Microsoft

Microsoft Cloud Compendium

FAQ zu Datenschutz, verantwortungsvoller KI-Nutzung und weiteren Compliance-Anforderungen

Veröffentlicht von Microsoft Germany & Austria Legal Affairs

Stand: August 2025

Inhalt

1. Datenschutz 4

1.1. Auftragsverarbeitung durch Microsoft 4
1.2. Speicherort und Drittlandtransfers 9
1.3. Technische und organisatorische Maßnahmen 13
1.4. Findet ein Austausch zwischen Microsoft und den deutschen Datenschutzaufsichtsbehörden statt? 14
1.5. Verarbeitet Microsoft Kundendaten zu eigenen Zwecken? 14
1.6. Notwendige Informationen für die Datenschutzdokumentation 15

2. Künstliche Intelligenz und EU AI Act 17

2.1. Wie entwickelt und nutzt Microsoft KI verantwortungsvoll? 17
2.2. EU AI Act 17
2.3. Wie wahrt Microsoft den Datenschutz bei der KI-Nutzung? 19
2.4. Vertragliche Regelungen der Generativen KI-Dienste von Microsoft 19
2.5. KI-Governance und Einbindung von Betriebsräten 21

3. Digitale Resilienz 22

3.1. Wie trägt Microsoft zu Europas digitaler Resilienz bei? 22
3.2. Welche Angebote bietet Microsoft hinsichtlich digitaler Souveränität? 22

4. Sonstige Compliance-Anforderungen 24

4.1. Können auch Berufsgeheimnisträger die Microsoft-Onlinedienste nutzen? 24
4.2. Wie kann der Kunde seine Daten revisionssicher zur Einhaltung von gesetzlichen Aufbewahrungspflichten aufbewahren? 24
4.3. Was gilt für andere, hier nicht aufgeführte Gesetze? 25

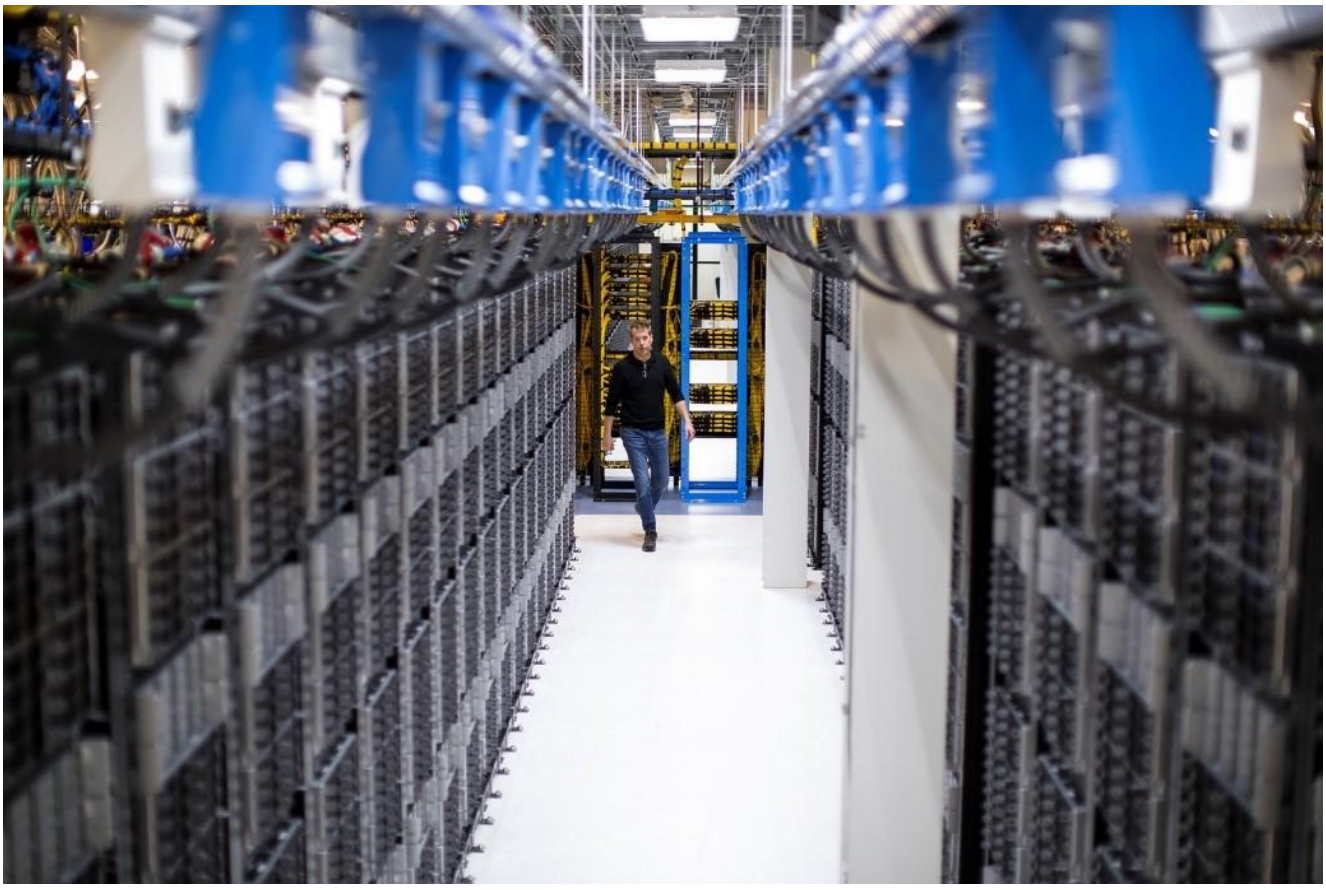
Einleitung

Mit diesem Cloud Compendium möchte Microsoft Antworten auf häufig gestellte Fragen zu den Microsoft Onlinediensten wie Microsoft 365 oder Azure von Unternehmen, der öffentliche Hand und des Bildungsbereichs geben und diese in den gesetzlichen und regulatorischen Rahmen einordnen.

Microsofts Produkte lassen sich selbstverständlich DSGVO-konform einsetzen und betreiben. 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 bietet Microsoft Technologielösungen an, die europäischen Gesetzen und Erwartungen (in Bezug auf Sicherheit und Datenlokalisierung) entsprechen. Moderne Technologien wie Cloud-Computing und Künstliche Intelligenz sind ein Schlüssel dazu, Klima und Umwelt zu schützen, Ressourcen effizienter zu nutzen und eine nachhaltige Zukunft für alle zu sichern.

Zudem ist es Microsofts Ziel, KI zu entwickeln und einzusetzen, die einen positiven Einfluss auf die Gesellschaft hat und deren Vertrauen genießt. Verantwortungsvolle KI-Nutzung ist für Microsoft von größter Bedeutung.



1. Datenschutz

1.1. Auftragsverarbeitung durch Microsoft

Wo finde ich den AVV/DPA und die sonstigen datenschutzrelevanten Vertragsinhalte von Microsoft?

Einbeziehung des DPA: Grundlage für die Leistungsbeziehung sind die Kundenverträge, wie Volumenlizenzverträge, über die Nutzung der jeweiligen Onlinedienste, die in Europa zwischen dem Kunden und der Microsoft Ireland Operations Limited abgeschlossen werden. In den Kundenverträgen wird auf die Produktbestimmungen verwiesen, die wiederum auf den online abrufbaren Datenschutznachtrag für die Produkte und Services von Microsoft (Data Protection Addendum, „DPA") verweisen. Auch bei Beziehung von Lizenzen über einen Partner wird der DPA direkt mit Microsoft Ireland Operations Limited abgeschlossen.

Inhalt des DPA: Der DPA gilt mit wenigen Ausnahmen grundsätzlich für alle Onlinedienste (wie Microsoft 365 oder Azure), Software und Professional Services von Microsoft. Der DPA beinhaltet im Abschnitt „Datenschutzbestimmungen" unter anderem Regelungen zur Verarbeitung von Kundendaten, die Pflichten von Microsoft sowie Details über getroffene Sicherheitsmaßnahmen. Auch wiederholt er in Anlage 1 „DSGVO-Bestimmungen" alle Pflichtinhalte nach Artikel 28 DSGVO.

Ergänzung durch Produktbestimmungen: Ergänzt wird der DPA durch die Produktbestimmungen, in die produktspezifische Bedingungen ausgelagert sind. Diese ergänzen oder ändern den DPA spezifisch für einzelne Produkte. So sind z. B. die konkreten Speicherorte („Geos") für bestimmte Onlinedienste im Abschnitt Datenschutz- und Sicherheitsbestimmungen der Produktbestimmungen festgelegt. Sämtliche produktspezifische Ausnahmen vom DPA finden sich ebenfalls im Abschnitt Datenschutz- und Sicherheitsbestimmungen, Unterabschnitt „Ausnahmen vom DPA".

Nachrangige Geltung des sonstigen Kundenvertrages: Der sonstige Kundenvertrag (z. B. Microsoft Business and Services Agreement / Microsoft-Kundenvertrag) ist in Datenschutzfragen nachrangig gegenüber dem vorrangigen DPA (siehe den Abschnitt „Einleitung" des DPA).

Die Infografik fasst das Verhältnis des DPA zu den anderen Bestandteilen des Kundenvertrags zusammen.

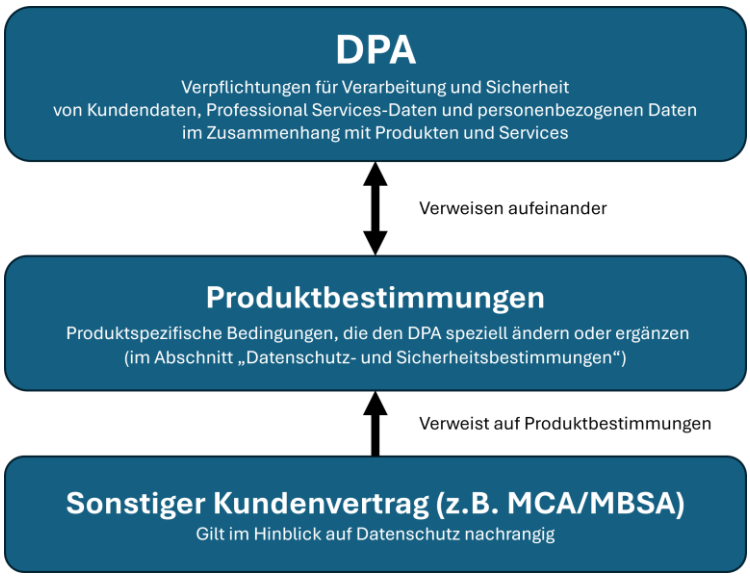


Abbildung 1: Vertragsverhältnisse

Welche Produkte und Services umfasst der DPA?

Der DPA gilt für alle Onlinedienste, Software (zusammen „Produkte") und Professional Services von Microsoft, soweit die Produktbestimmungen bei Produkten oder der Arbeitsauftrag bei Professional Services keine Ausnahmen regeln.

Diese drei erfassten Kategorien bestehen aus folgenden Produkten und Services:

1. **„Onlinedienste"**

   Definition:

   Abschnitt Glossar der Produktbestimmungen (einbezogen durch Verweis am Anfang des Abschnitts „Definitionen" des DPA):

   „Onlinedienste sind die von Microsoft gehosteten Dienste, die der Kunde gemäß der Microsoft-Volumenlizenzvereinbarung abonniert, einschließlich der Dienste, die im Abschnitt „Onlinedienste" der Produktbestimmungen aufgeführt sind. Sie enthalten weder Software noch gemäß separaten Lizenzbestimmungen bereitgestellte Dienste […]."

   Beispiele:

   - Microsoft 365
   - Microsoft Azure

   Weitere Onlinedienste sind im Abschnitt „Onlinedienste" der Produktbestimmungen aufgeführt

   Ausnahmen:

   Produktspezifische Ausnahmen vom DPA für Onlinedienste finden sich im Abschnitt Datenschutz- und Sicherheitsbestimmungen, Unterabschnitt „Ausnahmen vom DPA".

   Daneben gilt der DPA auch nicht für Daten, die in Kunden-Betriebsumgebungen verbleiben und nicht an Microsoft gesendet werden (siehe Abschnitt „Umfang" des DPA)

2. **„Software"**

   Definition:

   „Microsoft-Kundenvertrag", wenn der Kunde Produkte unter dem Microsoft-Kundenvertrag bezieht. Falls der Kunde unter einem anderen Volumenlizenzvertrag Onlinedienste bezieht, gilt jedenfalls die Definition aus den Produktbestimmungen, Abschnitt „Glossar". (einbezogen durch Verweis am Anfang des Abschnitts „Definitionen" des DPA):

   „‚Software' bezeichnet lizenzierte Kopien von Microsoft-Software, die in den Produktbestimmungen aufgeführt sind. Software umfasst keine Onlinedienste, die Software kann jedoch Teil eines Onlinedienstes sein."

   Beispiele:

   - Windows-Desktop-Betriebssystem
   - Windows Server

   Weitere Software ist im Abschnitt „Software" der Produktbestimmungen aufgeführt

   Ausnahmen:

   Produktspezifische Ausnahmen vom DPA für Software finden sich ebenfalls im Abschnitt Datenschutz- und Sicherheitsbestimmungen, Unterabschnitt „Ausnahmen vom DPA" und „Vom DPA ausgeschlossene Softwareprodukte".

   Daneben gilt der DPA auch nicht für Daten, die in Kunden-Betriebsumgebungen verbleiben und nicht an Microsoft gesendet werden (siehe Abschnitt „Umfang" des DPA).

3. **„Professional Services"**

   Definition:

   Abschnitt „Definitionen" des DPA:

   „‚Professional Services' bezeichnet die folgenden Dienstleistungen: (a) Beratungsdienste von Microsoft, bestehend aus der Planung, Beratung, Anleitung, Datenmigration, Bereitstellung und aus Lösungs-/Softwareentwicklungsdiensten, die im Rahmen eines Microsoft Enterprise Services-Arbeitsauftrags, sofern in der Projektbeschreibung vereinbart, oder eines Cloud Workload Acceleration-Vertrags bereitgestellt werden, in den dieser DPA durch Verweis aufgenommen wird; und (b) technische Support-Services, die von Microsoft bereitgestellt werden und dem Kunden helfen, die Produkte betreffende Probleme zu identifizieren und zu beheben, einschließlich technischen Supports, der als Teil der Microsoft Unified Support oder Premier Support Services bereitgestellt wird, sowie alle anderen kommerziellen technischen Support-Services. Die Professional Services

umfassen weder die Produkte noch, ausschließlich für die Zwecke des DPA, zusätzliche Professional Services."

Beispiele:

- Unified Support
- Industry Solutions Delivery

Ausnahmen:

Ausnahmen vom DPA gelten, soweit DPA-Bestimmungen im Arbeitsauftrag ausdrücklich als ausgeschlossen gekennzeichnet sind. Wenn der Arbeitsauftrag auf den Microsoft Professional Services-Datenschutznachtrag verweist, gilt dieser statt des regulären DPA.

Welche Version des DPA gilt für mich?

Kunden können sich stets auf die jeweilige DPA-Version berufen, die bei Abschluss oder Verlängerung eines Abonnements für Onlinedienste gilt. Diese wird für die Dauer des Abonnements „eingefroren" (siehe den Abschnitt „Beschränkung für Aktualisierungen" des DPA).

Zusätzlich sagt Microsoft im jeweils aktuellen DPA zu, die Verpflichtungen der aktuellen Version des DPA gegenüber allen Kunden mit einem bestehenden Kundenvertrag einzuhalten (siehe den Abschnitt „Einleitung" des DPA).

Kunden können also wählen, auf welche der beiden DPA-Versionen sie sich berufen können. Auch ein selektives Berufen auf einzelne neue Verpflichtungen aus der aktuellen DPA-Version ist möglich. In der Praxis ist es meistens einfacher, die aktuelle DPA-Version zu prüfen, weil diese an Microsofts aktuelle Produkte und Services angepasst ist und alle neuen regulativen Entwicklungen abdeckt (z. B. aktuelle Standardvertragsklauseln).

Wie können Kunden verbundene Unternehmen oder eigene Auftraggeber in die Auftragsverarbeitung einbinden?

Der DPA ist so ausgestaltet, dass Microsoft Ireland Operations Limited als Vertragspartner deutscher Unternehmenskunden grundsätzlich Auftragsverarbeiter i.S.d. Art. 28 DSGVO ist. Microsoft agiert allerdings automatisch als Unterauftragsverarbeiter, wenn der Kunde selbst Auftragsverarbeiter ist (siehe Abschnitt „Auftragsverarbeiter und Verantwortlicher – Rollen und Verantwortlichkeiten" des DPA).

Welche Daten umfasst der DPA?

Der DPA umfasst Kundendaten, personenbezogene Daten und Professional Services Daten. Nahezu alle Rechte und Verpflichtungen des DPA umfassen alle drei Datenkategorien.

Punktuelle Differenzierungen zwischen den Datenkategorien: Soweit zwischen den drei Datenkategorien differenziert wird, beruht dies auf technischen Unterschieden. Zum Beispiel enthält der DPA die Verpflichtung von Microsoft, keinem Microsoft-Mitarbeiter ständigen Zugriff auf „Kundendaten" zu gewähren. Für „Professional Services Daten" trifft diese Pflicht technisch gesehen nicht zu, weil z. B. die jeweils zuständigen Supportmitarbeiter ständigen Zugriff auf den Inhalt ihrer Supporttickets haben. Auch bei „personenbezogenen Daten" passt diese Pflicht nicht, weil z. B. das Microsoft-Sicherheitsteam auf Logdaten anlassbezogen nach dem Need-to-know-Prinzip zugreifen kann. Daher gilt z. B. diese Pflicht nur für „Kundendaten" (siehe Abschnitt „Datenzugriff" des DPA).

Kundendaten umfassen auch nicht-personenbezogene Daten: Die Sicherheitsstandards und die Datenverarbeitung sind bei Kundendaten gleich, egal ob die Kundendaten personenbezogene oder nicht-personenbezogene Daten enthalten. Microsoft hat keine Kenntnis, ob die Kundendaten personenbezogen sind oder nicht (Kundendaten als „Black Box"). Damit sind von den Sicherheits-standards des DPA auch z. B. etwaige nicht-personenbezogene Geschäftsgeheimnisse des Kunden erfasst.

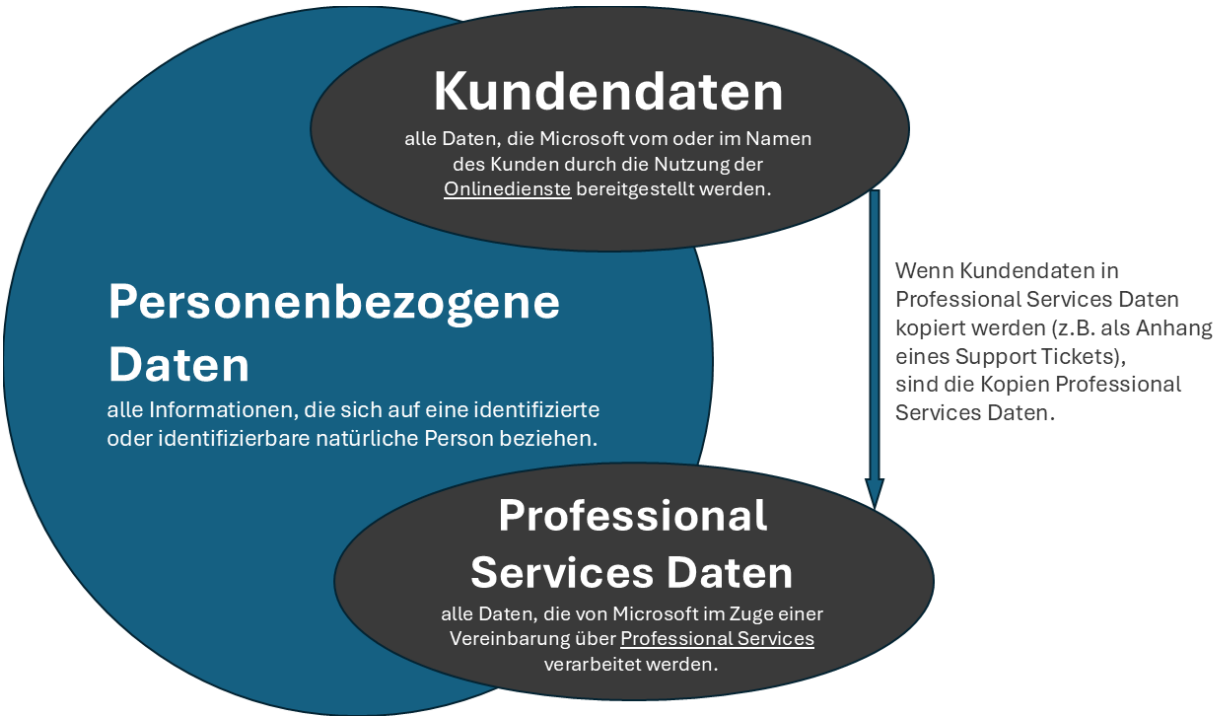


Abbildung 2: Bezeichnung von Daten

Wo finde ich die Pflichtinhalte nach Artikel 28 DSGVO?

Die Pflichtinhalte des DPA bestehen aus dem weltweit gültigen Hauptteil und der DSGVO-spezifischen Anlage 1 „Bestimmungen zur Datenschutz-Grundverordnung der Europäischen Union". Anlage 1 wiederholt größtenteils den Gesetzestext des Artikels 28 Abs. 3 DSGVO und gilt ergänzend.

Thema	Informationen
Verarbeitungsdetails (Artikel 28 Abs. 3 S. 1 DSGVO)	Fundstellen im DPA: • Abschnitt „Verarbeitungsdetails", der auf den Abschnitt „Art der Datenverarbeitung; Eigentumsverhältnisse" verweist. • Anhang B – Betroffene Personen und Kategorien personenbezogener Daten
Verarbeitung nur entsprechend der Weisungen des Kunden, soweit keine gesetzliche Pflicht besteht (Artikel 28 Abs. 3 lit. a), 29 DSGVO)	Fundstellen im DPA: • Abschnitt „Art der Datenverarbeitung; Eigentumsverhältnisse" • Abschnitt „Auftragsverarbeiter und Verantwortlicher – Rollen und Verantwortlichkeiten" • Hinsichtlich Drittlandtransfers und Offenlegungspflichten: Abschnitt „Offenlegung verarbeiteter Daten" und Anhang C „Nachtrag zu zusätzlichen Schutzmaßnahmen" • Anlage 1 – DSGVO-Bestimmungen
Drittstaatenübermittlung (Artikel 28 Abs. 3 lit. a), 44–51 DSGVO)	Fundstellen im DPA: • Abschnitt „Datenübermittlungen" und „Speicherorte von Kundendaten" • Anlage 1 – DSGVO-Bestimmungen

Thema	Informationen
Vertraulichkeitsverpflichtung (Artikel 28 Abs. 3 lit. b) DSGVO)	Fundstellen im DPA: • Abschnitt „Vertraulichkeitsverpflichtung des Auftragsverarbeiters“ • Anhang A – Sicherheitsmaßnahmen: Organisation der IT-Sicherheit • Anlage 1 – DSGVO-Bestimmungen
Umgesetzte TOMs (Artikel 28 Abs. 3 lit. c), 32 DSGVO)	Fundstellen im DPA: • Abschnitte „Sicherheitsverfahren und Sicherheitsrichtlinien“, „Datenverschlüsselung“ und „Datenzugriff“ • Anhang A – Sicherheitsmaßnahmen • Anlage 1 – DSGVO-Bestimmungen
Unterauftragsverarbeiter (Artikel 28 Abs. 3 lit. d) DSGVO)	Fundstellen im DPA: • Abschnitt „Hinweise und Kontrollen beim Einsatz von Unterauftragsverarbeitern“ • Anlage 1 – DSGVO-Bestimmungen
Unterstützung bei Betroffenenanfragen (Artikel 28 Abs. 3 lit. e), 12–21 DSGVO)	Fundstellen im DPA: • Abschnitt „Rechte der betroffenen Personen; Unterstützung bei Anfragen“ • Bei Auskunfts- und Löschanträgen: Abschnitt „Speicherung und Löschung von Daten“ • Anlage 1 – DSGVO-Bestimmungen
Benachrichtigung bei Sicherheitsvorfällen (Artikel 28 Abs. 3 lit. f), 33, 34 DSGVO)	Fundstellen im DPA: • Abschnitt „Meldung von Sicherheitsvorfällen“ • Anhang A – „Sicherheitsmaßnahmen“: „Handhabung eines Informationssicherheitsvorfalls“ • Anlage 1 – DSGVO-Bestimmungen
Unterstützung bei Datenschutzfolgenabschätzungen (Artikel 28 Abs. 3 lit. f), 45, 46 DSGVO)	Fundstellen im DPA: • Anlage 1 – DSGVO-Bestimmungen
Löschung bei Abschluss der Auftragsverarbeitung (Artikel 28 Abs. 3 lit. g) DSGVO)	Fundstellen im DPA: • Abschnitt „Speicherung und Löschung von Daten“ • Anhang A – Sicherheitsmaßnahmen: Physische und umgebungsbezogene Sicherheit • Anlage 1 – DSGVO-Bestimmungen
Nachweis der Einhaltung (Artikel 28 Abs. 3 lit. h) DSGVO)	Fundstellen im DPA: • Abschnitt „Sicherheitsverfahren und Sicherheitsrichtlinien“ • Abschnitt „Prüfung der Einhaltung“ • Anlage 1 – DSGVO-Bestimmungen

1.2. Speicherort und Drittlandtransfers

Wo werden Daten in der Microsoft Cloud gespeichert?

Microsoft bietet ein umfassendes Angebot von Cloud-Lösungen aus regionalen Cloud-Rechenzentrumsregionen an. Das geographische Gebiet (sogenannte „Geo"), welches der Administrator bei der erstmaligen Einrichtung der Dienste wählt, bestimmt den Speicherort der ruhenden Kundendaten („data at rest"). Weitere Informationen zum Speicherort und der Konfiguration finden Sie unter: Wo wir Ihre Daten speichern

Für EU-Datengrenzen-Dienste (z. B. Microsoft 365) speichert und verarbeitet Microsoft Kundendaten und personenbezogene Daten in der EU-Datengrenze. Zudem speichert Microsoft ruhende Professional Services Daten innerhalb dieser. Die EU-Datengrenze besteht aus den Microsoft-Rechenzentren, die sich ausschließlich in der Europäischen Union (EU) und der Europäischen Freihandelsassoziation (EFTA) befinden. Verbleibende Drittlandtransfers sind so weitgehend minimiert und werden in Microsofts Dokumentation transparent beschrieben. Vertraglich ist die EU-Datengrenze in den Produktbestimmungen verankert.

Die EU-Datengrenze gilt automatisch für EU-Datengrenzendienste, wenn der Kunde eine Geo innerhalb der EU konfiguriert hat und bei Microsoft 365 keine sog. Multi-Geo-Funktionalität nutzt. Dies ist näher in Microsofts Dokumentation beschrieben.

Die EU-Datengrenze geht über die datenschutzrechtlichen Anforderungen deutlich hinaus und vereinfacht somit die Risikobewertungen, die EU-Kunden durchführen müssen. Die EU-Datengrenze ermöglicht den Kunden eine größere Kontrolle über ihre Daten, einschließlich der Möglichkeit, personenbezogene Daten innerhalb der EU und EFTA zu speichern und zu verarbeiten. Damit schränkt Microsoft die Drittlandtransfers außerhalb der EU maßgeblich ein.

Weitere Informationen zur EU-Datengrenze finden Sie hier:

- Microsoft schließt richtungsweisende EU-Datengrenze ab und bietet mehr Datenresidenz und Transparenz – News Center
- Empowering Europe: Microsoft's EU Data Boundary Roadmap and Compliance Milestones
- Empowering Europe: Microsoft's EU Data Boundary Initiative FAQs

Wie sind verbleibende Drittlandtransfers abgesichert?

Microsoft übertragt Kundendaten nur nach dokumentierten Weisungen des Kunden in Drittländer (siehe Abschnitt „Datenübermittlungen" des DPA).

Microsofts primärer Transfermechanismus sind dabei die Standardvertragsklauseln nach Art. 46 Abs. 2 lit. c DSGVO. Microsofts Zertifizierung nach dem EU-US Data Privacy Framework bietet eine zusätzliche Absicherung:

- **Standardvertragsklauseln:** Microsoft Ireland Operations Limited (als der Vertragspartner europäischer Unternehmenskunden beim DPA) hat mit Microsoft Corp. die Standardvertragsklauseln von 2021 (Module 3) abgeschlossen. Microsoft Corp. hat jeweils mit allen weiteren Unterauftragsverarbeitern Standardvertragsklauseln vereinbart. Die Standardvertragsklauseln von 2021 zwischen Microsoft Corp. und Microsoft Ireland Operations Limited können Sie im Service Trust Portal einsehen.
- **EU-US Data Privacy Framework:** Microsoft Corp. ist nach dem Data Privacy Framework zertifiziert und hat mit allen weiteren Unterauftragsverarbeitern entsprechende Verträge nach Ziffer 3 der Data Privacy Framework Principles abgeschlossen.

Die Transfermechanismen sind in Abbildung 3: Transfermechanismen verdeutlicht.

Alle wesentlichen Informationen zu Microsofts Drittlandtransfers finden Sie im Whitepaper Compliance with EU transfer requirements for personal data in the Microsoft Cloud

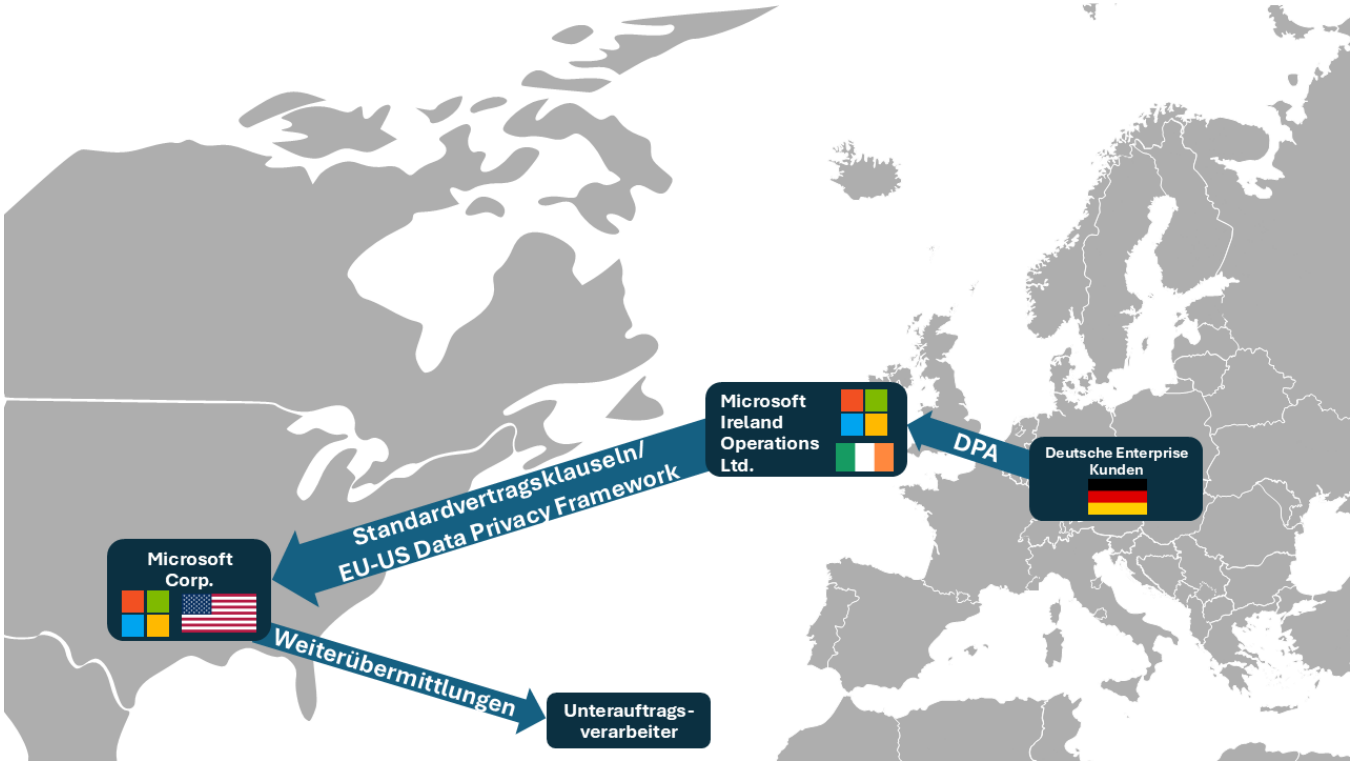


Abbildung 3: Transfermechanismen

Wie schützt Microsoft Kundendaten gegen Behördenanfragen?

Microsoft setzt sich für die Rechte seiner Kunden ein. Falls eine Regierung Kundendaten von Microsoft verlangt, muss sie den geltenden rechtlichen Verfahren folgen. Microsoft wird Forderungen nur dann nachkommen, wenn Microsoft eindeutig dazu gezwungen ist. Der erste Schritt besteht immer in dem Versuch, solche Anfragen an den jeweiligen Kunden weiterzuleiten oder sie darüber zu informieren. Wenn Microsoft überzeugt ist, dass Anfragen nicht legal sind, lehnt Microsoft sie ab oder fechtet sie an (siehe Blogpost zu Defending Your Data)

Im DPA sind folgende Verpflichtungen für Behördenanfragen geregelt (Abschnitt „Offenlegung verarbeiteter Daten"):

- **Einbindung des Kunden:** „Microsoft wird verarbeitete Daten gegenüber Strafverfolgungsbehörden nur offenlegen bzw. den Zugriff darauf ermöglichen, wenn dies gesetzlich vorgeschrieben ist. Wenn sich eine Strafverfolgungsbehörde mit Microsoft in Verbindung setzt und verarbeitete Daten anfordert, wird Microsoft versuchen, die Strafverfolgungsbehörde an den Kunden zu verweisen. Wenn Microsoft gezwungen wird, verarbeitete Daten an die Strafverfolgungsbehörden weiterzugeben, benachrichtigt Microsoft den Kunden unverzüglich und übermittelt eine Kopie der Anforderung, sofern dies nicht gesetzlich verboten ist."
- **Offenlegung nur zur Wahrung rechtsstaatlicher Mindeststandards:** „Microsoft wird verarbeitete Daten nur wie gesetzlich vorgeschrieben offenlegen oder zugänglich machen, vorausgesetzt, dass die Rechtsvorschriften und Gepflogenheiten den Wesensgehalt der Grundrechte und -freiheiten achten und nicht über Maßnahmen hinausgehen, die in einer demokratischen Gesellschaft erforderlich und verhältnismäßig sind, um gegebenenfalls eines der in Artikel 23 Absatz 1 der DSGVO aufgeführten Ziele sicherzustellen."
- **Kein uneingeschränkter Zugriff auf Kundendaten:** „Microsoft wird Dritten Folgendes nicht bereitstellen: (a) einen direkten, indirekten, pauschalen oder uneingeschränkten Zugriff auf verarbeitete Daten und (b) für die Sicherung der verarbeiteten Daten verwendete Verschlüsselungsschlüssel für die Plattform, oder die Möglichkeit, eine solche Verschlüsselung zu umgehen."

Zudem hat Microsoft im Nachgang des „Schrems II"-Urteil des Europäischen Gerichtshofs u. a. folgende zusätzlichen Schutzmaßnahmen in den DPA aufgenommen (siehe Anhang C des DPA):

- Erstens verpflichtet sich Microsoft, jede Anfrage einer staatlichen Stelle nach Daten von Unternehmenskunden oder Kunden aus dem öffentlichen Sektor anzufechten, wenn es dafür eine rechtliche Grundlage gibt.
- Zweitens wird Microsoft die betroffenen Personen der Kunden finanziell entschädigen, wenn Microsoft ihre Daten aufgrund einer Anfrage einer staatlichen Stelle unter Verletzung der DSGVO offenlegen muss.

Damit verpflichtet sich Microsoft, Daten von Unternehmenskunden und Kunden aus dem öffentlichen Sektor zu schützen und sie keiner unangemessenen Offenlegung auszusetzen.

Schließlich hat Microsoft auch zahlreiche technische zusätzliche Schutzmaßnahmen umgesetzt. Microsoft verschlüsselt Kundendaten bei dauerhafter Speicherung („at rest") und Übermittlung („in transit"). Azure kann Kundendaten für bestimmte Azure-Dienste verschlüsseln, während sie verarbeitet werden („in use"). Azure Confidential Computing ermöglicht die Verschlüsselung innerhalb hardwarebasierter vertrauenswürdiger Ausführungsumgebungen, so dass die Kundendaten bei ihrer Verwendung verschlüsselt bleiben.

Wesentliche Information für die Durchführung Ihrer eigenen Transfer Impact Assessments finden Sie in dem Whitepaper Compliance with EU transfer requirements for personal data in the Microsoft Cloud.

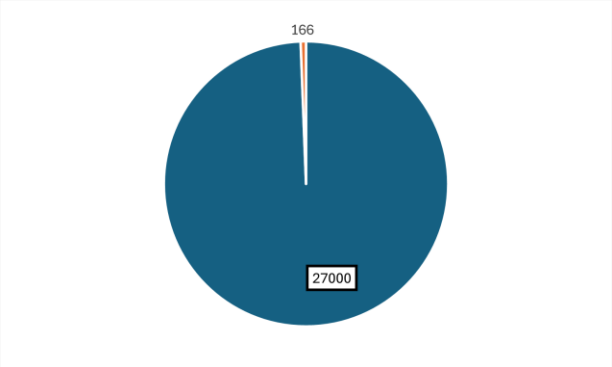
Informationen zu den fünf neuen digitalen Zusicherungen für Europa finden Sie hier: [Microsofts neue digitale Zusicherungen für Europa | News Center Microsoft]

Wie viele Anfragen von Ermittlungsbehörden erhält Microsoft?

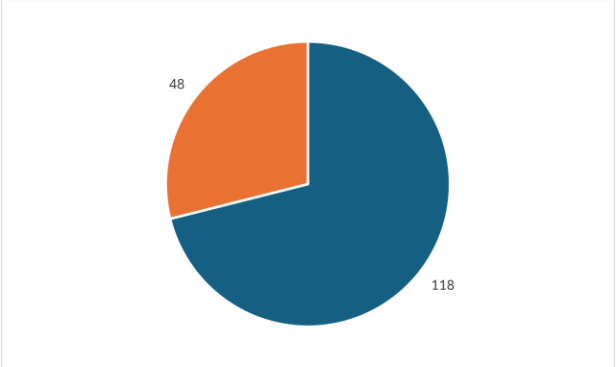
Microsoft erhält nur sehr wenige Behördenanfragen für Kundendaten seiner B2B-Unternehmenskunden. Die große Mehrheit der Behördenanfragen bezieht sich auf die B2C-Verbraucherdienste (aus Microsofts aktuell letztem Transparenzbericht):

Zum Beispiel hat Microsoft in der ersten Jahreshälfte 2024 (der aktuell letzten Berichtsperiode des Transparenzberichts) ca. 27.000 Anfragen erhalten. Davon waren:

- weltweit 166 Behördenanfragen nach Kundendaten von Unternehmenskunden erhalten.



- In 118 Fällen (d. h. 71 %) hat Microsoft diese Behördenanfragen erfolgreich abgewehrt, an den Kunden verwiesen oder es waren keine Kundendaten vorhanden.
- In 48 Fällen (29 %) musste Microsoft Kundendaten oder sonstige personenbezogene Daten herausgeben.
- In 0 Fällen betraf dies grenzüberschreitende Behördenanfragen hinsichtlich EU-Enterprise-Kunden.



Weitere Informationen finden Sie in im Transparenzbericht zu Behördenanfragen und dem Whitepaper Compliance with EU transfer requirements for personal data in the Microsoft Cloud.

1.3. Technische und organisatorische Maßnahmen

Welche technischen und organisatorischen Maßnahmen hat Microsoft umgesetzt?

- **ISO/IEC 27001, 27002 und 27018:** Für alle Produkte und Services, für die der DPA gilt, verpflichtet sich Microsoft zur Einhaltung von technischen und organisatorischen Maßnahmen („TOMs") für Kundendaten, Professional Services Daten und personenbezogene Daten und zur Sicherstellung, dass die Maßnahmen den Anforderungen von ISO/IEC 27001, ISO/IEC 27002 und ISO/IEC 27018 entsprechen.
- **SOC 1/SOC 2:** Für die in den Produktbestimmungen genannten Onlinedienste (insb. Microsoft 365; siehe den Abschnitt Datenschutz- und Sicherheitsbestimmungen der Produktbestimmungen) hat Microsoft die Anforderungen von SOC 1 Typ II und SOC 2 Typ II umgesetzt.
- **TOMs-Liste für alle Produkte und Services:** Für alle Produkte und Services, für die der DPA gilt hat Microsoft die in Annex II der Standardvertragsklauseln von 2021 vorgesehenen TOMs zum Schutz personenbezogener Daten umgesetzt (siehe Abschnitt „Datensicherheit" des DPA).
- **TOMs-Liste für Core-Onlinedienste und Professional Services:** Ergänzend findet sich für Core-Onlinedienste (insb. Microsoft 365, Azure Core Services und Dynamics 365) und Professional Services in Anhang A des DPA eine zusätzliche Liste umfassender TOMs. Core-Onlinedienste sind alle Onlinedienste, die in der entsprechenden Tabelle der Produktbestimmungen aufgeführt sind (siehe den Abschnitt Datenschutz- und Sicherheitsbestimmungen der Produktbestimmungen).

Wie können Kunden sich von der Einhaltung aller vereinbarten TOMs zu überzeugen?

Kunden sind bei einer Auftragsverarbeitung datenschutzrechtlich verpflichtet, sich von der Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten beim Auftragsverarbeiter zu überzeugen (Artikel 28 Abs. 1 DSGVO). Sie können dieser Pflicht nachkommen, indem sie sich vom Dienstleister relevante Zertifizierungen durch unabhängige Dritte nachweisen lassen. Deshalb unterzieht sich Microsoft jedes Jahr Überprüfungen von international anerkannten unabhängigen Auditoren. Diese überprüfen, ob Microsoft die Richtlinien und Verfahren für Sicherheit, Datenschutz, Kontinuität und Konformität gewährleistet. Grundlage ist der ISO/IEC 27001-Standard. Microsoft stellt seinen Kunden im Service Trust Portal einen Auditbericht nach ISO/IEC 27001 zur Verfügung. Zudem stellt Microsoft u. a. auch Auditberichte nach SOC 1 Typ II und SOC 2 Typ II zur Verfügung, der auch den Kriterienkatalog C5:2020 des BSI abdeckt.

Weltweit ist Microsoft der Cloudanbieter mit der größten Anzahl solcher Zertifizierungen. Mehr als 100 nationale und internationale Standards sind damit abgedeckt. Eine große Anzahl sektorspezifischer Industriestandards kommen noch mit hinzu, zu denen in Deutschland beispielsweise TISAX gehört, oder aber nationale Standards wie der vom Bundesamt für Sicherheit in der Informationstechnik (BSI) festgelegte Kriterienkatalog C5 (Cloud Computing Compliance Criteria Catalogue). Dahinter verbirgt sich ein Regelwerk, das den Mindeststandard für eine sichere Cloud-Computing-Umgebung definiert und das Microsoft für alle Rechenzentrumsregionen weltweit anwendet.

Weitere Informationen zu umgesetzten TOMs finden Sie hier:

- Service Trust Portal: Auditberichte und zahlreiche weitere Dokumente zur IT-Sicherheit und zur Einhaltung der DSGVO (nur für Kunden zugänglich)
- Microsoft Trust Center: umfassende Informationen zur Compliance bei der Nutzung von Microsoft Onlinediensten.
- Microsoft Security Whitepaper: Sichere Datenhaltung im Cloud-Zeitalter
- Im Daten-Dschungel: Zertifizierung der Microsoft Cloud

1.4. Findet ein Austausch zwischen Microsoft und den deutschen Datenschutzaufsichtsbehörden statt?

Ja. Microsoft hat schon lange vor Inkrafttreten der DSGVO das Gespräch mit den europäischen Datenschutzaufsichtsbehörden gesucht. Es findet weiterhin ein kontinuierlicher Austausch statt.

Microsoft ist an einem konstruktiven und lösungsorientierten Austausch mit Datenschutzbehörden jederzeit interessiert, um seine Verantwortung als globaler Technologieanbieter, der seit mehr als 40 Jahren in Europa tätig ist, nachzukommen.

Zu dem Bericht der Datenschutzkonferenz zu Microsoft 365 hat Microsoft neben langjährigen, umfangreichen Gesprächen direkt mit der Datenschutzkonferenz auch eine umfassende Stellungnahme veröffentlicht.

1.5. Verarbeitet Microsoft Kundendaten zu eigenen Zwecken?

Nein, Microsoft verarbeitet **keine** Kundendaten für eigene Zwecke.

Microsoft verarbeitet Kundendaten **nur** zur Bereitstellung der Produkte/Professional Services und der dadurch veranlassten, mit der Leistungserbringung eng zusammenhängenden Geschäftstätigkeiten (siehe Abschnitt „Art der Datenverarbeitung; Eigentumsverhältnisse“ des DPA):

- Sofern Daten für Geschäftstätigkeiten verarbeitet werden, sind dies allein aggregierte, nicht-personenbezogene Daten für die im DPA eingegrenzten zulässige Zwecke: (i) Abrechnungs- und Kontoverwaltung, (ii) Vergütung wie etwa Berechnung von Mitarbeiterprovisionen und Partner-Incentives, (iii) interne Berichterstattung und Geschäftsmodellierung und (iv) Finanzberichterstattung.
- Nur für diese Zwecke erstellt Microsoft Statistiken und sonstige aggregierte Daten (ohne die Inhalte von Kundendaten zu analysieren oder individuelle Nutzer zu identifizieren). Die resultierenden Daten sind stets nicht-personenbezogene Daten.

Die Datenverarbeitung für eigene Geschäftstätigkeiten, die durch die Bereitstellung der Produkte und Services veranlasst sind, ist im Whitepaper hierzu transparent und ausführlich dargestellt: Microsoft data protection and security terms for products and services: Business operations. (siehe dort insb. das Datenflussdiagramm auf S. 9).

1.6. Notwendige Informationen für die Datenschutzdokumentation

Wo finde ich die wichtigsten Informationen, um meiner Rechenschaftspflicht bei Microsoft 365 nachzukommen?

Microsoft stellt das „M365-Kit" als Hilfestellung für Verantwortliche zur Erfüllung ihrer Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO bereit. Es wurde von Microsoft in Abstimmung mit dem Bayerischen Landesamt für Datenschutzaufsicht und dem Hessischen Beauftragten für Datenschutz und Informationsfreiheit entwickelt.

Es richtet sich insbesondere an kleine und mittelständische Unternehmen, die mit dem Einsatz von Microsoft 365 beginnen. Angesichts der Fülle der Einsatzmöglichkeiten von Microsoft 365 bietet das M365-Kit breite Auswahlmöglichkeiten, die aber nicht für jeden Verantwortlichen erforderlich sein müssen. Genauso bleiben alternative Compliance-Lösungen möglich.

Um das Ziel des M365-Kit zu erreichen, enthält es Beispiele für Dokumente bzw. Dokumentenbestandteile, welche Verantwortliche aufgrund ihrer Verpflichtungen aus der DSGVO regelmäßig erstellen müssen.

Das M365 Kit ist unter folgenden Links verfügbar:

- 01_Deckblatt
- 02_Verzeichnis der Verarbeitungstätigkeiten_Beispieleinträge
- 03_Beispielhafte Schwellwertanalysen
- 04_Rechtmäßigkeit der Verarbeitung
- 05_Beispielhafte Datenschutzerklärung
- 06_Erläuterungen zu Microsofts Verständnis der Anonymisierung von Daten_Microsoft_M365

Wo finde ich eine Hilfestellung für meine Datenschutz-Folgenabschätzung?

Um Kunden klare und prägnante Informationen zur Unterstützung bei der Erstellung von Datenschutz-Folgenabschätzungen nach Art. 35 DSGVO (DSFA) bereitzustellen, hat Microsoft anpassbare Vorlagen für eine DSFA entwickelt. Diese basieren auf Microsofts Produktbestimmungen und dem DPA. Sie sollen öffentlichen Organisationen helfen, potenzielle Datenschutzrisiken systematisch zu identifizieren, zu bewerten und zu adressieren.

Derzeit bietet Microsoft folgende anpassbare Vorlagen auf Englisch an:

- Build your own DPIA for Office 365 for Enterprise
- Build your own DPIA for Office 365 for Public Sector
- Build your own DPIA for Microsoft 365 Copilot for Enterprise
- Build your own DPIA for Microsoft 365 Copilot for Public Sector
-

Wo finde ich Informationen zu weiteren Bausteinen meiner Datenschutzdokumentation?

Microsoft stellt umfangreiche, öffentliche Dokumentation zur Verfügung, die Verantwortliche als Bausteine für ihre Datenschutzdokumentation nutzen können:

Teil der Datenschutzdokumentation	Von Microsoft bereitgestellte Informationen
Löschrichtlinie (Artikel 5, 17 DSGVO)	Fundstellen im DPA: • Abschnitt „Hinweise und Kontrollen beim Einsatz von Unterauftragsverarbeitern“ • Anlage 1 – DSGVO-Bestimmungen Weitere Informationen: • Datenaufbewahrung, Löschung und Vernichtung in Microsoft 365 • Automatisches Aufbewahren oder Löschen von Inhalten mithilfe von Aufbewahrungsrichtlinien
Richtlinie zu Betroffenenanfragen (Artikel 12–21 DSGVO)	Fundstellen im DPA: Abschnitt „Rechte der betroffenen Personen; Unterstützung bei Anfragen“ Weitere Informationen: • Anträge betroffener Personen für Office 365 im Rahmen der DSGVO • Anträge betroffener Personen für Azure im Rahmen der DSGVO
Hinreichende Garantien für technische und organisatorische Maßnahmen (Artikel 28 Abs. 1 DSGVO)	Die technische und organisatorische Maßnahmen sind bereits im Abschnitt 1.3 „Technische und organisatorische Maßnahmen“ näher beschrieben.
Richtlinien zu Sicherheitsvorfällen (Artikel 33, 34 DSGVO)	Fundstellen im DPA: Abschnitt „Meldung von Sicherheitsvorfällen“ Weitere Informationen: • MSRC – Microsoft Security Response Center • Verwaltung von Microsoft-Sicherheitsvorfällen • Office 365 Benachrichtigungen bei Datenschutzverletzungen im Rahmen der DSGVO
Transfer Impact Assessment („TIA“) (Artikel 46 DSGVO)	Die Speicherorte und Drittlandtransfers sind bereits in Abschnitt 1.2 „Speicherort und Drittlandtransfers“ näher beschrieben.

2. Künstliche Intelligenz und EU AI Act

2.1. Wie entwickelt und nutzt Microsoft KI verantwortungsvoll?

Microsofts Ziel ist es, KI zu entwickeln und einzusetzen, die einen positiven Einfluss auf die Gesellschaft hat und deren Vertrauen gewinnt. Verantwortungsvolle KI-Nutzung ist für Microsoft von größter Bedeutung. Bereits 2016 hat Microsofts Chairman und CEO Satya Nadella einen klaren Kurs vorgegeben, um einen prinzipienfesten und menschenzentrierten Ansatz für Investitionen in KI zu verfolgen. Seitdem habt Microsoft intensiv daran gearbeitet, KI so zu entwickeln, dass sie mit Microsofts Werten in Einklang steht.

Wie in Microsofts jährlichen Responsible AI Transparency Report dargelegt, hat Microsoft einen Risikomanagement-Ansatz entwickelt, der die gesamte KI-Entwicklung und -Nutzung erfasst. Microsoft beschäftigt etwa 400 Mitarbeitende, die sich mit verantwortungsvoller KI befassen (darunter etwa 200 ausschließlich in diesem Bereich).

Mehr Information finden Sie hier:

- Prinzipien und Ansatz für verantwortungsvolle KI
- How M365 Delivers Trustworthy AI (Service Trust Portal)

2.2. EU AI Act

Was ist der EU AI Act?

Der EU AI Act ist ein umfassendes neues Gesetz, das einheitliche Regeln für potenzielle KI-Risiken für Gesundheit, Sicherheit und Grundrechte in der EU festlegt:

- **Risikobasierter Ansatz:** Der EU AI Act verfolgt einen risikobasierten Ansatz für die Regulierung von KI-Systemen und -Modellen, wobei die wichtigsten Verpflichtungen den Anbietern von Hochrisiko-KI-Systemen und KI-Modellen mit allgemeinem Verwendungszweck mit systemischem Risiko auferlegt werden.
- **Rollenverteilung:** Der EU AI Act verteilt die Verpflichtungen auf alle Akteure in der KI-Lieferkette, von Anbietern der KI-Modelle und KI-Systeme über deren Betreiber bis hin zu Einführern und Händlern.
- **Konkretisierung durch Leitlinien:** In Übereinstimmung mit dem europäischen Rahmen für Produktsicherheit legt der EU AI Act grundlegende Anforderungen abstrakt fest. Verhaltenskodizes und technische Normen werden eine Schlüsselrolle bei der Konkretisierung der Umsetzung des EU AI Acts spielen.
- **Zeitlich gestaffelte Umsetzung:** Der Zeitplan für die Umsetzung des EU AI Acts ist gestaffelt. Die ersten Bestimmungen sind ab Februar 2025 anwendbar, danach werden verschiedene Teile des EU AI Acts bis zum August 2027 gestaffelt anwendbar:

Abbildung 4: EU AI Act Zeitschiene

Weitere Informationen zum EU AI Act finden Sie hier:

- EU AI Act Overview: Eine Zusammenfassung des EU AI Acts, einschließlich der wichtigsten regulatorischen Verpflichtungen, des Anwendungsbereiches und Microsofts Compliance-Ansatzes.
- EU AI Act Infographic: Diese Infografik fasst die Anforderungen des EU AI Acts und Microsofts Compliance-Ansatz zusammen und bietet Kunden einen leicht verständlichen visuellen Leitfaden.
- Microsoft AI Literacy Getting Started Guide: Die Bestimmungen zur KI-Kompetenz des EU AI Acts sind bereits am 2. Februar in Kraft getreten. Dieses Dokument enthält Ressourcen zum Thema KI, um eine informierte Nutzung und den Betrieb von KI-Systemen zu unterstützen und das Bewusstsein für Chancen, Risiken und mögliche Schäden durch KI-Systeme zu schärfen.

Wie setzt Microsoft den AI Act um?

Microsoft ist bereit, seine Kunden bei zwei zentralen Herausforderungen zu unterstützen: Innovation mit KI voranzutreiben und gleichzeitig die Anforderungen des EU AI Acts zu erfüllen.

Microsofts Produkte und Services werden so entwickelt, dass sie den Vorgaben des EU AI Acts entsprechen. Darüber hinaus arbeitet Microsoft eng mit Kunden zusammen, um sicherzustellen, dass sie KI-Technologien gesetzeskonform implementieren und einsetzen können.
In Kooperation mit europäischen Entscheidungsträger*innen entwickelt Microsoft praxistaugliche und effiziente Ansätze zur Umsetzung des EU AI Acts, die sich an internationalen Standards orientieren. Dabei folgt Microsoft den gestaffelten Umsetzungsfristen des AI Acts von Februar 2025 bis August 2027.

Bevor das neu eingerichtete KI-Büro der EU Kommission in den kommenden Monaten weitere Richtlinien veröffentlicht, verfolgt Microsoft bereits jetzt einen proaktiven, mehrstufigen Compliance-Ansatz. Microsoft gehört zu den ersten Organisationen, die sich zu den drei Kernverpflichtungen des AI Pact | Shaping Europe's digital future bekannt haben. Diese freiwilligen Verpflichtungen unterstützen Unternehmen bei der Umsetzung der regulatorischen Anforderungen, die im Rahmen des EU AI Acts auf sie zukommen.

Weitere Informationen finden Sie hier:

- Innovation im Einklang mit dem EU AI Act: Blogpost über Microsofts Maßnahmen zur Umsetzung des EU AI Act.
- EU AI Act Trust Center: Microsofts stets aktuelle Anlaufstelle für Kunden, um über Microsofts Ansatz zum EU AI Act auf dem Laufenden zu bleiben.
- Prohibited Practices One Pager: Zusammenfassung von Microsofts Compliance-Ansatz hinsichtlich verbotener KI-Praktiken.

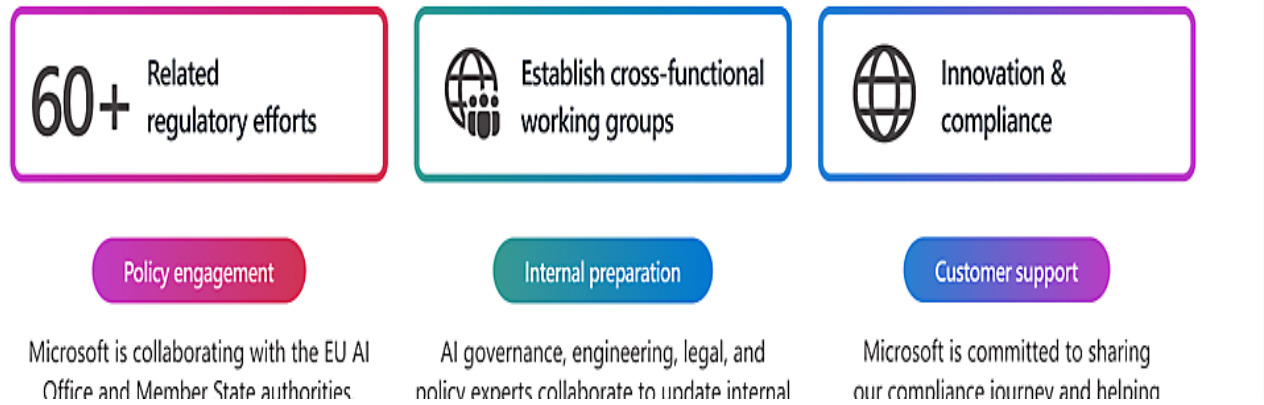


Abbildung 5: Microsoft's Ansatz zum EU AI Act

2.3. Wie wahrt Microsoft den Datenschutz bei der KI-Nutzung?

Microsofts Ansatz für verantwortungsvolle KI basiert auf dem Schutz der Privatsphäre. Microsoft setzt sich weiterhin für seine Grundwerte Datenschutz, Sicherheit und Zuverlässigkeit in seinen Generativen KI-Diensten ein.

Microsoft hält die Verpflichtungen aus dem DPA natürlich auch in Bezug auf KI-Systeme ein. So werden z. B. Kundendaten nur auf dokumentierte Weisung und zur Bereitstellung der Produkte / dadurch veranlasste Geschäftstätigkeiten genutzt (siehe den Abschnitt „Art der Datenverarbeitung" des DPA).

Darüber hinaus hält Microsoft in den Produktbestimmungen ausdrücklich fest:

> *„Generative KI-Dienste von Microsoft verwenden Kundendaten nicht zum Trainieren von Grundlagenmodellen für generative KI, es sei denn, dies geschieht gemäß den dokumentierten Anweisungen des Kunden.*" (siehe die Universellen Lizenzbestimmungen für Onlinedienste in den Produktbestimmungen).

Allgemeine Materialien zum Datenschutz bei Microsofts Generativen KI-Diensten:

- Schutz von Daten für unsere Geschäftskunden und den öffentlichen Sektor im KI Zeitalter
- GDPR & Generative AI – A Guide for Customers (alternativ gibt es auch eine Version dieses Whitepapers für Kunden der öffentlichen Hand: GDPR and Generative AI: A Guide for Public Sector Organizations)

Produktspezifische Materialien zum Datenschutz bei Microsoft 365 Copilot/Microsoft 365 Copilot Chat:

- Microsoft 365 – Microsoft 365 Copilot & Copilot Chat Risk Assessment Quickstart
- Daten, Datenschutz und Sicherheit für Microsoft 365 Copilot
- Schutz von Unternehmensdaten in Microsoft 365 Copilot und Microsoft 365 Copilot Chat
- Transparenzhinweis für Microsoft 365 Copilot

Produktspezifische Materialien zum Datenschutz bei Azure AI Foundry:

- Daten, Datenschutz und Sicherheit für die Verwendung von Modellen über den Modellkatalog im Azure AI Foundry-Portal
- Übersicht über die verantwortungsvolle Verwendung von KI – Azure AI services

2.4. Vertragliche Regelungen der Generativen KI-Dienste von Microsoft

Welche Vertragstexte gelten für Microsoft 365 Copilot/Microsoft 365 Copilot Chat und worin unterscheiden sich beide Produkte?

Unterschiede zwischen beiden Produkten: Microsoft 365 Copilot Chat ist ein KI-Chat, der ohne Zusatzkosten mit Microsoft 365 oder mit einer Entra ID verfügbar ist. Wenn Kunden für den jeweiligen Nutzer eine Microsoft 365 Copilot-Lizenz hinzufügen, werden auch die Unternehmensdaten aus dem Microsoft Graph einbezogen und Microsoft 365 Copilot ist direkt in den Microsoft 365 Apps wie Word, Outlook und Teams integriert (siehe KI-Produktivitätstools für Microsoft 365).

Gleiche Vertragsbedingungen wie sonstiges Microsoft 365: Für Microsoft 365 Copilot/Microsoft 365 Copilot Chat gelten grundsätzlich dieselben Vertragsbedingungen wie sonst auch für Microsoft 365:

- Für beide gilt der DPA, da diese Onlinedienste sind (siehe oben unter 1.1 die Frage „Welche Produkte und Services umfasst Microsofts DPA").
- Ebenfalls sind beide Produkte EU-Datengrenzen-Dienste (siehe den Unterabschnitt „EU-Datengrenzen-Dienste" in den Datenschutz- und Sicherheitsbestimmungen der Produktbestimmungen).
- Auch gelten die sonstigen lizenzrechtlichen Regelungen des Kundenvertrages (insb. MCA oder MBSA/EA).

Ergänzend gilt der Abschnitt „Generative KI-Dienste von Microsoft" der Produktbestimmungen, der produktspezifische Bedingungen für die Generativen KI-Dienste von Microsoft regelt. Zum Beispiel enthält dieser Abschnitt Microsofts Customer Copyright Commitment. Nach diesem wird Microsoft Kunden unter bestimmten Bedingungen gegen Ansprüche Dritter auf geistiges Eigentum hinsichtlich Ausgabeinhalten seiner Generativen KI-Dienste verteidigen (siehe den Blogpost: Microsoft announces new Copilot Copyright Commitment for customers – Microsoft On the Issues)

Websuche in Microsoft 365 Copilot (Chat): Microsoft 365 Copilot und Microsoft 365 Copilot Chat verfügen über ein optionales Feature, das es Copilot ermöglicht, bei der Beantwortung von Benutzerfragen auf Webinhalte zuzugreifen. Dies kann die Qualität der Copilot-Antworten verbessern, weil Copilot dann aktuelle Informationen aus dem Web nutzen kann. Die an Bing gesendete Suchanfrage unterscheidet sich von der ursprünglichen Frage des Benutzers – sie besteht aus nur einigen Wörtern, die Copilot von der Frage des Benutzers ableitet (vgl. Daten, Datenschutz und Sicherheit für die Websuche in Microsoft 365 Copilot und Microsoft 365 Copilot Chat). Diese verkürzten Suchanfragen unterliegen dem Microsoft-Servicevertrag zwischen den einzelnen Benutzern und Microsoft sowie den Microsoft-Datenschutzbestimmungen. Ergänzend gelten die produktspezifischen Bedingungen in den Produktbestimmungen, nach denen Abfragedaten als vertrauliche Kundeninformationen geschützt werden und nur wie dort beschrieben eingeschränkt von Bing genutzt werden.

Welche Vertragstexte gelten für die Azure KI-Services wie Azure AI Foundry?

Für Azure KI-Dienste gelten zunächst dieselben Bedingungen wie für andere Azure-Dienste:

- Der DPA, da diese Onlinedienste sind (siehe oben unter 1.1 die Frage „Welche Produkte und Services umfasst Microsofts DPA").
- Azure AI Foundry ist ein EU-Datengrenzen-Dienst (siehe den Unterabschnitt „EU-Datengrenzen-Dienste" in den Datenschutz- und Sicherheitsbestimmungen der Produktbestimmungen).
- Auch gelten die sonstigen lizenzrechtlichen Regelungen des Kundenvertrages (insb. MCA oder MBSA/EA).

Ergänzend gelten für Azure-KI-Dienste der Abschnitt „Generative KI-Dienste von Microsoft" sowie ggf. produktspezifische Produktbestimmungen (z. B. für Azure AI Foundry). Auch das Customer Copyright Commitment gilt für die Nutzung von Azure OpenAI in Azure AI Foundry.

2.5. KI-Governance und Einbindung von Betriebsräten

Welche Materialien stellt mir Microsoft für meine eigene KI-Governance bereit?

Microsoft teilt seine Erfahrung mit verantwortungsvoller KI-Nutzung und stellt Kunden Materialien und Vorlagen zur Verfügung:

- Verantwortungsvolle KI-Tools und -Methoden | Microsoft KI
- Embrace responsible AI principles and practices – Training | Microsoft Learn
- Responsible AI Impact Assessment Guide
- Responsible AI Impact Assessment Template
- Responsible AI Transparency Report | Microsoft
- AI Literacy Starting Guide
- KI Kompetenz für die Öffentliche Verwaltung

Welche Materialien stellt Microsoft hinsichtlich der Einbindung von Betriebsräten zur Verfügung?

Microsoft agiert als „Customer Zero" und bindet seine Betriebsräte proaktiv ein. Dies ist in den folgenden Materialien dargestellt:

- KI für den Betriebsrat: Übersichtsseite zu Microsofts Webinaren und Materialien für Betriebsräte
- Microsoft workers' council partnerships boost the company's product and service rollouts
- Microsoft's Tips: Partnering with European Works Councils
- Deploying Microsoft 365 Copilot and AI at Microsoft with our works councils: Bericht dazu, wie Microsoft seinen Betriebsrat bei der Einführung von Microsoft 365 Copilot eingebunden hat
- M365 – Copilot adoption with Works Council: Häufigen Themen bei für Betriebsräte bei der Microsoft-365-Copilot-Einführung

3. Digitale Resilienz

3.1. Wie trägt Microsoft zu Europas digitaler Resilienz bei?

Microsoft ist seit 42 Jahren in Europa tätig. Microsoft respektiert europäische Werte, hält sich an europäische Gesetze und verteidigt aktiv Europas Cybersicherheit. In einer Zeit geopolitischer Volatilität verpflichtet sich Microsoft, als verlässlicher Partner Europas digitale Stabilität zu unterstützen.

Darum hat Microsoft im April 2025 die folgenden fünf digitalen Zusicherungen bekannt gegeben:

1. Microsoft wird dabei helfen, ein breit aufgestelltes Cloud- und KI-Ökosystem in Europa zu bauen.
2. Microsoft wird Europas digitale Resilienz aufrechterhalten, und zwar auch in Zeiten von geopolitischer Volatilität.
3. Microsoft wird die Privatsphäre europäischer Daten weiterhin bewahren.
4. Microsoft wird stets helfen, Europas Cybersicherheit zu schützen und zu verteidigen.
5. Microsoft wird zur Stärkung der wirtschaftlichen Wettbewerbsfähigkeit Europas beitragen, auch im Bereich Open Source.

Weitere Informationen finden Sie im Blogbeitrag Microsofts neue digitale Zusicherungen für Europa.

3.2. Welche Angebote bietet Microsoft hinsichtlich digitaler Souveränität?

Die **Microsoft Sovereign Cloud** stellt sicher, dass Kunden das richtige Gleichgewicht zwischen Kontrolle, Compliance und Leistungsfähigkeit für ihre Bedürfnisse wählen können. Sie umfasst sowohl die Public Cloud als auch Private Clouds:

- **Sovereign Public Cloud**: in allen bestehenden europäischen Rechenzentrumsregionen für alle europäischen Kunden verfügbar und umfasst sämtliche Onlinedienste wie Microsoft Azure und Microsoft 365. Die Sovereign Public Cloud stellt sicher, dass die Daten der Kunden in Europa bleiben, dem europäischen Recht unterliegen, der Betrieb und der Zugriff durch europäisches Personal kontrolliert werden und die Verschlüsselung unter der vollen Kontrolle der Kunden steht. Dies ist ohne Migration für alle Kunden-Workloads möglich, die in Microsofts europäischen Rechenzentrumsregionen laufen. Mit der EU-Datengrenze, dem neuen Data Guardian und der Customer Lockbox stellt Microsoft sicher, dass Zugriffe aus Drittstaaten soweit wie möglich reduziert werden. Der Kunde kann mit Confidential Computing zudem seine Kundendaten jederzeit nachweislich verschlüsseln – auch zur Laufzeit.
- **National Partner Cloud:** Das Angebot der **Delos**, einer Tochtergesellschaft von SAP, als National Partner Cloud bietet zukünftig umfassende Funktionen von Office 365 und Microsoft Azure in einer unabhängig betriebenen Umgebung. Dazu besteht eine Technologiepartnerschaft zwischen Microsoft und **Delos**, die eine souveräne Cloud für den deutschen öffentlichen Sektor betreiben wird – konzipiert zur Erfüllung der Cloud-Plattform-Anforderungen des BSI.
- **Sovereign Private Cloud:** Unterstützt kritische Arbeitslasten für Zusammenarbeit, Kommunikation und Virtualisierung über Azure Local und Microsoft 365 Local sowie Microsofts Sicherheitsplattform mit Azure Local und bietet konsistente Funktionen für hybride oder isolierte Umgebungen. Diese Lösung integriert

nun Microsoft 365 Local und Microsofts Sicherheitsplattform mit Azure Local und bietet konsistente Funktionen für hybride oder *Air-Gapped*-Umgebungen, um die Anforderungen an Ausfallsicherheit und Business Continuity zu erfüllen.

Weitere Informationen finden Sie hier:

- Entdecken Sie die Microsoft Sovereign Cloud | Microsoft
- Microsoft kündigt umfassende souveräne Lösungen an, um europäische Organisationen zu unterstützen | News Center Microsoft
- Microsoft Sovereign Cloud Frequently Asked Questions

Diese drei Angebote sind in der folgenden Grafik zusammengefasst:

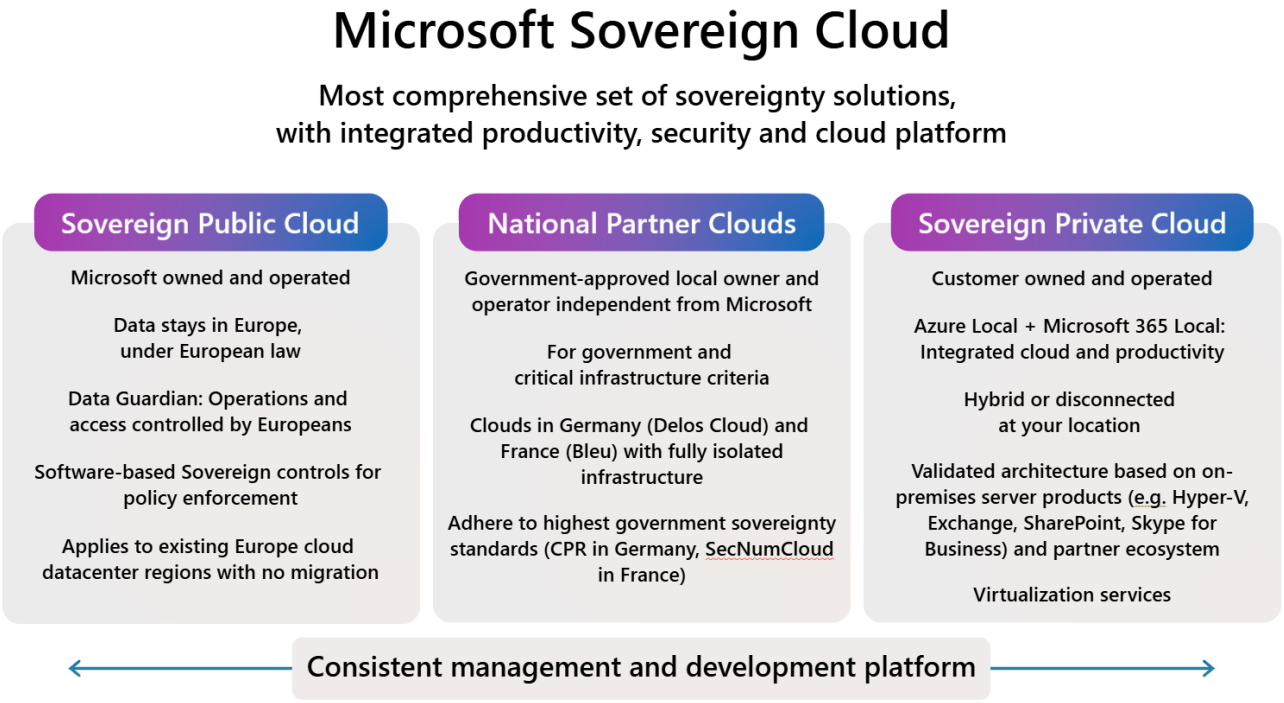


Abbildung 6: Microsoft Sovereign Cloud

4. Sonstige Compliance-Anforderungen

4.1. Können auch Berufsgeheimnisträger die Microsoft-Onlinedienste nutzen?

Ja. § 203 StGB erlaubt es Berufsgeheimnisträgern (beispielsweise Ärzten, Psychologen und Rechtsanwälten) und Amtsträgern, die ihnen anvertrauten Geheimnisse sonstigen mitwirkenden Personen zu offenbaren (z. B. IT-Dienstleistern). Voraussetzung ist, dass nicht mehr Berufsgeheimnisse offengelegt werden, als für die Inanspruchnahme des Dienstleisters erforderlich ist, und der Berufsgeheimnisträger den Dienstleister zur Geheimhaltung verpflichtet. Eine organisatorische Einbindung in die Sphäre des Berufsgeheimnisträgers oder Amtsträger ist nicht erforderlich.

Damit können unterstützende IT-Dienstleistungen, wie die Bereitstellung und der Support von IT-Systemen und Anwendungen, ebenso wie eine Cloudnutzung durch Berufsgeheimnisträger umgesetzt werden. Hierfür bietet Microsoft eine Zusatzvereinbarung für § 203 StGB unterliegende Kunden an, die Onlinedienste über Konzernverträge oder den Microsoft-Kundenvertrag lizenzieren. Kunden, die den Vertrag über einen Microsoft-Partner abschließen, können sich dazu an diesen Partner wenden.

4.2. Wie kann der Kunde seine Daten revisionssicher zur Einhaltung von gesetzlichen Aufbewahrungspflichten aufbewahren?

Microsoft speichert die Daten georedundant an mehreren Stellen in verschiedenen Rechenzentren. Dementsprechend sind zur Wiederherstellung bei Datenverlust in der Regel keine eigenständigen Backups des Kunden erforderlich. Sofern der Kunde die Möglichkeit einer Wiedergabe von historischen Datenständen benötigt, muss er zusätzlich zum Onlinedienst eine Archivierungslösung einsetzen. Der Kunde hat die Möglichkeit im jeweiligen Produkt die Archivierungsfunktionen seinen Bedürfnissen anzupassen und diese selbst einzustellen und zu konfigurieren.

Nach den allgemeinen handels- und steuerrechtlichen Grundsätzen zur Buchführung bedarf es insbesondere der Einhaltung einer ordnungsgemäßen Behandlung elektronischer Dokumente und eines ordnungsgemäßen Zugriffs auf Daten (GoBD). Wesentlicher Kernpunkt ist hierbei das sogenannte „Interne Kontrollsystem“ (IKS). Zum Nachweis eines funktionierenden IKS, welches unternehmensgefährdende Entwicklungen frühzeitig erkennt, bietet Microsoft dem Kunden bzw. dessen Wirtschaftsprüfer eine Attestierung nach dem international anerkannten Prüfungsstandard ISAE 3402 an.

4.3. Was gilt für andere, hier nicht aufgeführte Gesetze?

Im DPA verpflichtet sich Microsoft wie folgt zur Einhaltung gesetzlicher Bestimmungen (siehe Abschnitt „Einhaltung von gesetzlichen Bestimmungen"):

> *„Microsoft befolgt alle für die Bereitstellung der Produkte und Services durch Microsoft geltenden Gesetze und Vorschriften, einschließlich Gesetzen zu Meldepflichten bei Sicherheitsverletzungen, sowie Datenschutzvorschriften. Microsoft ist jedoch nicht für die Einhaltung von Gesetzen oder Regelungen verantwortlich, die für den Kunden oder seine Branche gelten, jedoch nicht allgemein für Serviceprovider im Bereich Informations-technologie. […]*
>
> *Der Kunde muss alle Gesetze und Regelungen einhalten, die für dessen Nutzung von Produkten und Services gelten, einschließlich Gesetzen zu biometrischen Daten, zur Vertraulichkeit von Kommunikation, sowie Datenschutzvorschriften. Der Kunde ist dafür verantwortlich, zu ermitteln, ob die Produkte und Services für die Speicherung und Verarbeitung von Informationen, die spezifischen Gesetzen oder Vorschriften unterliegen, geeignet sind, und muss die Produkte und Services in einer Weise nutzen, die mit den gesetzlichen und regulatorischen Verpflichtungen des Kunden im Einklang steht."*

Dieser Abschnitt gilt auch für Nicht-Datenschutzgesetze (z. B. EU AI Act, Data Act und NIS2-Richtlinie).

Soweit Gesetze sektorspezifisch für den Kunden gelten, muss er selbst prüfen, inwieweit er die jeweiligen Compliance-Pflichten erfüllen kann. Microsoft stellt für manche sektorspezifische Gesetze auch Dokumentation zur Verfügung und bietet teilweise Standard-Zusatzvereinbarungen an. Weitere Informationen finden Sie im Microsoft Trust Center.

Rechtlicher Hinweis

Dieses Compendium enthält eine allgemeine Darstellung von Fragen, die Kunden beim Einsatz von Onlinediensten häufig stellen. Sie sollen damit in die Lage versetzt werden, die rechtlichen Hintergründe beim Einsatz einer Cloud-Computing-Lösung besser zu verstehen. Das Compendium beinhaltet keine einzelfallbezogene Prüfung individueller Rechtsverhältnisse. Für die individuelle und abschließende rechtliche Beurteilung über die Zulässigkeit des Einsatzes von Microsoft Onlinediensten in einem konkreten Anwendungsfall müssen Sie daher eine separate rechtliche Beratung in Anspruch nehmen.

Bitte beachten Sie, dass dieses Dokument nur zu Informationszwecken dient und keine Rechtsberatung darstellt. Es gibt keinen Ersatz dafür, die relevanten Vertragsbedingungen vollständig zu lesen.

Dieses Compendium spiegelt die Versionen des DPA und der Produktbestimmungen wider, die im August 2025 gelten. DPA und der Produktbestimmungen können von Zeit zu Zeit aktualisiert werden, daher sollte immer die neueste Version überprüft werden. Daher enthält das Compendium möglicherweise nicht die aktuellsten Informationen oder Richtlinien.

Microsoft Deutschland GmbH, Walter-Gropius-Str. 5, 80807 München

Bildquelle: eigene