Microsoft

Microsoft Cloud Compendium

Fragen und Antworten zur

Compliance in der Microsoft Enterprise Cloud

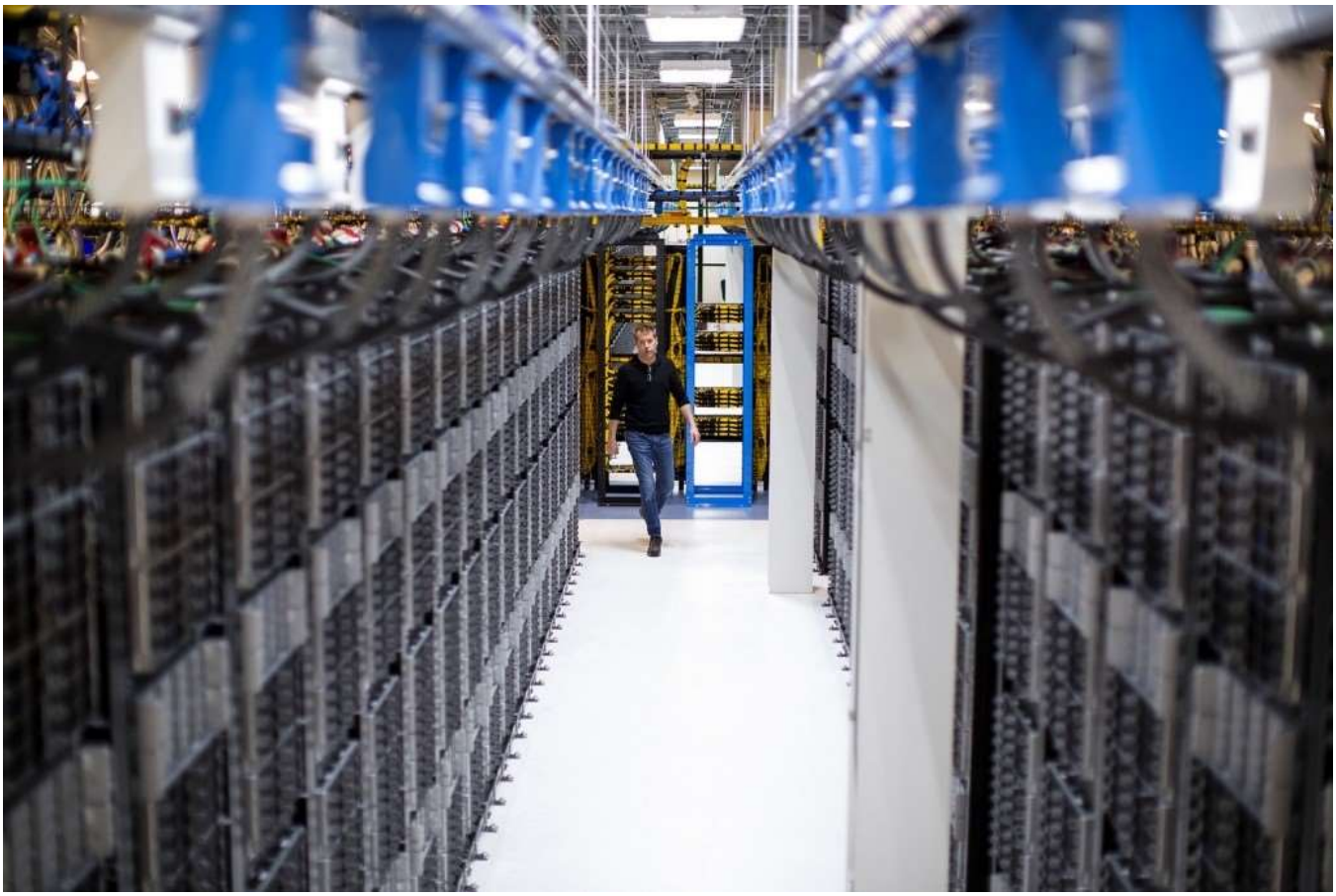
Veröffentlicht von Microsoft Corporate, External and Legal Affairs (CELA) Deutschland
Stand: Dezember 2020

Inhalt

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) ein wichtiger Schritt nach vorn 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 sog. 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 „Online Services Terms" (OST) http://aka.ms/ost, und den „Anhang zu den Datenschutzbestimmungen für Microsoft-Onlinedienste", Data Protection Addendum (DPA) http://aka.ms/dpa, ergänzt. Der DPA beinhaltet im Abschnitt „Datenschutzbestimmungen" unter anderem Angaben über die Verarbeitung von Daten, die Pflichten von Microsoft sowie Details über getroffene Sicherheitsmaßnahmen.

Zudem beinhaltet das DPA als Anlage 2 die Standardvertragsklauseln (auch „EU-Standarddatenschutzklauseln" genannt), die zwischen dem Kunden und der Microsoft Corporation abgeschlossen werden. Die Standardvertragsklauseln sind im Jahre 2010 von der EU-Kommission verabschiedet worden. Mit dem Abschluss der Standardvertragsklauseln ist die Microsoft Corporation verpflichtet, die EU-Datenschutzstandards einzuhalten und diese auch etwaigen Subunternehmern vertraglich aufzuerlegen.

3. Was hat sich durch das Urteil des Europäischen Gerichtshofs („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 sogenannte Drittstaaten (wie z.B. die USA) bedarf es nach der DSGVO einer Rechtsgrundlage. Hierfür gibt es mehrere Möglichkeiten, u.a. die vorstehend genannten EU-Standardvertragsklauseln. Auch das EU-U.S. Privacy Shield konnte Datentransfers in die USA legitimieren. Es ist ein auf einem Abkommen zwischen der EU und der US-Regierung basierender Angemessenheitsbeschluss, demzufolge sich US-Unternehmen freiwillig zur Einhaltung der in dem Abkommen niedergelegten EU-Datenschutzstandards verpflichten können. Der Europäische Gerichtshof („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 EU-Standardvertragsklauseln dagegen weiterhin gültig. Der EuGH hält allerdings zusätzlich zu den Standardvertragsklauseln ggf. noch weitere Maßnahmen für erforderlich, um ein angemessenes Datenschutzniveau im Drittland herzustellen.

4. Was hat Microsoft als Reaktion auf das Urteil des EuGH in der Rechtssache „Schrems II" unternommen?

Microsoft hat als Reaktion auf die mit dem Urteil einhergehende Ungültigkeit des EU-US Privacy Shields Anpassungen am DPA vorgenommen und darin alle Datenflüsse den Standardvertragsklauseln unterworfen. Als weitere Maßnahmen zum Schutz personenbezogener Daten hat Microsoft bereits die Verschlüsselung bei der Übertragung der Daten und im Ruhezustand implementiert und speichert, entsprechend der Bestimmungen der OST und des DPA, die meisten Kundendaten im Ruhezustand in der Region. Zudem hat Microsoft bereits auf die Handlungsempfehlungen des Europäischen Datenschutzausschusses vom 11.November 2020 mit folgenden Verpflichtungen reagiert: Erstens verpflichten wir uns, dass wir jede Anfrage einer staatlichen Stelle 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. Diese Schutzmaßnahmen nennen wir „Defending Your Data". Wir werden unverzüglich damit beginnen, sie in unsere Verträge mit Unternehmenskunden und Kunden aus dem öffentlichen Sektor aufzunehmen.

5. 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 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 Datenübermittlungen dient.

6. Ändert sich etwas an den Vertragsbeziehungen, wenn die Cloud Services von verschiedenen Konzerngesellschaften des Kunden genutzt werden?

Die Enterprise Cloud Services können von einer zentralen Konzerngesellschaft, beispielsweise der IT-Dienstleistungsgesellschaft des Konzerns, bezogen werden. Der Lizenzvertrag wird zwischen dieser Konzerngesellschaft und MIOL abgeschlossen. Auf Kundenseite sollten alle nutzenden Konzerngesellschaften die Auftragsverarbeitungsvereinbarung und die EU-Standardvertragsklauseln unterzeichnen. Diese sind aus Sicht der Datenschutzaufsichtsbehörden die sog. Verantwortlichen, welche die unmittelbare Vertragsbeziehung zu der nicht in der EU ansässigen Microsoft Corporation haben sollen. Hierfür bietet Microsoft eine Zusatzvereinbarung an.

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.

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

Microsoft entwickelt seine Cloud-Strategie kontinuierlich weiter und bietet ein umfassendes Angebot seiner weltweiten Cloud-Lösungen aus lokalen Cloud-Rechenzentrumsregionen an. Das geographische Gebiet (sog. Geo), das der Administrator bei der erstmaligen Einrichtung der Dienste wählt, bestimmt den Speicherort der ruhenden Kundendaten („data at rest").

Weitere 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 den Behörden keine Daten zur Verfügung stellen, sondern die anfordernde Behörde direkt an den Kunden verweisen. Sollte die Behörde gleichwohl die Herausgabe von gespeicherten Inhaltsdaten von Microsoft verlangen, wird Microsoft die Legitimation des Herausgabeverlangen umfassend rechtlich prüfen und wenn rechtlich erforderlich, der Aufforderung nachkommen (siehe hierzu auch unsere Schutzmaßnahmen „Defending Your Data" unter Ziffer 4 des 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.

12. Welche Folgen hat der CLOUD Act für Microsoft?

Microsoft hält sich an die folgenden fünf Prinzipien, um die Privatsphäre seiner Geschäftskunden auch in Zukunft zu schützen:

- 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 wir erhalten, transparent sein.
- Microsoft wird unseren Kunden weiterhin mehrere Alternativen zur Speicherung ihrer Daten anbieten.

13. Wie viele Anfragen von Ermittlungsbehörden erhält Microsoft?

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

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

Ja. § 203 StGB erlaubt die Offenlegung der Berufsgeheimnisträgern (beispielsweise Ärzte, Psychologen oder Rechtsanwälte) anvertrauten Geheimnisse an sonstige mitwirkende Personen, z.B. externe IT-Dienstleister, sofern dabei 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 im Übrigen 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 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 Zertifikate unabhängiger Dritter vorlegen lassen. Jedes Jahr unterzieht sich Microsoft daher Überprüfungen durch Dritte. Diese Überprüfungen werden von international anerkannten Auditoren durchgeführt. Diese überprüfen, ob Microsoft die Richtlinien und Verfahren für Sicherheit, Datenschutz, Kontinuität und Konformität gewährleistet. Grundlage ist der ISO 27001-Standard. Dies ist einer der besten globalen Sicherheitsvergleichs-Benchmarks. Microsoft stellt seinen Kunden auf deren Anforderung einen Überprüfungsbericht nach ISO 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, dass Microsoft Azure, Office 365 und Dynamics 365 mit den „Codes of Practice" des Standards zum Schutz von personenbezogenen Daten in Public Clouds entsprechen. Zudem wurde dieser Test für Microsoft Intune vom Bureau Veritas durchgeführt.

Diese Zertifizierungen werden in den Microsoft Online Services Terms vertraglich vereinbart (für den ISO/IEC 27018-Standard seit April 2015), ändern aber nicht die Rechte aus den EU-Standardvertragsklauseln oder unter der DSGVO ab. Eine Übersicht der ISO-Standards und weiterer Zertifizierungen, unter anderem unterschiedliche SOC Kontrollstandards für die Microsoft Cloud finden Sie unter https://www.microsoft.com/de-de/cloud/iso-standards-

und-zertifikate.aspx und https://docs.microsoft.com/de-de/microsoft-365/compliance/offering-soc?view=o365-worldwide.

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 Back-ups 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 legitime Geschäftstätigkeiten von Microsoft zu verfolgen?

Microsoft ist für den Großteil der Datenverarbeitungen als Auftragsverarbeiter tätig. Im begrenzten Umfang verarbeitet Microsoft Daten auch als unabhängiger Datenverantwortlicher.

Microsoft verarbeitet Daten für legitime Geschäftstätigkeiten als unabhängiger Datenverantwortlicher ausschließlich zu folgenden sechs im DPA definierten Zwecken: (1) Abrechnungs- und Kontoverwaltung; (2) Vergütung (z. B. Berechnung von Mitarbeiterprovisionen und Partneranreizen); (3) interne Berichterstattung und Modellierung (z. B. Prognose, Umsatz, Kapazitätsplanung, Produktstrategie); (4) Bekämpfung von Betrug, Cyberkriminalität oder Cyberangriffen, die Microsoft oder Microsoft-Produkte betreffen könnten; (5) Verbesserung der Kernfunktionalität in Bezug auf Barrierefreiheit, Datenschutz oder Energieeffizienz; und (6) Finanzberichterstattung und Einhaltung gesetzlicher Verpflichtungen (vorbehaltlich der im DPA beschriebenen Offenlegungsbeschränkungen).

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

Nein, bei der Verarbeitung von Daten für legitime Geschäftstätigkeiten verarbeitet Microsoft Daten als selbstständiger Verantwortlicher nicht für Benutzerprofilierung, Werbung oder ähnliche kommerzielle Zwecke. Die Verarbeitung erfolgt ausschließlich zu den in der Antwort auf Frage 19 genannten Zwecken.

20. Warum ist Microsoft bei der Verarbeitung von Daten für legitime Geschäftszwecke unabhängige Datenverantwortliche?

Im Rahmen der Verarbeitung von Daten zu legitimen Geschäftszwecken, bestimmt Microsoft sowohl die Mittel als auch die Zwecke der Datenverarbeitung. Damit ist Microsoft allein für die Einhaltung aller geltenden Gesetze sowie die Erfüllung der Verpflichtungen als Verantwortliche für diese Datenverarbeitungen verantwortlich.

21. 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 Unternehmen gefährdende Entwicklungen frühzeitig erkennt, bietet Microsoft dem Kunden bzw. dessen Wirtschaftsprüfer eine Zertifizierung nach dem international anerkannten Prüfungsstandard ISAE 3402 an. Sofern ein Kunde steuerrechtlich relevante Daten ausschließlich in Microsofts Enterprise Cloud in Rechenzentren in der EU 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
  aka.ms/DatenschutzMicrosoft365
- Office 365 Trust Center
  https://www.microsoft.com/de-de/trustcenter/CloudServices/office365/default.aspx
- Diagnostische Daten
  https://blogs.microsoft.com/on-the-issues/2019/04/30/increasing-transparency-and-customer-control-over-data/
- Microsoft Azure Trust Center
  http://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 Kunde 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