserer Kunden aus dem öffentlichen Sektor anfechten werden, wenn es dafür eine rechtliche Grundlage gibt. Diese umfassende Verpflichtung geht über die vorgeschlagenen Empfehlungen des Europäischen Datenschutzausschusses hinaus.

Zweitens werden wir die Nutzer*innen unserer Kunden finanziell entschädigen, wenn wir ihre Daten aufgrund einer Anfrage einer staatlichen Stelle unter Verletzung der EU-Datenschutz-Grundverordnung (EU-DS-GVO) offenlegen müssen. Diese Verpflichtung geht ebenfalls über die Empfehlungen des Europäischen Datenschutzausschusses hinaus. Damit zeigen wir unsere Zuversicht, dass wir die Daten unserer Unternehmenskunden und unserer Kunden aus dem öffentlichen Sektor schützen können und sie keiner unangemessenen Offenlegung aussetzen werden.

Sicherheits-maßnahmen

Ereignisprotokollierung. Microsoft protokolliert den Zugriff und die Nutzung von Informationssystemen, die Kundendaten enthalten, indem die Zugangs-ID, die Uhrzeit, die erteilte oder verweigerte Berechtigung und die entsprechende Aktivität registriert werden, oder ermöglicht dem Kunden eine Protokollierung.

Zugriffsberechtigung. Wenn mehrere Personen Zugriff auf die Systeme haben, in denen Kundendaten enthalten sind, stellt Microsoft sicher, dass diese Personen über separate Kennungen/Anmeldedaten verfügen.

Geringste Rechte. Technischen Supportmitarbeitern ist der Zugriff auf Kundendaten nur gestattet, wenn dies erforderlich ist. Microsoft schränkt den Zugriff auf Kundendaten auf solche Personen ein, die diesen Zugriff benötigen, um ihre berufliche Tätigkeit auszuführen.

Netzwerkdesign. Microsoft führt Kontrollen durch, um zu verhindern, dass Personen Zugriffsrechte erhalten, die ihnen nicht zugewiesen wurden, um Zugang zu Kundendaten zu erhalten, auf die sie nicht zugreifen dürfen.

Auszug aus dem DPA

Sicherheits-maßnahmen

Sicherheitsschulungen. Microsoft informiert seine Mitarbeiter über relevante Sicherheitsverfahren und ihre jeweiligen Rollen. Microsoft informiert seine Mitarbeiter auch über mögliche Folgen einer Verletzung der Sicherheitsregeln und -verfahren. Microsoft verwendet in der Schulung nur anonyme Daten.

Verschlüsselung. Microsoft verschlüsselt Kundendaten, die über öffentliche Netzwerke übermittelt werden, oder ermöglicht dem Kunden eine solche Verschlüsselung.

Zugriffskontrolle. Microsoft überwacht wiederholte Versuche, sich mit ungültigen Kennwörtern Zugriff auf Informationssysteme zu verschaffen, oder ermöglicht dem Kunden eine solche Überwachung.

Meldungen. Für jede Sicherheitsverletzung, bei der es sich um einen Sicherheitsvorfall handelt, erfolgt (…) unverzüglich und auf jeden Fall innerhalb von 72 Stunden eine Benachrichtigung seitens Microsoft.

Disaster Recovery. Microsoft unterhält Notfall- und Alternativpläne für die Einrichtungen, in denen sich Microsoft Informationssysteme befinden, die Kundendaten verarbeiten.

Auszug aus dem DPA

Zertifizierungen

Standard	Bezeichnung
ISO 27001	Information Security Management System
ISO 27018	Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
ISO 27701	Privacy Management Systems
SOC 1, 2 und 3	System and Organization Control
C5 (BSI)	Cloud Computing Compliance Criteria Catalogue
TISAX	Trusted Information Security Assessment Exchange
KRITIS	Nachweis über angemessene IT Sicherheit
BAIT	Bankaufsichtliche Anforderungen an die IT

Wo liegen Ihre Daten?

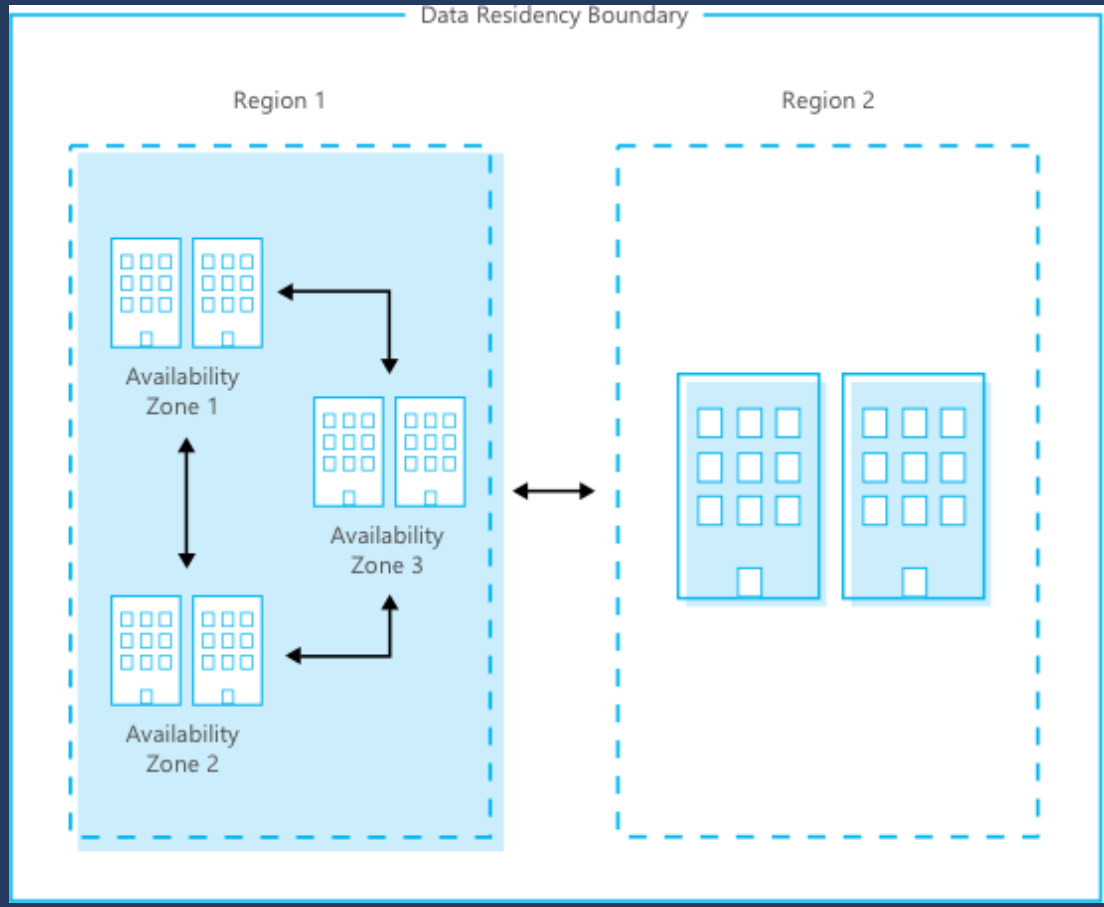
Geo, Regionen, Zonen, Rechenzentren

Eine **Geo** hat typischerweise zwei oder mehr Regionen. Geo's werden fehlertolerant ausgelegt, um den Ausfall einer kompletten Region kompensieren zu können.

Eine **Region** besteht aus einer Menge von Rechenzentren innerhalb eines Latenzradius.

Availability Zones sind physisch getrennte Standorte innerhalb einer Region und bestehen jeweils aus einem oder mehreren Rechenzentren.

Regionen und Geos sind durch einen dedizierten Microsoft Netzwerk-Backbone verbunden.



Data at Rest / in Transit

Data at Rest:

Im Fall der Kernonlinedienste speichert Microsoft Kundendaten in bestimmten größeren geografischen Gebieten („Geo“).

Data in Transit:

Unter Berücksichtigung solcher Sicherheitsmaßnahmen beauftragt der Kunde Microsoft, Kundendaten und personenbezogenen Daten in die Vereinigten Staaten von Amerika oder in jedes andere Land zu übermitteln, in dem Microsoft oder ihre Unterauftragsverarbeiter tätig sind, und Kundendaten und personenbezogenen Daten zur Bereitstellung der Onlinedienste zu speichern und zu verarbeiten, ausgenommen wie an anderer Stelle in den DPA-Bestimmungen beschrieben.

Microsoft Azure entspricht europäischem Cloud Code of Conduct

[PRESS RELEASE: Microsoft Azure adheres to the EU Cloud Code of Conduct: EU Cloud CoC (eucoc.cloud)]

EU-Datengrenze für die Cloud

Microsoft wird es in der EU ansässigen Kunden aus dem öffentlichen Sektor und Unternehmenskunden künftig ermöglichen, all ihre Daten innerhalb der EU zu verarbeiten und zu speichern. In anderen Worten: Wir werden keine Daten dieser Kunden aus der EU heraus transferieren müssen. Diese Zusage gilt für alle zentralen Cloud-Dienste von Microsoft – Azure, Microsoft 365 und Dynamics 365. Mit dieser Maßnahme gehen wir über unsere bestehenden Zusagen bei der Datenspeicherung hinaus. Wir sprechen von einer „EU Data Boundary for the Microsoft Cloud“, einer EU-Datengrenze für unsere Cloud-Lösungen.

Startschuss zur ersten souveränen Cloud-Plattform für den öffentlichen Sektor in Deutschland: SAP und Arvato Systems kündigen Partnerschaft an

3. Februar 2022 von SAP News

Kernbotschaften

Kernbotschaften	Quellen
Die DSGVO ist eine Verordnung der Europäischen Union. Microsoft hat seine Verträge bereits vor Inkrafttreten der DSGVO Mai 2018 umgestellt. Microsoft Cloud-Dienste können DSGVO-konform eingesetzt werden.	In den aktuellen Datenschutzbestimmungen von Microsoft wird 74x auf die DSGVO referenziert. v.a. DPA, Anlage 3. : „Microsoft geht die in diesen Bestimmungen zur Datenschutz-Grundverordnung der Europäischen Union („DSGVO – Bestimmungen“) enthaltenen Verpflichtungen gegenüber allen Kunden mit Wirkung vom 25. Mai 2018 ein.“
EUGH Schrems II hat nichts daran geändert, dass Enterprise Kunden Microsoft Cloud-Dienste datenschutzkonform einsetzen können.	Der EUGH hat das Privacy Shield für unwirksam erklärt, die Standard Vertragsklauseln gelten aber nach wie vor und MS hat die SCC ausgeweitet.
Microsoft beschreibt sehr eng in dem DS-Addendum (**DPA**) welche wie Daten verarbeitet werden. Microsoft hält sehr transparent, wie es mit Anfragen von Behörden umgeht und hat seit Ende 2020 zusätzlich einen **Rechtsschutz** eingebaut.	1. Law Enforcement Request Report | Microsoft CSR 2. https://blogs.microsoft.com/on-the-issues/2020/11/19/defending-your-data-edpb-gdpr/ 3. https://news.microsoft.com/de-de/datenschutz-und-datensicherheit-in-bildungseinrichtungen/
Microsoft wird auch die Data in Transit bis Ende 2022 ausschließlich innerhalb der EU verarbeiten.	„EU Data Boundary for the Microsoft Cloud“ (EU-Datengrenze für unsere Cloud-Lösungen)

Quellen

- **Cloud Compendium** *https://www.microsoft.com/de-de/download/details.aspx?id=50830*
- Im Daten-Dschungel – Datenschutz von A bis Z | News Center Microsoft
- Microsoft Webinar: Zertifizierungen von Microsoft
- Microsoft Webinar: Informationen zu den Online Service Terms (OSTs) und zum Data Privacy Addendum (DPA)
- Microsoft Webinar: Diagnosedaten in Microsoft 365 und Windows 10
- Datenschutz bei Microsoft: https://privacy.microsoft.com/de-DE/
- Service Trust Portal: https://servicetrust.microsoft.com/
- Online Services Terms (OST): https://aka.ms/OST
- Data Protection Addendum (DPA) https://aka.ms/DPA
- Statement des bayrischen Justizministeriums zum datenschutzkonformen Einsatz von Teams (ab Minute 48)