Microsoft Cloud Compendium
Fragen und Antworten

Compliance in der Microsoft Enterprise Cloud

Veröffentlicht von Microsoft Corporate, External and Legal Affairs (CELA) Deutschland
Stand: Oktober 2017

Compliance in der Microsoft Enterprise Cloud

Veröffentlicht von Microsoft Corporate, External and Legal Affairs (CELA), Deutschland
Stand: Oktober 2017

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 eingibt, 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: **http://aka.ms/dataflowmap**. 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. Auftragsdatenverabeitung, 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 – Angaben über eine bestimmte oder bestimmbare natürliche Person, 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.

Microsoft bietet mit der Microsoft Cloud Deutschland auch Cloud Services ausschließlich aus Rechenzentren in Deutschland an. Heißt das, dass aus datenschutzrechtlichen Gründen ein deutscher Kunde die Microsoft Cloud Deutschland nutzen muss?

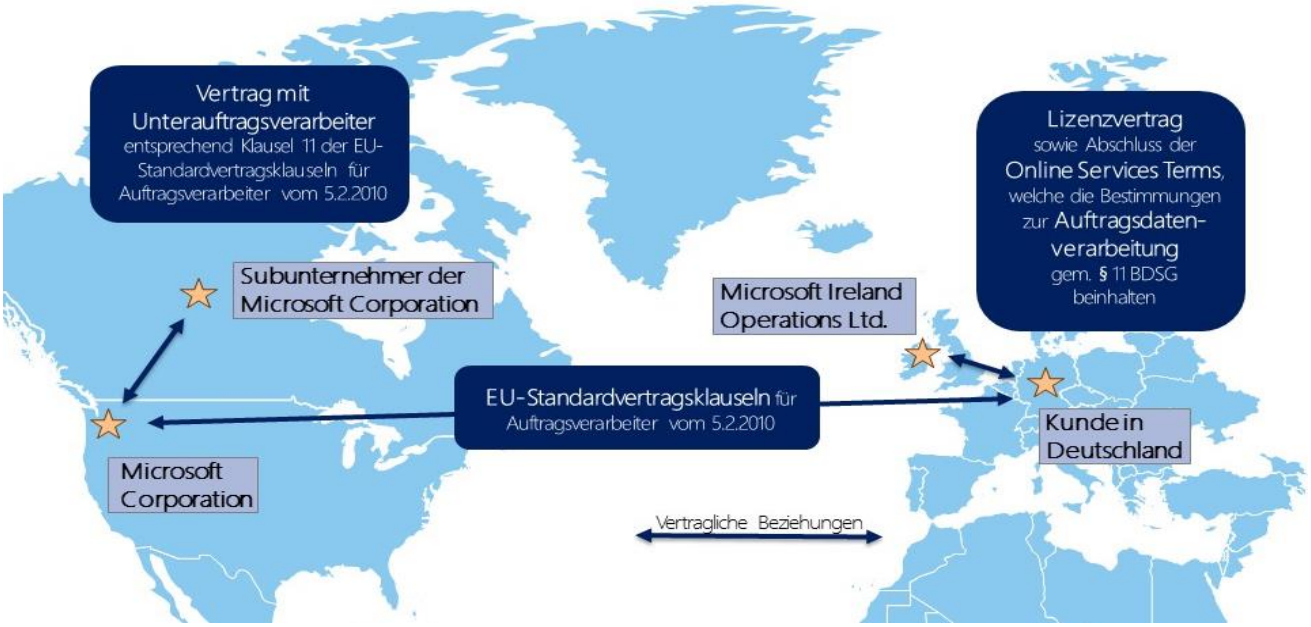
Nein. Rechenzentren in anderen EU-Ländern sind Rechenzentren in Deutschland datenschutzrechtlich gleichgestellt. Datenschutzrechtlich ist es also unerheblich, wo sich ein Rechenzentrum in der EU bzw. im EWR befindet. Dies folgt aus der Waren- und Dienstleistungsfreiheit in der Europäischen Union. Die Dienstleistungsfreiheit ist eine der vier Grundfreiheiten des Europäischen Binnenmarktes. Sie ermöglicht Anbietern den freien Zugang zu den Dienstleistungsmärkten aller Mitgliedstaaten der EU. Ein Rechenzentrum in Deutschland ist datenschutzrechtlich demnach nicht vorteilhafter als ein Rechenzentrum in einem anderen Mitgliedsstaat der EU. Für den Teil der Enterprise Cloud Services Office 365, Dynamics 365, Azure Core Services, Windows Intune, die Microsoft von außerhalb der EU erbringt, bietet Microsoft seinen Kunden die EU-Standardvertragsklauseln an. Diese begründen hierfür nach verbindlicher Entscheidung der EU-Kommission eine adäquate datenschutzrechtliche Lösung.

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 „Bestimmungen für die Datenverarbeitung" unter anderem die gesetzlich vorgeschriebenen Regelungen für eine Auftragsdatenverarbeitung gemäß § 11 Bundesdatenschutzgesetz (BDSG) bzw. zukünftig des Art. 28 DSGVO.

Grafisch stellt sich das Vertragskonstrukt wie folgt dar:



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 wird sich durch die EU-Datenschutz-Grundverordnung ändern?

Ab dem 25. Mai 2018 wird die EU-Datenschutz-Grundverordnung (nachfolgend: DSGVO) die Datenschutzrichtlinie 95/46/EG aus dem Jahr 1995 ersetzen. 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 wird die DSGVO in allen Mitgliedsstatäten der EU ab dem 25. Mai 2018 direkt gelten.

Zu wichtigen Regelungen der DSGVO gehören unter anderem die erhöhten Anforderungen an die Informationspflichten oder das Recht auf Datenportabilität. Eine in der Praxis wichtige Neuerung aus der DSGVO betrifft auch die Auftragsverarbeitung. Ab Geltung der DSGVO am 25. Mai 2018 erledigt sich der zum aktuellen BDSG geführte Meinungsstreit, ob eine Auftragsverarbeitung bezüglich besonders schützenswerter personenbezogener Daten i.S.d. Art. 9 DSGVO auch bei Auftragnehmern außerhalb der EU möglich ist.

Solche Daten umfassen Angaben über rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gesundheit oder Sexualleben. Derartige Daten dürfen auch dann auf Basis einer Auftragsverarbeitung weitergegeben werden, wenn der Dienstleister außerhalb der EU tätig wird.

Microsoft bietet seinen Kunden seit September 2017 die Online Services Terms mit einer Anlage 4 – Bestimmungen der Datenschutz-Grundverordnung der Europäischen Union und Anhang 1 – Zusätzliche GDPR-Bestimmungen an. Damit bietet Microsoft seinen Kunden jetzt schon diejenigen Regelungen an, die ab dem 25. Mai 2018 nach Art. 28 der DSGVO bei einer sog. Verarbeitung von Daten im Auftrag abzuschließen sind. Dadurch ist gewährleistet, dass die Microsoft Enterprise Services auch ab Mai 2018 rechtskonform eingesetzt werden können.

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

Die 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 Auftragsdatenverarbeitungsvereinbarung und EU-Standardvertragsklauseln unterzeichnen. Diese sind aus Sicht der Datenschutzaufsichtsbehörden die sog. verantwortlichen Stellen, 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. Die Artikel 29-Datenschutzgruppe – ein Abstimmungsgremium aller 28 nationalen Datenschutzaufsichtsbehörden der EU-Mitgliedstaaten (auch sog. Article 29 Working Party genannt, http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/index_en.htm) – 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, http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140402_microsoft.pdf). 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?

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 zertifizierten 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. 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 der in den EU-Rechenzentren gespeicherten Inhaltsdaten von Microsoft verlangen, wird Microsoft hiergegen gerichtlich vorgehen, weil nach Auffassung von Microsoft US-Gesetze nicht für solche Sachverhalte innerhalb der EU gelten.

Dies wurde Microsoft mit Urteil vom 14. Juli 2016 durch den United States Court of Appeals for the Second Circuit bestätigt. In diesem Fall ging es um eine Anfechtungsklage von Microsoft gegen einen Durchsuchungsbeschluss (sog. „search warrant"), der von einem New Yorker Gericht erlassen wurde. Microsoft wurde darin aufgefordert, den E-Mail-Verkehr eines Kunden herauszugeben, der in einem irischen Rechenzentrum von Microsoft gespeichert ist. Dem hat sich Microsoft widersetzt. Durch das Urteil des Court of

Appeals wurde klargestellt, dass der US-Kongress der US-Regierung nicht die Befugnis erteilt hat, unilateral Durchsuchungsbeschlüsse zu erlassen, die über die US-Grenzen hinausreichen. Microsoft hat damit eine wegweisende Entscheidung dafür erstritten, dass das Recht auf Privatsphäre entsprechend der jeweiligen geltenden nationalen Rechtsordnung geschützt wird und geschützt bleibt. Allerdings hat die US Regierung den United States Supreme Court um Überprüfung des Urteils gebeten. Am 16. Oktober 2017 hat der US Supreme Court entschieden, das Urteil des Court of Appeals zu überprüfen. Es wird mit einem Urteil des US Supreme Court vor Juni 2018 gerechnet. Weitere Einzelheiten finden Sie in dem Blogpost von Brad Smith hier: Blog.

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.

Zudem informiert Microsoft halbjährlich über die Anzahl der weltweiten behördlichen Ermittlungsanfragen auf seiner Website. Diese sog. Transparenzberichte finden Sie hier.

Um die Öffentlichkeit von der Sicherheit ihrer Services zu überzeugen, hat Microsoft im Sommer 2015 ein Transparency Center in Brüssel eröffnet. Nunmehr können Regierungsvertreter den Windows-Quellcode sowie die technische Dokumentation einsehen und überprüfen. Zu den Prüfern auf deutscher Seite gehört unter anderem das Bundesamt für Sicherheit in der Informationstechnik, welches das Transparency-Center begrüßt.

Weiteres dazu finden Sie hier: https://blogs.microsoft.com/eupolicy/2015/06/03/microsoft-transparency-center-opens-in-brussels

Können die Microsoft Cloud Services auch von Berufsgeheimnisträgern eingesetzt werden?

Die alte Fassung des § 203 StGB erlaubte den Einsatz externer Dienstleister wie einem Cloud-Anbieter durch Berufsgeheimnisträger – z.B. Ärzte, Anwälte, Steuerberater und Versicherer – nur unter engen Voraussetzungen. Ein Verstoß kann mit Geld- oder Freiheitsstrafe geahndet werden.

Der Bundestag und der Bundesrat haben einer Strafrechtsreform zugestimmt. Die Gesetzesverkündung wird täglich erwartet. Der neue § 203 StGB erlaubt die Offenlegung der Berufsgeheimnisträgern 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 mehr erforderlich.

Damit ist der Weg für unterstützende IT-Dienstleistungen, wie die Bereitstellung und den Support von IT-Systemen und Anwendungen, geebnet, und auch eine Cloudnutzung wird für die eingangs genannten Personengruppen einfacher möglich.

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 Auftragsdatenverarbeitung 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 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.

Microsoft bietet Microsoft Azure, Microsoft Office 365 und jüngst auch Microsoft Dynamics 365 in der Microsoft Cloud Deutschland an. Welche technischen und rechtlichen Änderungen bedeutet das für die Kunden gegenüber der europäischen Cloud?
Sofern Kunden – aus welchen Gründen auch immer – Bedenken wegen der Speicherung in EU-Rechenzentren haben, können sie auch die Microsoft Cloud Technologie aus deutschen Rechenzentren beziehen. Dort agiert T-Systems als Datentreuhänderin im Auftrag des Kunden, muss jeden einzelnen Zugriff von Dritten auf die Daten freigeben und kann den Zugriff bei Missbrauch jederzeit unterbrechen. Sofern ein spezialisierter Microsoft-Mitarbeiter aus den USA zu Supportzwecken einen Incident bearbeiten soll, ist dies nur möglich, wenn T-Systems ihn freischaltet. Dadurch wird unabhängig von dem oben genannten Grundsatzurteil des Court of Appeals for the Second Circuit die Sicherheit weiter erhöht, dass Microsoft gegenüber US-Behörden nicht zur Herausgabe von Kundendaten verpflichtet ist.

Einrichtungen des Bundes, die schützenswerte Informationen (z.B. Betriebs- und Geschäftsgeheimnisse oder sensible Informationen über IT-Infrastrukturen des Bundes) verarbeiten, können in Übereinstimmung mit der Empfehlung des Rates der IT-Beauftragten der Bundesressorts (Beschluss 2015/5) damit auch die Microsoft Technologie in einer deutschen Cloud nutzen.

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
  http://www.microsoft.com/en-us/trustcenter
- Office 365 Trust Center
  http://trust.office365.de
- Microsoft Azure Trust Center
  http://azure.microsoft.com/de-de/support/trust-center
- Dynamics Trust Center
  http://www.microsoft.com/de-de/dynamics/crm-trust-center.aspx
- Transparenzberichte
  http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency

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