Microsoft

# Microsoft Cloud Compendium

## Fragen und Antworten zur

## Compliance in der Microsoft Enterprise Cloud

Veröffentlicht von Microsoft Corporate, External and Legal Affairs (CELA) Deutschland
Stand: Dezember 2021

# Inhalt


**1. Inwiefern ist das Datenschutzrecht für Kunden von Microsoft Enterprise Cloud Services relevant?** ... 2

**2. Auf welcher rechtlichen Grundlage verarbeitet Microsoft personenbezogene Daten in den Enterprise Cloud Services?** ... 2

**3. Was hat sich durch das Urteil des Gerichtshofs der Europäischen Union („EuGH") in der Rechtssache „Schrems II" vom 16. Juli 2020 für den internationalen Datenverkehr verändert?** ... 3

**4. Was hat Microsoft als Reaktion auf das Urteil des EuGH in der Rechtssache „Schrems II" und die Empfehlungen des Europäischen Datenschutzausschusses unternommen?** ... 3

**5. Hat die Implementierung der neuen Standardvertragsklauseln vom 04. Juni 2021 Auswirkungen auf bereits bestehende Verträge mit Microsoft, in denen die alten Standardvertragsklauseln vereinbart wurden?** ... 4

**6. Das neue DPA gilt auch für alle neuen Verträge und zum Zeitpunkt der Abonnementverlängerung für bestehende Kunden, ohne dass die Kunden etwas unternehmen müssen. Warum befinden sich weiterhin Verweise auf das Privacy Shield im DPA?** ... 5

**7. Welchen Inhalt haben die Vertragsbeziehungen, wenn Unternehmen, insbesondere Microsoft Partner, eine Microsoft-Plattform wie Microsoft Azure nutzen, und darauf aufbauend Services ihren Kunden anbieten?** ... 5

**8. Wo werden Daten in der Microsoft Enterprise Cloud gespeichert?** ... 5

**9. Findet ein Austausch zwischen Microsoft und den Datenschutzaufsichtsbehörden statt?** ... 5

**10. Gibt Microsoft Kundendaten an US-Behörden heraus?** ... 5

**11. Welche Bedeutung hat der amerikanische CLOUD Act?** ... 6

**12. Welche Folgen hat der CLOUD Act für Microsoft?** ... 6

**13. Wie viele Anfragen von Ermittlungsbehörden erhält Microsoft?** ... 7

**14. Können die Microsoft Cloud Services auch von Berufsgeheimnisträgern eingesetzt werden?** ... 7

**15. Wie geht Microsoft mit Verschlüsselung um?** ... 7

**16. Wie können Kunden ihrer Pflicht nachkommen, sich von der Einhaltung aller vereinbarten technischen und organisatorischen Maßnahmen zum Schutz von personenbezogenen Daten zu überzeugen?** ... 7

**17. Wie kann der Kunde seine Daten revisionssicher aufbewahren?** ... 8

**18. Zu welchen Zwecken verarbeitet Microsoft Daten, um Geschäftstätigkeiten von Microsoft zu verfolgen?** ... 8

**19. Verarbeitet Microsoft Daten bei der Verarbeitung für Geschäftstätigkeiten auch für Werbung?** ... 9

**20. Welche sonstigen regulatorischen Anforderungen können neben dem Datenschutzrecht zum Tragen kommen?** ... 9

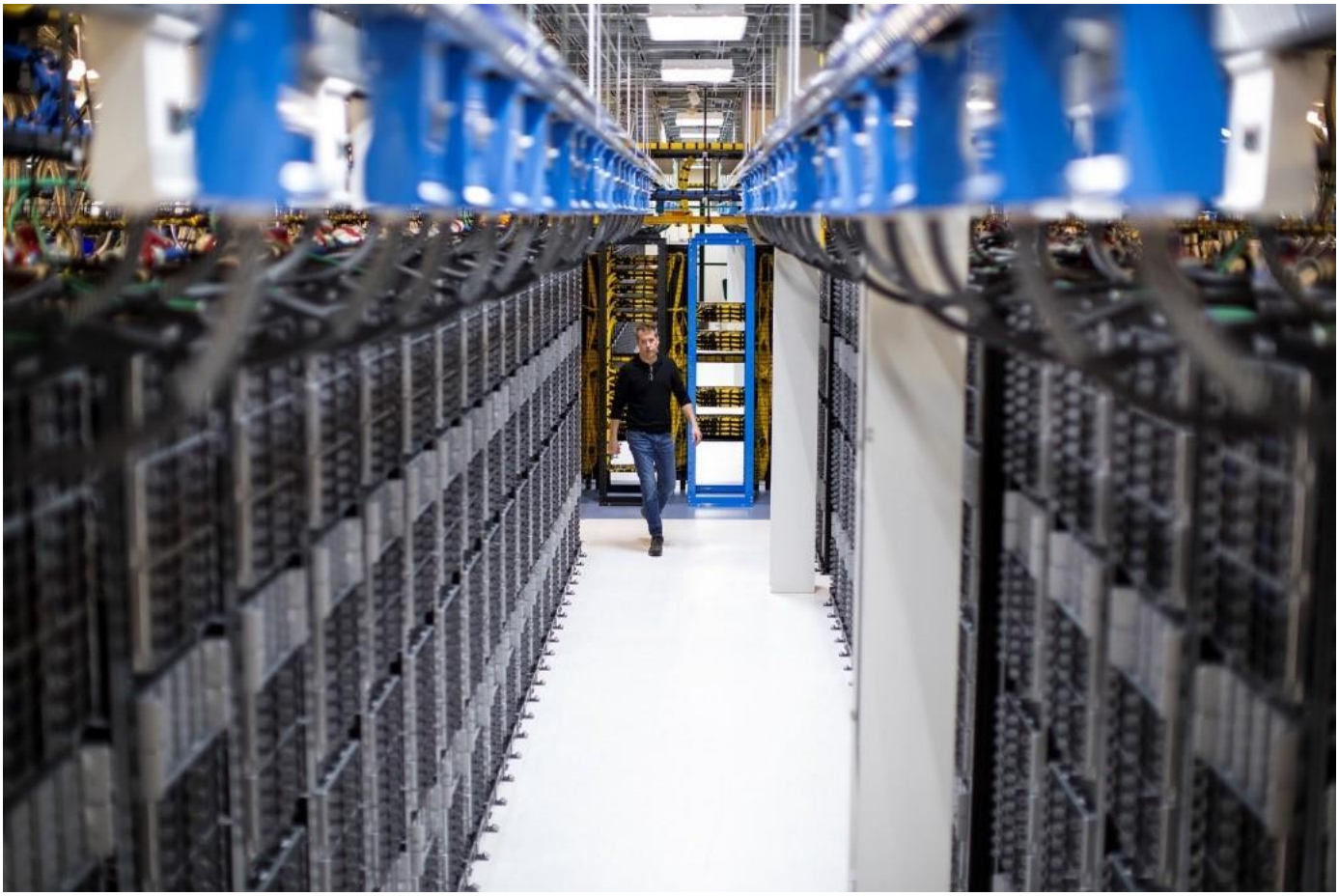
Weitere aktuelle Informationen ... 10

Rechtlicher Hinweis ... 10

# Einleitung

Mit diesem Cloud Compendium möchten wir Antworten auf häufig gestellte Fragen zu den Microsoft Cloud Services geben und ordnen diese in den gesetzlichen und regulatorischen Rahmen ein.

Microsoft ist davon überzeugt, dass Datenschutz und Privatsphäre wichtige Grundrechte sind, und dass die Datenschutz-Grundverordnung (DSGVO) wichtig ist, um die Rechte des Einzelnen zu präzisieren und zu stützen.



## 1. Inwiefern ist das Datenschutzrecht für Kunden von Microsoft Enterprise Cloud Services relevant?

Personenbezogene Daten dürfen von Kunden nur dann in der Cloud verarbeitet werden, wenn dafür eine rechtliche Erlaubnis besteht. Eine Erlaubnis ergibt sich bei Cloud Services in der Regel aus der sogenannten Auftragsverarbeitung, die Microsoft in seinen Verträgen abgebildet hat (siehe dazu nachstehend). Das Datenschutzrecht gilt dabei nur für die Verarbeitung von personenbezogenen Daten. Dies sind – verkürzt gesagt – alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, wie beispielsweise das Geburtsdatum einer natürlichen Person oder deren E-Mail-Adresse. In der Praxis finden sich zumeist eine Vielzahl von personenbezogenen Daten in der Microsoft Enterprise Cloud.

## 2. Auf welcher rechtlichen Grundlage verarbeitet Microsoft personenbezogene Daten in den Enterprise Cloud Services?

Grundlage für die Leistungsbeziehung sind die Lizenzverträge über die Nutzung der jeweiligen Microsoft-Technologie. Diese werden in Europa zwischen dem Kunden und der Microsoft Ireland Operations Limited (nachfolgend: MIOL) abgeschlossen.

Die Lizenzverträge werden durch die „Product Terms" https://www.microsoft.com/licensing/docs/view/Product-Terms und den „Datenschutznachtrag zu den Produkten und Services von Microsoft", „Data Protection Addendum (DPA)" http://aka.ms/dpa, ergänzt (die aktuelle Fassung ist vom 15. September 2021). Das DPA beinhaltet im Abschnitt „Datenschutzbestimmungen" unter anderem Angaben über die Verarbeitung von Daten, die Pflichten von Microsoft sowie Details über getroffene Sicherheitsmaßnahmen.

Zudem schließt Microsoft Standardvertragsklauseln ab. Die Standardvertragsklauseln sind im Jahre 2010 erstmals von der EU-Kommission verabschiedet und am 04. Juni 2021 erneuert worden. Mit dem Abschluss der Standardvertragsklauseln ist Microsoft (inklusive der in den USA ansässigen Microsoft Corporation) verpflichtet, die EU-Datenschutzstandards einzuhalten und diese auch etwaigen Unterauftragsverarbeitern vertraglich aufzuerlegen. Das DPA enthält, auch in der aktualisierten Version vom September 2021, die Standardvertragsklauseln von 2010, die zwischen dem Kunden und der Microsoft Corporation abgeschlossen werden. Diese gelten jedoch nur für bestimmte, im DPA genauer festgelegte Datenübermittlungen von Großbritannien in die USA. Da die Schweiz mittlerweile die neuen Standardvertragsklauseln implementiert hat, gelten für diese nun die aktuellen Standardvertragsklauseln (im DPA von September 2021 unterliegen diese zwar nach dem Wortlaut nach auch noch den Standardvertragsklauseln von 2010, dies ist allerdings durch die aktuelle Rechtslage in der Schweiz nicht mehr relevant). Die neuen Standardvertragsklauseln bieten, neben den bereits bekannten „Controller to Controller" und „Controller to Processor" Modellen, auch die Möglichkeit, die Standardvertragsklauseln in der Verarbeitungskette „Processor to Processor" abzuschließen. Diesem Modell folgt Microsoft, das heißt die für Datenübermittlungen aus der EU in sogenannte Drittstaaten (wie zum Beispiel die USA) geltenden aktualisierten Standardvertragsklauseln vom 04. Juni 2021 wurden zwischen der MIOL und der Microsoft Corporation (als Auftragsverarbeiter-zu-Auftragsverarbeiter-Modul III) abgeschlossen und sind daher nicht mehr Vertragsbestandteil der Kundenverträge. Die zwischen der MIOL und der Microsoft Corporation abgeschlossenen Standardvertragsklauseln vom 04. Juni 2021 sind im Microsoft Service Trust Portal zu finden.

## 3. Was hat sich durch das Urteil des Gerichtshofs der Europäischen Union („EuGH") in der Rechtssache „Schrems II" vom 16. Juli 2020 für den internationalen Datenverkehr verändert?

Für die rechtmäßige Übermittlung von Daten aus der EU in Drittstaaten bedarf es nach der DSGVO einer Rechtsgrundlage. Hierfür gibt es mehrere Möglichkeiten, unter anderem die vorstehend genannten Standardvertragsklauseln. Auch das EU-US Privacy Shield konnte Datentransfers in die USA legitimieren. Der EuGH hat in seinem Urteil vom 16. Juli 2020 in der Rechtssache „Schrems II" das EU-US-Privacy Shield mit sofortiger Wirkung für ungültig erklärt. Damit sind alle Datenübermittlungen, die weiterhin auf alleiniger Grundlage des Privacy Shields erfolgen, unzulässig. Nach dem Urteil des EuGH sind die Standardvertragsklauseln dagegen weiterhin gültig. Der EuGH hält allerdings zusätzlich zu den Standardvertragsklauseln gegebenenfalls noch weitere Maßnahmen für erforderlich, um ein angemessenes Datenschutzniveau im Drittland herzustellen.

Der Europäische Datenschutzausschuss hat nach dem Urteil des EuGH in der Rechtssache Schrems II am 11. November 2020 Handlungsempfehlungen zu den vom EuGH angesprochenen zusätzlichen Maßnahmen ausgesprochen.

Die endgültige Fassung der Handlungsempfehlungen des Europäischen Datenschutzausschusses vom 21. Juni 2021 finden Sie unter https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en. Die Handlungsempfehlungen zielen darauf ab, Verantwortliche und Auftragsverarbeiter, die als Datenexporteure auftreten, bei der Ermittlung und Umsetzung geeigneter zusätzlicher Maßnahmen zu unterstützen, wenn diese erforderlich sind, um ein der Sache nach gleichwertiges Schutzniveau für die Daten, die sie an Drittstaaten übermitteln, zu gewährleisten.

## 4. Was hat Microsoft als Reaktion auf das Urteil des EuGH in der Rechtssache „Schrems II" und die Empfehlungen des Europäischen Datenschutzausschusses unternommen?

(i) Anpassungen am DPA

Microsoft hat als Reaktion auf die mit dem Urteil des EuGH einhergehende Ungültigkeit des EU-US Privacy Shields Anpassungen am DPA vorgenommen und darin alle Datenflüsse aus der EU in Drittstaaten den Standardvertragsklauseln unterworfen. Zudem haben MIOL und Microsoft Corporation die am 04. Juni 2021 aktualisierte Version der Standardvertragsklauseln als Auftragsverarbeiter-zu-Auftragsverarbeiter-Modul III abgeschlossen und in dem am 15. September 2021 veröffentlichten neuen DPA implementiert. Als weitere Maßnahmen zum Schutz personenbezogener Daten hat Microsoft die Verschlüsselung bei der Übertragung von Daten und im Ruhezustand implementiert und speichert - entsprechend der Bestimmungen der Product Terms und des DPA - die meisten Kundendaten im Ruhezustand in einer vom Kunden ausgewählten Region. Zudem hat Microsoft über die Handlungsempfehlungen des Europäischen Datenschutzausschusses hinsichtlich ergänzender Maßnahmen im November 2020 hinausgehend mit folgenden Verpflichtungen reagiert:

- 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 Nutzer*innen 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. Diese Schutzmaßnahmen nennt Microsoft „Defending Your Data" und hat sie als Anhang C in das DPA aufgenommen. Microsoft prüft fortlaufend, ob und welche weiteren ergänzenden Maßnahmen angemessen sind, um den Anforderungen des Europäischen Datenschutzausschusses ausreichend Rechnung zu tragen.

(ii) EU Data Boundary for the Microsoft Cloud

Im Mai 2021 hat Microsoft eine wichtige Ankündigung für unsere Kunden in Europa gemacht: 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. Die Umsetzung ist bis Ende 2022 geplant.

Dabei ist anzumerken, dass die Microsofts Cloud-Services bereits jetzt (auch ohne EU-Datengrenze) die Vorschriften der EU erfüllen. Unternehmenskunden und Kunden aus dem öffentlichen Sektor können Daten in der EU speichern. Viele Azure-Services lassen sich so konfigurieren, dass Daten auch innerhalb der EU verarbeitet werden. Zudem bieten wir ihnen hochwirksame Verschlüsselungen und robuste Lockbox-Lösungen an, die den derzeitigen regulatorischen Vorgaben entsprechen. Bei vielen unserer Services liegt die Kontrolle über die Verschlüsselung der Daten durch die Verwendung von kundenverwalteten Schlüsseln in den Händen der Kunden selbst. Zudem schützen wir die Daten unserer Kunden vor unzulässigem Zugriff durch staatliche Stellen.

Ein Update zu unserem Fortschritt bei diesem ambitionierten Projekt finden Sie hier: https://blogs.microsoft.com/eupolicy/2021/12/16/eu-data-boundary-for-the-microsoft-cloud-a-progress-report/

5. Hat die Implementierung der neuen Standardvertragsklauseln vom 04. Juni 2021 Auswirkungen auf bereits bestehende Verträge mit Microsoft, in denen die alten Standardvertragsklauseln vereinbart wurden?

Das DPA gilt grundsätzlich für die Laufzeit des Abonnements und wird nicht automatisch angepasst. Es besteht jedoch für Kunden, die mit Microsoft bis zum 14. September 2021 ein DPA mit alten Standardvertragsklauseln von 2010 gezeichnet haben, keine Notwendigkeit, eine Zusatzvereinbarung oder ähnliches abzuschließen. Im Einklang mit früheren Aktualisierungen des DPA gelten die hierin geregelten Verpflichtungen von Microsoft, ohne dass die Kunden eine Änderung unterzeichnen oder bis zur Erneuerung ihrer bestehenden Abonnements oder Verträge warten müssen. Die Änderungen sind für Microsoft verbindlich, sobald Microsoft das aktualisierte DPA veröffentlicht. Hierbei handelt es sich um eine einseitige Garantieerklärung von Microsoft, die ein anderes Rechtsinstrument gem. Art. 28 DSGVO darstellt, dem Kunden steht es frei, diese anzunehmen, ein Zugang der Annahme ist hierbei nicht erforderlich.

6. Das neue DPA gilt auch für alle neuen Verträge und zum Zeitpunkt der Abonnementverlängerung für bestehende Kunden, ohne dass die Kunden etwas unternehmen müssen. Warum befinden sich weiterhin Verweise auf das Privacy Shield im DPA?

   Verweise auf das EU-US Privacy Shield bleiben im DPA enthalten, jedoch verlässt sich Microsoft angesichts des „Schrems II"-Urteils nicht länger auf das Privacy Shield als Rechtsgrundlage für die Übermittlung von Daten aus der EU in Drittstaaten. Das US-Handelsministerium hat bekanntgegeben, dass es das Privacy Shield-Regime in den USA aufrechterhalten wird. Microsoft hat sich gegenüber dem US-Handelsministerium verpflichtet, die Privacy-Shield-Bedingungen einzuhalten und wird daher weiterhin – zusätzlich zu den Standardvertragsklauseln – Privacy Shield-konform arbeiten, obwohl dieser Übertragungsmechanismus nicht länger als Rechtsgrundlage für Daten-übermittlungen dient.

7. Welchen Inhalt haben die Vertragsbeziehungen, wenn Unternehmen, insbesondere Microsoft Partner, eine Microsoft-Plattform wie Microsoft Azure nutzen, und darauf aufbauend Services ihren Kunden anbieten?

   Beim sogenannten „Platform as a Service" (PaaS) hängt die Vertragsgestaltung vom Einzelfall ab. Sofern der Microsoft Partner die von ihm entwickelten Applikationen als Service anbieten möchte, ist es zweckmäßig, dass er in seinen Vertragsbedingungen keine weitergehenden Leistungspflichten verspricht, als er mit Microsoft vereinbart hat. Darüber hinaus wird der Partner gegenüber seinen Kunden häufig Auftragsverarbeiter sein, während Microsoft wiederum Unterauftragsverarbeiter ist. Diese Konstellation ist im dem DPA bereits vorgesehen und entsprechend abgebildet.

8. Wo werden Daten in der Microsoft Enterprise Cloud gespeichert?

   Microsoft bietet ein umfassendes Angebot von Cloud-Lösungen aus lokalen Cloud-Rechenzentrumsregionen an. Das geographische Gebiet (sogenannte „Geo"), das der Administrator bei der erstmaligen Einrichtung der Dienste wählt, bestimmt den Speicherort der ruhenden Kundendaten („data at rest").

   Detailliertere Informationen finden Sie hier: https://www.microsoft.com/de-de/trust-center/privacy/data-location, bzw. https://www.microsoft.com/de-de/trust-center/privacy/customer-data-definitions.

9. Findet ein Austausch zwischen Microsoft und den Datenschutzaufsichtsbehörden statt?

   Ja. Microsoft hat lange vor Inkrafttreten der DSGVO das Gespräch mit den nationalen Datenschutzaufsichtsbehörden der EU-Mitgliedstaaten gesucht. Es findet weiterhin ein kontinuierlicher Austausch statt.

10. Gibt Microsoft Kundendaten an US-Behörden heraus?

    Sollte Microsoft eine behördliche Aufforderung zur Herausgabe von Daten erhalten, wird Microsoft die Behörde direkt an den Kunden verweisen. Sollte die Behörde gleichwohl die Herausgabe von gespeicherten Inhaltsdaten von Microsoft verlangen, wird Microsoft die Legitimation des Herausgabeverlangens umfassend rechtlich prüfen und nur

wenn rechtlich erforderlich, der Aufforderung nachkommen (siehe hierzu auch Microsofts Schutzmaßnahmen „Defending Your Data“ unter Ziffer 4 dieses Cloud Compendiums).

## 11. Welche Bedeutung hat der amerikanische CLOUD Act?

US-Amerikanische Strafverfolgungsbehörden erhalten aufgrund des „Clarifying Lawful Overseas Use of Data Act“ („CLOUD Act“) die Möglichkeit, auf Basis von Ermittlungsanordnungen Informationen von amerikanischen Diensteanbietern und deren Tochterunternehmen zu erlangen.

Der CLOUD Act dient der Aufklärung von Straftaten und ändert grundsätzlich nichts an den Prozessen und Anforderungen für Auskunftsanfragen von Strafverfolgungsbehörden. Er schafft einen Rechtsrahmen für die Lösung von Gesetzeskonflikten, indem er die Vereinigten Staaten in die Lage versetzt und ausländische Regierungen ermutigt, bilaterale Abkommen über grenzüberschreitende Ermittlungsersuchen abzuschließen.

Während der CLOUD Act neue Rechte im Rahmen neuer internationaler Abkommen schafft, bleibt das Recht der Cloud Service Provider erhalten, im Falle eines Gesetzeskonflikts vor Gericht zu gehen, um die Rechtmäßigkeit von Durchsuchungsbefehlen überprüfen zu lassen. Greifen Cloud Service Provider Ermittlungsanordnungen an, weil sie gegen das nationale Recht eines Staates verstoßen, kann dieser Verstoß die Aufhebung der Anordnung rechtfertigen. Gleichwohl gibt der CLOUD Act den zuständigen US-Gerichten vor, dass nicht allein der Verstoß gegen ausländisches Recht zur Aufhebung führt. Vielmehr haben die Gerichte eine Gesamtabwägung anzustellen, die in der Konsequenz zu einem überwiegenden Interesse der Strafverfolgungsbehörde an der (unveränderten) Aufrechterhaltung der Ermittlungsanordnung führen kann.

Weitere Einzelheiten zum CLOUD Act finden Sie hier: https://blogs.microsoft.com/on-the-issues/2018/04/03/the-cloud-act-is-an-important-step-forward-but-now-more-steps-need-to-follow und https://news.microsoft.com/de-de/im-daten-dschungel-wie-microsoft-mit-dem-cloud-act-umgeht.

## 12. Welche Folgen hat der CLOUD Act für Microsoft?

Microsoft schützt die Daten seiner Geschäftskunden im Einklang mit den folgenden fünf Prinzipien:

- Microsoft wird die US-Behörden weiterhin an Geschäftskunden verweisen, anstatt freiwillig Daten von Microsoft zu übergeben.
- Microsoft wird weiterhin vor Gericht gehen, um die lokalen Rechte unserer Kunden zu verteidigen, wenn sie von der US-Regierung verletzt werden.
- Microsoft wird weiterhin auf neue internationale Abkommen drängen, die die Rechte unserer Kunden stärken.
- Microsoft wird weiterhin über die Anzahl der internationalen Durchsuchungsbeschlüsse, die Microsoft erhält, transparent informieren.
- Microsoft wird den Kunden weiterhin mehrere Alternativen zur Speicherung ihrer Daten anbieten.

## 13. Wie viele Anfragen von Ermittlungsbehörden erhält Microsoft?

Seit vielen Jahren informiert Microsoft halbjährlich auf seiner Website über die Anzahl der weltweiten erhaltenen behördlichen Ermittlungsanfragen. Diese sogenannten Transparenzberichte finden Sie unter der Rubrik „Digital Trust Reports" hier: https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report. Dort finden Sie auch FAQs, die insbesondere auf die Anzahl der Ermittlungsanfragen in Bezug auf „Enterprise Cloud Customers" genauer eingehen.

## 14. Können die Microsoft Cloud Services auch von Berufsgeheimnisträgern eingesetzt werden?

Ja. § 203 StGB erlaubt es, Berufsgeheimnisträgern (beispielsweise Ärzten, Psychologen und Rechtsanwälten) die ihnen anvertrauten Geheimnisse sonstigen mitwirkende Personen, zum Beispiel externen IT-Dienstleistern, zu offenbaren. 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 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 eingesetzt werden. Hierfür bietet Microsoft eine Zusatzvereinbarung an.

## 15. Wie geht Microsoft mit Verschlüsselung um?

Als Reaktion auf die Berichte über Zugriffe auf Datenleitungen durch Geheimdienste verschiedener Länder übermittelt Microsoft Daten zwischen seinen Rechenzentren ausschließlich verschlüsselt. Microsoft hat Ende 2014 auch die Verschlüsselung der Daten auf seinen Servern bei einzelnen Enterprise Cloud Services eingeführt. Microsoft erfüllt den Anforderungskatalog Cloud Computing (C5) des BSI, in dem auf das Thema Kryptographie und Schlüsselmanagement detailliert eingegangen wird. Ein Link zum Anforderungskatalog und weitergehende Informationen zum Thema finden Sie unter: https://news.microsoft.com/de-de/microsoft-erfuellt-den-anforderungskatalog-cloud-computing-c5-des-bsi-fuer-mehr-als-100-seiner-weltweiten-rechenzentren/.

## 16. Wie können Kunden ihrer Pflicht nachkommen, sich von der Einhaltung aller vereinbarten technischen und organisatorischen Maßnahmen zum Schutz von personenbezogenen Daten 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. 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. Dies ist einer der besten globalen Sicherheitsvergleichs-Benchmarks. Microsoft stellt seinen Kunden auf deren Anforderung einen Überprüfungsbericht nach ISO/IEC 27001 zur Verfügung.

Microsoft hat überdies als erster führender Anbieter von Cloud-Diensten eine Zertifizierung nach dem internationalen ISO/IEC 27018-Standard für Datenschutz in der Cloud erhalten.

Der ISO/IEC 27018-Standard, eine Erweiterung des oben genannten ISO 27001-Standards, wurde von der International Organization for Standardization (ISO) mit dem Ziel entwickelt, ein einheitliches und international gültiges Konzept zu schaffen, um in der Cloud gelagerte personenbezogene Daten zu schützen. Die British Standards Institution hat von unabhängiger Seite überprüft und bestätigt, dass Microsoft Azure, Office 365 und Dynamics 365 mit den „Codes of Practice" des Standards zum Schutz von personenbezogenen Daten in Public Clouds entsprechen.

Diese Zertifizierungen werden im DPA von Microsoft vertraglich vereinbart (für den ISO/IEC 27018-Standard seit April 2015), ändern aber nicht die Rechte aus den Standardvertragsklauseln oder unter der DSGVO ab. Eine Übersicht über weitere Zertifizierungen oder Attestierungen wie zum Beispiel die ISO/IEC 27701, BSI C5 oder den Cloud Code of Conduct finden Sie unter https://www.microsoft.com/de-de/cloud/iso-standards-und-zertifikate.aspx. Weitere Informationen zu den Zertifizierungen der Microsoft Cloud finden Sie hier: https://news.microsoft.com/de-de/im-daten-dschungel-zertifizierungen-der-microsoft-cloud/

## 17. Wie kann der Kunde seine Daten revisionssicher aufbewahren?

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

## 18. Zu welchen Zwecken verarbeitet Microsoft Daten, um Geschäftstätigkeiten von Microsoft zu verfolgen?

Microsoft ist für den Großteil der Datenverarbeitungen als Auftragsverarbeiter des Kunden tätig. Hier bestimmt einzig der Kunde über die Zwecke der Verarbeitung. In begrenztem Umfang verarbeitet Microsoft Daten für Geschäftstätigkeiten von Microsoft, die mit der Bereitstellung der Produkte und Services an den Kunden verbunden sind. Microsoft setzt sich bei dieser Art der Verarbeitung mittels der folgenden vertraglichen Zusagen im DPA enge Grenzen:

(i) Keine Verarbeitung für Benutzerprofilerstellung und Werbung (oder ähnliche kommerzielle Zwecke);

(ii) Verarbeitung ausschließlich für die folgenden sechs Zwecke:

   a. Abrechnungs- und Kontoverwaltung;

   b. Vergütung (zum Beispiel Berechnung von Mitarbeiterprovisionen und Partneranreizen);

   c. interne Berichterstattung und Geschäftsmodellierung (zum Beispiel Prognose, Umsatz, Kapazitätsplanung, Produktstrategie);

d. Bekämpfung von Betrug, Cyberkriminalität oder Cyberangriffen, die Microsoft oder Microsoft-Produkte betreffen könnten;

e. Verbesserung der Kernfunktionalität in Bezug auf Barrierefreiheit, Datenschutz oder Energieeffizienz; und

f. Finanzberichterstattung und Einhaltung gesetzlicher Verpflichtungen (vorbehaltlich der im DPA beschriebenen Offenlegungsbeschränkungen);

(iii) Verarbeitung nach Grundsätzen der Datenminimierung; und

(iv) Soweit die Daten der DSGVO unterliegen, erfüllt Microsoft die Pflichten eines unabhängigen Verantwortlichen gemäß der DSGVO.

## 19. Verarbeitet Microsoft Daten bei der Verarbeitung für Geschäftstätigkeiten auch für Werbung?

Nein, bei der Verarbeitung von Daten für Geschäftstätigkeiten verarbeitet Microsoft Daten nicht für Benutzer-profilierung, Werbung oder ähnliche kommerzielle Zwecke. Die Verarbeitung erfolgt ausschließlich zu den in der Antwort auf Frage 18 genannten Zwecken.

## 20. Welche sonstigen regulatorischen Anforderungen können neben dem Datenschutzrecht zum Tragen kommen?

Sonstige regulatorische Anforderungen können hier nicht abschließend aufgezählt werden. In der Praxis können beispielsweise sektorspezifische Anforderungen wie im Finanzdienstleistungsbereich einschlägig sein. 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. Sofern ein Kunde steuerrechtlich relevante Daten ausschließlich in Microsofts Enterprise Cloud in Rechenzentren in der EU (außerhalb von Deutschland) speichert, muss er sich dies außerdem vom zuständigen Finanzamt genehmigen lassen.

Weitere aktuelle Informationen

- Microsoft Trust Center
  https://www.microsoft.com/de-de/trustcenter

- Neue Maßnahmen zum Schutz Ihrer Daten, Blogbeitrag vom 20.11.2020
  Neue Maßnahmen zum Schutz Ihrer Daten | News Center Microsoft

- Verschlüsselung in der Microsoft Cloud
  Encryption in the Microsoft Cloud - Microsoft 365 Compliance | Microsoft Docs

- Übersicht über die Azure Verschlüsselung und Azure Backup Service
  Übersicht über die Azure-Verschlüsselung | Microsoft Docs
  What is Azure Backup? - Azure Backup | Microsoft Docs

- Datenschutz und Compliance
  https://www.microsoft.com/de-de/trust-center/privacy/gdpr-overview

  https://www.microsoft.com/de-de/trust-center/compliance/compliance-overview

- Datenschutz mit Windows 10 und Microsoft 365 White Paper
  https://aka.ms/DatenschutzMicrosoft365

- Office 365 Trust Center
  https://www.microsoft.com/de-de/trustcenter/CloudServices/office365/default.aspx

- Diagnose Daten
  https://blogs.microsoft.com/on-the-issues/2019/04/30/increasing-transparency-and-customer-control-over-data/

- Microsoft Azure Trust Center
  https://azure.microsoft.com/de-de/support/trust-center

- Dynamics Trust Center
  https://www.microsoft.com/de-de/TrustCenter/CloudServices/dynamics365/default.aspx

- Transparenzberichte
  https://www.microsoft.com/en-us/corporate-responsibility/reports-hub

- Navigating your Way to the Cloud in Europe – Ein Compliance Guide für Cloud Entscheider
  https://www.microsoft.com/en-ie/lcc_cloud/default.aspx

Rechtlicher Hinweis

Dieses Compendium enthält eine allgemeine Darstellung von Fragen, die unsere Kunden beim Einsatz von Cloud Computing Lösungen häufig stellen. Sie sollen damit in die Lage versetzt werden, die rechtlichen Hintergründe beim Einsatz einer Cloud Computing Lösung besser zu verstehen. Dieses Compendium beinhaltet keine einzelfallbezogene Prüfung individueller Rechtsverhältnisse. Für die individuelle und abschließende rechtliche Beurteilung über die Zulässigkeit des Einsatzes von

Microsoft Cloud Lösungen in einem konkreten Anwendungsfall müssen Sie daher eine separate rechtliche Beratung in Anspruch nehmen.

**Microsoft Deutschland GmbH, Walter-Gropius-Str. 5, 80807 München** Bildquelle: eigene