Microsoft Cloud Compendium
Fragen und Antworten

Compliance in der Microsoft Enterprise Cloud

Veröffentlicht von Microsoft Corporate, External and Legal Affairs (CELA) Deutschland
Stand: March 2019

Compliance in der Microsoft Enterprise Cloud

Veröffentlicht von Microsoft Corporate, External and Legal Affairs (CELA), Deutschland
Stand: March 2019

Wo werden Daten in der Microsoft Enterprise Cloud gespeichert?

Microsoft verfolgt bei den Rechenzentren eine an den Regionen orientierte Strategie. Das Land oder die Region des Kunden, das oder die der Administrator bei der erstmaligen Einrichtung der Dienste wählt, bestimmt den primären Speicherort für die Daten des Kunden bei Office 365, Dynamics 365 und Windows Intune („data at rest"). Für deutsche Kunden werden daher standardmäßig die Kundendaten der Microsoft Enterprise Services (Office 365, Dynamics 365 und Windows Intune) in den Microsoft Rechenzentren in der Europäischen Union (EU), vor allem in Dublin und Amsterdam, gespeichert. Weitere Informationen finden Sie hier: https://www.microsoft.com/de-de/trustcenter/Privacy/Where-your-data-is-located. Bei Azure Services können Kunden die Region, in der die Daten gespeichert werden, regelmäßig wählen. Einige Services ermöglichen keine regionale Speicherung; Informationen dazu finden sich im Trust Center. Die entsprechenden Links finden Sie am Ende dieses Dokumentes.

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

Personenbezogene Daten dürfen Kunden nur dann in der Cloud verarbeiten, wenn dafür eine rechtliche Erlaubnis besteht. Eine Erlaubnis ergibt sich bei Cloud Services in der Regel aus der sog. Auftragsverabeitung, 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 der Name einer natürlichen Person oder deren E-Mail-Adresse. In der Praxis finden sich zumeist eine Vielzahl von personenbezogenen Daten in der Microsoft Enterprise Cloud. Es gibt aber auch Fälle, in denen nur wenige und wenig schutzbedürftige personenbezogene Daten verarbeitet werden, beispielsweise wenn Schnittmuster eines Modeherstellers in Azure gespeichert werden.

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 ergänzt (aktuelle Fassung unter http://aka.ms/Wkcowi). Diese beinhalten im Abschnitt „Datenschutzbestimmungen" unter anderem die gesetzlich vorgeschriebenen Regelungen für eine Auftragsverarbeitung gemäß Art. 28 DSGVO.

Zudem beinhalten sie als Anhang 3 die EU-Standardvertragsklauseln, die zwischen dem Kunden und der Microsoft Corporation als Subunternehmerin der MIOL abgeschlossen werden.

Die EU-Standardvertragsklauseln sind von der EU-Kommission verabschiedet worden. Werden diese Klauseln unverändert eingesetzt, ist eine Weitergabe von personenbezogenen Daten datenschutzrechtlich zulässig. Damit ist die Microsoft Corporation verpflichtet, die EU-Datenschutzstandards einzuhalten und diese auch etwaigen Subunternehmern vertraglich aufzuerlegen.

Was hat sich durch die EU-Datenschutz-Grundverordnung geändert?

Seit dem 25. Mai 2018 gilt die EU-Datenschutz-Grundverordnung (nachfolgend: DSGVO). Sie ersetzt die Datenschutzrichtlinie 95/46/EG aus dem Jahr 1995.

Im Unterschied zu der Richtlinie handelt es sich bei der DSGVO nicht um eine Vorgabe, die von den Parlamenten der Mitgliedsstaaten in nationales Recht umgesetzt werden muss. Vielmehr gilt die DSGVO in allen Mitgliedsstatateen der EU ohne Umsetzungsakt direkt. Die DSGVO ermöglicht den Mitgliedstaaten aufgrund sog. Öffnungsklauseln, in bestimmten Bereichen nationales Datenschutzrecht zu schaffen. Diese nationalen Regelungen modifizieren die Regelungen der DSGVO. Nationale Regelungen hat der deutsche Gesetzgeber beispielsweise im neuen Bundesdatenschutzgesetz für die Bereiche Beschäftigtendatenschutz oder Videoüberwachung geschaffen.

Die Auftragsverarbeitung ist für privatwirtschaftliche Unternehmen abschließend in Art. 28 DSGVO geregelt, ohne dass das BDSG diese Regelung modifiziert. Zwar hält das BDSG in den §§ 62 und 64 BDSG Regelungen zur Auftragsverarbeitung vor; diese gelten allerdings nur für staatliche Ermittlungsbehörden und nicht für privatwirtschaftliche Unternehmen.

Art. 28 DSGVO ist daher bei einer sog. Verarbeitung von Daten im Auftrag die maßgebliche Vorschrift. Microsoft bietet seinen Kunden die Online Services Terms mit einer Anlage 4 (Bestimmungen der Datenschutz-Grundverordnung der Europäischen Union) diejenigen Regelungen an, die nach Art. 28 der DSGVO abzuschließen sind. Dies gewährleistet, dass die Microsoft Enterprise Services rechtskonform im Sinne der DSGVO eingesetzt werden können.

Grafisch stellt sich das Vertragskonstrukt wie folgt dar:

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

Die Cloud Services können weiterhin 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.

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

Sind die Enterprise Cloud-Verträge von Microsoft mit den Datenschutzaufsichtsbehörden abgestimmt?
Ja. Das European Data Protection Board (EDPB) – ein Abstimmungsgremium aller 28 nationalen Datenschutzaufsichtsbehörden der EU-Mitgliedstaaten (auch sog. Article 29 Working Party genannt – hat Microsoft mit Schreiben vom 2. April 2014 bestätigt, dass das vorgelegte Microsoft-Vertragswerk eine ordnungsgemäße Umsetzung der EU-Standardvertragsklauseln darstellt und damit ein angemessenes Datenschutzniveau bei Empfängern außerhalb der EU herstellt (Ref. Ares(2014)1033670 - 02/04/2014). Sie hat damit festgestellt, dass das Microsoft-Vertragswerk alle Inhalte aufweist, die für eine weisungsgebundene Beauftragung von Dienstleistern außerhalb der EU erforderlich sind.

Für Unternehmen in Deutschland bedeutet dies, dass die Nutzung von Enterprise Cloud Services nicht durch die Aufsichtsbehörden genehmigt werden muss. Die Aufsichtsbehörden können nur prüfen, ob die Datenverarbeitung an sich zulässig ist, so wie sie dies auch im eigenen Rechenzentrum des Kunden überprüfen könnten.

Welche Bedeutung hat das EU-U.S. Privacy Shield für den Einsatz der Microsoft Cloud Services?
Prinzipiell gibt es mehrere Möglichkeiten, Datentransfers in die USA zu legitimieren, insbesondere EU-Standardvertragsklauseln, Angemessenheitsbeschlüsse der EU-Kommission sowie – genehmigungspflichtige – Binding Corporate Rules oder individualisierte Datenexportverträge.

Auch das EU-U.S. Privacy Shield kann Datentransfers in die USA legitimieren. Es ist ein datenschutzrechtliches Abkommen zwischen der EU und der US-Regierung, demzufolge sich US-Unternehmen freiwillig zur Einhaltung der in dem Abkommen niedergelegten EU-Datenschutzstandards verpflichten können. Am 12. Juli 2016 hat die EU-Kommission durch einen Angemessenheitsbeschluss festgestellt, dass bei jenen Unternehmen, die sich nach EU-U.S. Privacy Shield zertifizieren lassen, ein für die Weitergabe in die USA erforderliches angemessenes Datenschutzniveau besteht. Das EU-U.S. Privacy Shield gilt als Nachfolger des zuvor durch den EuGH aufgehobenen „Safe Harbor"-Abkommens.

Microsoft ist seit August 2016 nach den Regeln des EU-U.S. Privacy Shield zertifiziert (https://www.privacyshield.gov/participant?id=a2zt0000000KzNaAAK&status=Active). Somit besteht für die Übermittlung von personenbezogenen Daten sowohl in den Microsoft Core Services als auch in den Non-Core Services, z.B. die Azure Non-Core Services, an die Microsoft Corp in den USA – ungeachtet der EU-Standardvertragsklauseln – die erforderliche rechtliche Grundlage.

Eine Genehmigung des Datentransfers durch die Datenschutzaufsicht ist angesichts der verbindlichen Entscheidung der EU-Kommission zum EU-U.S. Privacy Shield nicht erforderlich.

Gibt Microsoft Kundendaten an US-Behörden wie die National Security Agency (NSA) heraus?
Sollte Microsoft eine 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 dieses Herausgabeverlangen umfassend rechtlich prüfen.

Wie ist das Gerichtsverfahren vor dem Supreme Court ausgegangen?
Dem Supreme Court Verfahren lag die Frage der Rechtmäßigkeit eines Durchsuchungsbeschluss (sog. „search warrant") zugrunde, der von einem New Yorker Gericht erlassen worden war. Der Durchsuchungsbeschluss forderte Microsoft auf, den E-Mail Verkehr eines Kunden herauszugeben, der in einem irischen Rechenzentrum von Microsoft gespeichert ist. Dem hatte sich Microsoft widersetzt und vor dem US Court of Appeals obsiegt.

Während der Fall dann vom US Supreme Court verhandelt wurde, beschloss der Kongress im März 2018 den „Clarifying Lawful Overseas Use of Data Act" (nachfolgend CLOUD Act). Mit dem CLOUD Act wurde die bisherige Gesetzeslage unter anderem dahingehend geändert, dass speziell die Speicherung von Daten in der Cloud durch Kommunikationsanbieter mit US-Bezug unabhängig vom Standort der Cloud-Server einbezogen wurde. Da die rechtlichen Fragestellungen des „New York Search Warrant"-Falles auf Grundlage des CLOUD Acts obsolet wurden, wurde der Fall für ungültig erklärt und an die unteren Gerichte zurückverwiesen, um die Klage abzuweisen. Weitere Einzelheiten finden Sie in dem Blogpost von Brad Smith hier: Blog Brad Smith 11 Sept 2018

Welche Bedeutung hat der neue amerikanische CLOUD Act?
Amerikanische Strafverfolgungsbehörden erhalten aufgrund des CLOUD Acts die Möglichkeit, auf Basis von Ermittlungsanordnungen Informationen von amerikanischen Diensteanbietern und deren Tochterunternehmen zu erlangen, die diese im Ausland speichern. Der CLOUD Act dient der Aufklärung von Straftaten. Der CLOUD Act verpflichtet nicht automatisch die Cloud Service-Provider, Kundendaten an US-

Ermittlungsbehörden herauszugeben. Es schafft lediglich einen Rechtsrahmen für die Lösung von Gesetzeskonflikten, indem es 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 alleine 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.

Zu beachten ist, dass Cloud Service Provider Ermittlungsanordnungen bereits dann angreifen können, wenn sie einen Verstoß gegen das internationale "comity" befürchten. Dies ist weiterreichender als eine bloße Verletzung nationalen Rechts, weil es die gegenseitige Rücksichtnahme auf staatlicher Ebene umfasst. Der Grundsatz der Völkercourtoise (prinicple of comity) bedeutet, dass die Staaten aus völkerrechtlichen Gründen unter anderem auf das in den anderen Staaten bestehende Recht Rücksicht nehmen müssen. Weitere Einzelheiten zum CLOUD Act finden Sie hier.

Welche Folgen hat der neue amerikanische CLOUD Act für Microsoft?

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

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

Weitere Informationen über den prinzipientreuen Weg für Microsoft nach der Verabschiedung des CLOUD Act finden Sie hier.

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. 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.

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 den Support von IT-Systemen und Anwendungen, ebenso wie eine Cloudnutzung durch Berufsgeheimnisträger eingesetzt werden. Hierfür bietet Microsoft eine Zusatzvereinbarung an.

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.

Kann die Anwendbarkeit des Datenschutzrechts durch Verschlüsselung ausgeschlossen werden?

Dies hängt vor allem von der Art und Weise der Verschlüsselung ab. Sofern eine Verschlüsselung sowohl auf dem Transportweg zwischen Kunde und Microsoft als auch der gespeicherten Daten in der Cloud erfolgt und der Schlüssel allein beim Kunden liegt, liegen aus der Sicht von Microsoft keine personenbezogenen Daten vor. In diesem Fall ist auf die Verarbeitung durch Microsoft das Datenschutzrecht nicht anwendbar.

Microsoft bietet seinen Kunden hierzu an, ihren eigenen Schlüssel für die Verschlüsselung von Daten in Microsoft Azure Rights Management zu verwenden. Dabei wird der Schlüssel durch ein Hardware-Sicherheitsmodul (HSM) des Herstellers Thales geschützt, so dass Microsoft den Schlüssel nicht exportieren und weitergeben kann. Eine solche Verschlüsselung würde den Personenbezug von Daten ausschließen, kann jedoch die Funktionalität, wie die Suchfunktion, einschränken.

Es werden aber immer Daten wie die Admin- bzw. Metadaten entstehen, die nicht verschlüsselt werden können, so dass zumindest insofern das Datenschutzrecht zu beachten ist. In jedem Fall ist eine Verschlüsselung ein datenschutzrechtlich positiv zu bewertender Schutz.

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 zu überzeugen. Kunden können dieser Pflicht nachkommen, indem sie sich Zertifikate unabhängiger Dritter vorlegen lassen. Jedes Jahr unterzieht sich Microsoft daher einer Überprüfung durch Dritte. Diese Überprüfung wird 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 (BSI) 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 (OST) 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.

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.

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

Die 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 finden Sie hier:

- Microsoft Trustcenter
  https://www.microsoft.com/de-de/trustcenter
- Office 365 Trust Center
  https://products.office.com/de-DE/business/office-365-trust-center-welcome
- Microsoft Azure Trust Center
  http://azure.microsoft.com/de-de/support/trust-center
- Dynamics Trust Center
  https://www.microsoft.com/en-us/trustcenter/cloudservices/dynamics365
- Transparenzberichte
  https://www.microsoft.com/en-us/corporate-responsibility/reports-hub

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.

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

Bildquelle: eigene, shutterstock_78032764, bartzuza