Microsoft

Microsoft Cloud Compendium

Fragen und Antworten

Compliance in der Microsoft Enterprise Cloud

Stand: April 2016

Compliance in der Microsoft Enterprise Cloud

Veröffentlicht von Microsoft Schweiz GmbH
Stand April 2016

Wo werden Daten in der Microsoft Enterprise Cloud gespeichert?

Für schweizerische Kunden werden standardmässig die wesentlichen Kundendaten (Core Customer Data) der Microsoft Enterprise Services (Office 365, Microsoft Azure, CRM Online, Windows Intune) in den Microsoft Rechenzentren in Dublin und Amsterdam 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. Weitere Informationen finden Sie hier: http://aka.ms/dataflowmap.

Die Anforderungen zur Bereitstellung der Dienste können im Einzelfall beinhalten, dass einige Daten Mitarbeitern bzw. Zulieferern von Microsoft ausserhalb der primären Speicherregion zugänglich gemacht werden. Darüber hinaus kann es vorkommen, dass sich die Mitarbeiter mit der meisten technischen Erfahrung für die Behandlung spezieller Dienstprobleme an anderen Standorten als am primären Standort befinden, und sie ggf. Zugriff auf Systeme oder Daten benötigen, um das Problem lösen zu können.

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

Kunden dürfen Personendaten 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. Auftragsdatenbearbeitung die Microsoft in seinen Verträgen abgebildet hat (siehe dazu nachstehend).

Das Datenschutzrecht gilt dabei nur für die Bearbeitung von Personendaten. Dies sind – verkürzt gesagt – Angaben, die sich auf eine bestimmte oder bestimmbare natürliche oder juristische Person beziehen, wie beispielsweise Name/Firma einer Person oder deren E-Mail-Adresse. In der Praxis finden sich zumeist eine Vielzahl von Personendaten in der Microsoft Enterprise Cloud. Es gibt aber auch Fälle, in denen kaum oder keine Personendaten bearbeitet werden, beispielsweise wenn Designdaten eines Modeherstellers in Azure gespeichert werden.

Microsoft hat derzeit kein schweizerisches Rechenzentrum. Kann ein schweizerischer Kunde trotzdem datenschutzkonform Microsoft Enterprise Cloud Services nutzen?

Ja. Rechenzentren in EU-Ländern sind Rechenzentren in der Schweiz datenschutzrechtlich gleichgestellt, da diese Länder ein angemessenes Datenschutzniveau gewährleisten. Datenschutzrechtlich ist es also unerheblich, ob sich ein Rechenzentrum in der Schweiz oder der EU befindet. Ein Rechenzentrum in der Schweiz ist datenschutzrechtlich demnach nicht vorteilhafter als ein Rechenzentrum in der EU. Für den Teil der Services, die Microsoft von ausserhalb der EU erbringt, bietet Microsoft seinen Kunden die EU-Standardvertragsklauseln an. Diese begründen nach Ansicht des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (nachfolgend EDÖB) hierfür eine adäquate datenschutzrechtliche Lösung.

Auf welcher rechtlichen Grundlage verarbeitet Microsoft Personendaten in ihren Enterprise Cloud Services?

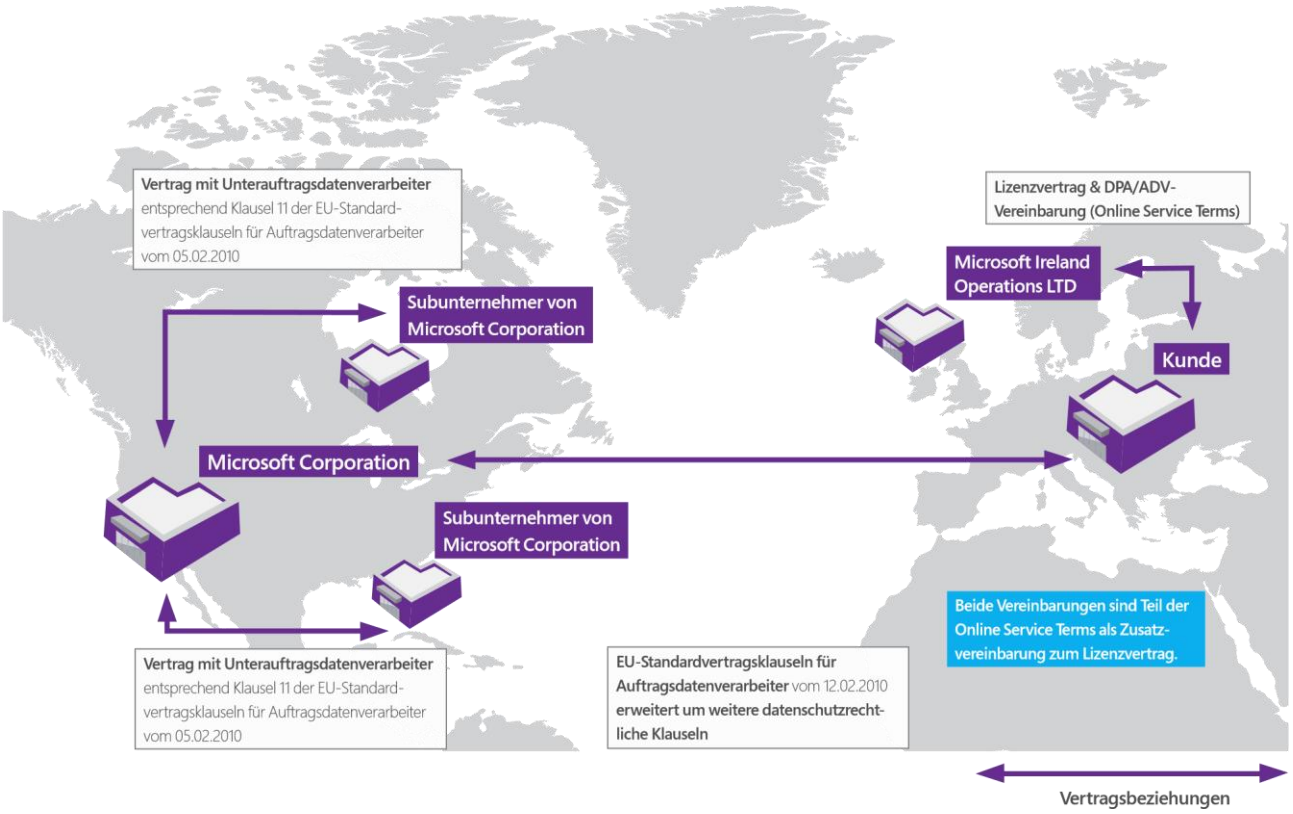
Grundlage für die Leistungsbeziehung sind die Lizenzverträge über die Nutzung der jeweiligen Microsoft-Technologie. Diese werden zwischen dem Kunden und der Microsoft Ireland Operations Limited (nachfolgend MIOL) abgeschlossen. Die Lizenzverträge werden durch die Online Services Terms (OST) ergänzt (aktuelle Fassung unter http://aka.ms/Wkcowi). Diese Bestimmungen beinhalten im Abschnitt „Bestimmungen für die Datenbearbeitung" unter anderem die gesetzlich vorgeschriebenen Regelungen für eine Auftragsdatenbearbeitung (gemäss Art. 10a des Bundesgesetzes über den Datenschutz vom 19. Juni 1992 (nachfolgend DSG)).

Die Online Services Terms beinhalten als Anhang 3 die EU-Standardvertragsklauseln, die zwischen dem Kunden und der Microsoft Corporation abgeschlossen werden.

Die EU-Standardvertragsklauseln sind von der EU-Kommission verabschiedet worden und werden auch vom EDÖB anerkannt. Zusätzlich hat Microsoft dem EDÖB die Online Services Terms (OST) zur Prüfung vorgelegt und er hat diese als hinreichende vertragliche Garantien für den Datentransfer ins Ausland (i.S.V. Art. 6 Abs. 2 lit. a DSG) anerkannt.

Werden diese Klauseln unverändert eingesetzt, ist eine Weitergabe von Personendaten insbesondere in die USA datenschutzrechtlich zulässig. Damit ist die Microsoft Corporation verpflichtet, die EU-Datenschutzstandards einzuhalten und diese auch etwaigen Subunternehmern vertraglich aufzuerlegen.

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 Services können weiterhin von einer zentralen Konzerngesellschaft, beispielsweise der IT-Dienstleistungsgesellschaft des Konzerns, bezogen werden. Der Lizenzvertrag wird zwischen dieser Konzerngesellschaft und MIOL abgeschlossen.

Welchen Inhalt haben die Vertragsbeziehungen, wenn Unternehmen eine Microsoft-Plattform wie Microsoft Azure nutzen 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 insofern in seinen Vertragsbedingungen keine weitergehenden Leistungspflichten verspricht als er mit Microsoft vereinbart hat.

Sind die Enterprise Cloud-Verträge von Microsoft mit den Datenschutzaufsichtsbehörden abgestimmt?
Da Microsoft bei der Weitergabe von Personendaten in Drittstaaten ausserhalb der Schweiz und der EU die EU-Standardvertragsklauseln einsetzt, ist ein angemessenes Datenschutzniveau stets gegeben. Der Kunde muss allerdings den EDÖB über den Einsatz solcher EU-Standardvertragsklauseln in allgemeiner Weise informieren.

Welche Rolle spielt die Safe Harbor Zertifizierung der Microsoft Corporation für schweizerische Kunden?
Am 6. Oktober 2015 hat der Europäische Gerichtshof für die EU die EU-US Safe Harbor Zertifizierung für ungültig erklärt, wodurch für eine datenschutzkonforme Übermittlung von Personendaten in die USA kein angemessenes Datenschutzniveau mehr vorliegt. Der EDÖB hat sich dieser Ansicht sinngemäss angeschlossen. Aus diesem Grund stützt sich Microsoft bei der Weitergabe von Personendaten in Drittstaaten ausserhalb der Schweiz und der EU auf die EU-Standardvertragsklauseln ab.

Können US-Behörden, wie die National Security Agency (NSA), auf die Daten der Kunden in der Microsoft Cloud zugreifen?

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 Rechenzentren in der EU gespeicherten Inhaltsdaten verlangen, wird Microsoft hiergegen gerichtlich vorgehen, weil die US-Gesetze nach Auffassung von Microsoft nicht für solche Sachverhalte ausserhalb der USA gelten. Microsoft hat in diesen Zusammenhang ein Anfechtungsverfahren gegen die von einem erst-instanzlichen New Yorker Gericht angeordnete Herausgabe von Daten, die in der EU gespeichert sind, initiiert. Dieses Urteil wurde zwar in der zweiten Instanz bestätigt, so dass Microsoft zur Herausgabe der Daten verpflichtet gewesen wäre. Allerdings wurde Microsoft ein Aufschub gewährt. Microsoft hat zudem angekündigt, sämtliche Rechtsmittel auszuschöpfen, da diese Herausgabe von Daten nicht rechtmässig sei. Nähere Einzelheiten hierzu finden Sie hier:

http://blogs.microsoft.com/on-the-issues/2015/04/09/our-legal-challenge-to-a-us-government-search-warrant/ (englisch)

http://blogs.technet.com/b/microsoft_presse/archive/2014/06/16/microsoft-wehrt-sich-gegen-die-herausgabe-von-kundendaten.aspx (deutsch)

http://digitalconstitution.com/ (englisch)

Bis zur Erstellung dieses Dokuments gab es im Übrigen noch nie den Fall, dass die NSA von Microsoft die Herausgabe von Daten von schweizerischen Unternehmenskunden verlangt hat.

Als Reaktion auf die Berichte über Zugriffe auf Datenleitungen durch Behörden verschiedener Länder übermittelt Microsoft im Übrigen Daten zwischen seinen Rechenzentren nunmehr ausschliesslich verschlüsselt.

Können sog. sensitive Daten (wie beispielsweise Gesundheitsdaten) verarbeitet werden?

Ja. Besonders schützenswerte Personendaten (umgangssprachlich «sensitive Daten» genannt) sind gemäss Art. 3 lit. c DSG Daten über die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten, die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit, Massnahmen der sozialen Hilfe, oder administrative oder strafrechtliche Verfolgungen und Sanktionen. Diese unterliegen einem besonderen Schutz und dürfen grundsätzlich nur mit Einwilligung der betroffenen Person bearbeitet und weitergegeben oder auf Basis einer Auftragsdaten-bearbeitung weitergegeben werden. Dies gilt auch, wenn der Dienstleister ausserhalb der EU tätig wird. Denn das DSG macht – ungeachtet der Tatsache, dass beim Dienstleister ein angemessenes Datenschutzniveau bestehen muss – bei einer Auftragsdatenbearbeitung keinen Unterschied zwischen den Anforderungen für die Beauftragung von Dienstleistern in der Schweiz und der EU und ausserhalb der Schweiz und der EU. Allerdings müssen neben einer Auftragsdatenbearbeitungs-vereinbarung, für die Weitergabe von Personendaten in Drittstaaten ausserhalb der Schweiz und der EU auch entsprechende vertragliche Garantien für ein angemessenes Datenschutzniveau vorliegen. Microsoft verwendet hierzu die vom EDÖB anerkannten EU-Standardvertragsklauseln für Auftragsdatenbearbeiter.

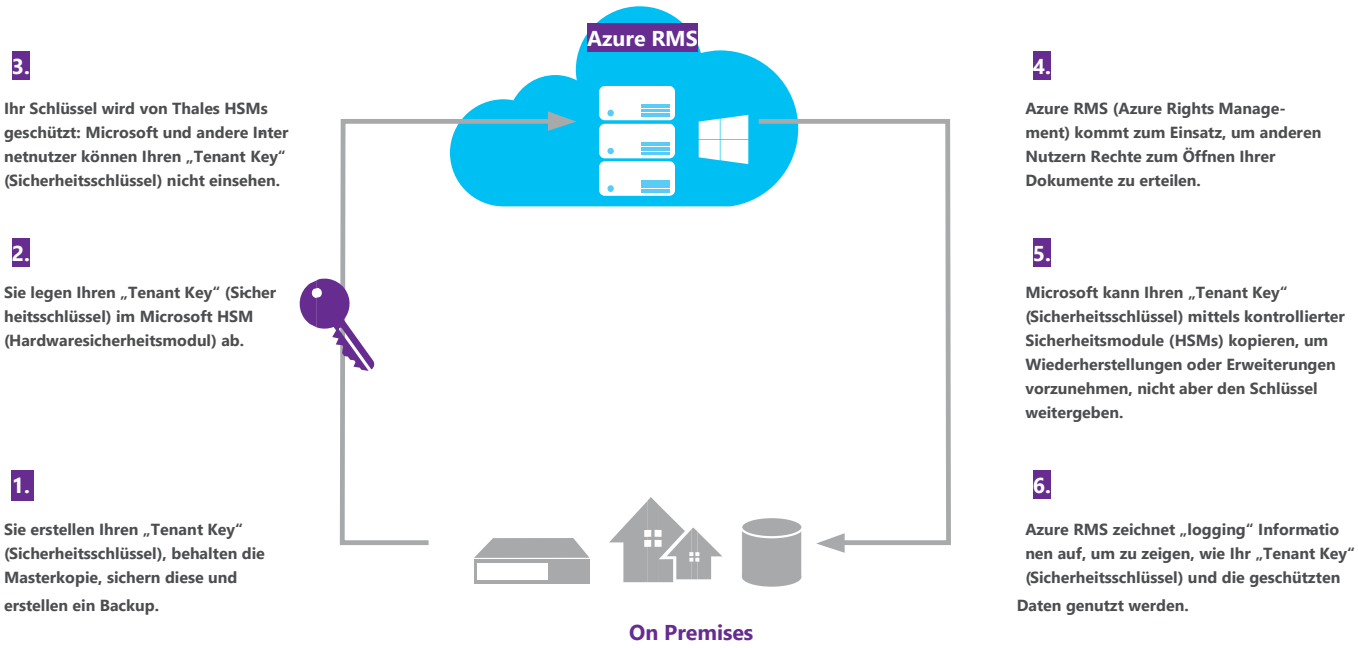
Kann die Anwendbarkeit des Datenschutzrechts durch Verschlüsselung ausgeschlossen werden?

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, fehlt es bereits an der Übermittlung von Personendaten. Microsoft bietet seinen Kunden hierzu an, ihren eigenen Schlüssel für die Verschlüsselung von Daten in Windows Azure Rights Management zu verwenden. Dabei wird der Schlüssel durch ein Hardware-Sicherheitsmodul (HSM) des Herstellers Thales geschützt, so dass Microsoftden 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.

Grafisch stellt sich der Schutz bei der Verwendung des eigenen Schlüssels des Kunden wie auf der folgenden Seite dar:

Der ISO/IEC 27018-Standard, eine Erweiterung des oben



Grafische Darstellung des Schutzmechanismus bei der Verwendung eines eigenen Kundenschlüssels

Wie können Kunden ihrer Pflicht nachkommen, sich von der Einhaltung aller technischen und organisatorischen Massnahmen gemäss DSG zu überzeugen?

Kunden sind bei einer Auftragsdatenbearbeitung datenschutzrechtlich verpflichtet, sich von der Umsetzung der vereinbarten und gesetzlichen technischen und organisatorischen Massnahmen zum Schutz der Personendaten zu überzeugen. Kunden können dieser Pflicht im Allgemeinen 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 ISO27001-Standard. Dies ist einer der besten globalen Sicherheitsvergleichs-Benchmarks. Microsoft stellt seinen Kunden auf deren Aufforderung hin eine Zusammenfassung des Überprüfungsberichts nach ISO 27001 zur Verfügung.

Microsoft übernimmt aktuell als erster führenden Anbieter von Cloud-Diensten den internationalen ISO/IEC 27018 Standard für Datenschutz in der Cloud.

genannten ISO27001-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 Personendaten zu schützen.

Das British Standards Institution (BSI) hat nun von unabhängiger Seite überprüft, dass Microsoft Azure, Office 365 und Dynamics CRM Online mit den „Codes of Practice“ des Standards zum Schutz von Personendaten (Personally Identifiable Information, PII) in Public Clouds entsprechen. Zudem wurde dieser Test für Microsoft Intune vom Bureau Veritas durchgeführt.

Diese Überprüfungen werden in den Microsoft Online Services Terms (OST) vertraglich vereinbart (für den ISO/IEC27018-Standard ab April 2015), ändern aber nicht die Rechte aus den EU-Standardvertragsklauseln ab.

http://blogs.microsoft.com/on-the-issues/2015/02/16/microsoft-adopts-first-international-cloud-privacy-standard/ (englisch)

Wie kann der Kunde seine Daten revisionssicher aufbewahren?
Microsoft speichert die Daten georedundant an mehreren Stellen in zwei 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 und die nachfolgenden Ausführungen erheben daher keinen Anspruch auf Vollständigkeit.

In der Praxis können beispielsweise sektorspezifische Anforderungen wie im Finanzdienstleistungs- oder im Gesundheitsbereich einschlägig sein. Insbesondere sind in diesen Bereichen allfällige gesetzliche Geheimhaltungspflichten zu beachten. Jedoch weder das Amts-/Berufsgeheimnis noch die verschiedenen Spezialgeheimnisse (z.B. Bankkundengeheimnis oder im Sozialversicherungs- und Krankenversicherungsbereich die Schweigepflicht) stehen grundsätzlich einer Auslagerung in die Cloud entgegen. Allerdings ist der Kunde dafür verantwortlich die notwendigen detaillierten gesetzlichen und regulatorischen Voraussetzungen für die Auslagerung in die Cloud in seinem Sektor zu evaluieren, berücksichtigen und hat für deren Einhaltung zu sorgen.

Im Finanzdienstleistungsbereich hat die Eidgenössische Finanzmarktaufsicht (nachfolgend FINMA) in einem Rundschreiben Grundsätze für das Outsourcing von Geschäftsbereichen festgelegt, wozu beispielsweise auch die Auslagerung der Datenaufbewahrung zählt. Insbesondere beim Outsourcing ins Ausland muss stets sichergestellt werden, dass die banken- und börsengesetzliche Prüfgesellschaft des Kunden sowie die FINMA ihre Prüfrechte wahrnehmen können. Auch je nach Geheimhaltungspflichten des Kunden müssen unterschiedliche Voraussetzungen erfüllt werden. Microsoft hat verschiedene Lösungen, wie beispielsweise die bereits oben beschriebene Verschlüsselung, um die Geheimhaltungspflichten des Kunden berücksichtigen zu können.

Ähnliches gilt auch im Versicherungsbereich, für welchen ebenfalls eine gesetzliche Schweigepflicht zu beachten ist. In den Verträgen mit Microsoft werden daher die Verschwiegenheitspflichten auf die Mitarbeitenden von Microsoft ausgeweitet, so dass gepaart mit anderen Vertragsbestandteilen (wie den EU-Standardvertragsklauseln) ein datenschutzrechtskonformes Auslagern der Daten möglich ist. Darüber hinaus kann der Kunde auch die Daten so verschlüsseln, dass nur der Kunde Zugriff auf diese hat.

Im Gesundheitsbereich ist es aus datenschutzrechtlicher Sicht möglich Gesundheitsdaten in die Cloud auszulagern. Allerdings sind in diesem Bereich spezifische Geheimhaltungspflichten wie das Amts- und Berufsgeheimnis zu berücksichtigen und abhängig von den gesetzlichen Vorschriften können unterschiedliche Lösungen angebracht sein. Microsoft bietet die Möglichkeit Patientendaten so zu verschlüsseln, dass nur der Kunde Zugriff auf diese hat und somit keine gegen die gesetzliche Geheimhaltungspflichten und gegen das Datenschutzgesetz verstossende Bekanntgabe erfolgt.

Grundsätzlich können nach den allgemeinen handels- und steuerrechtlichen Grundsätzen zur Buchführung Geschäftsbücher und Buchungsbelege auch elektronisch aufbewahrt werden. Die Ausnahme bilden in diesem Zusammenhang lediglich der Geschäftsbericht und der Revisionsbericht, welche schriftlich und unterzeichnet aufbewahrt werden müssen. Im Übrigen vertritt die Eidgenössische Steuerverwaltung die Ansicht, dass mehrwertsteuerrelevante Dokumente zwar in elektronischer Form aufbewahrt werden können, dann aber mit einer elektronischen Signatur signiert werden müssen.

Weitere aktuelle Informationen finden Sie hier:

- Microsoft Trustcenter für alle Dienste (englisch)
  https://www.microsoft.com/en-us/TrustCenter/default.aspx
- Office 365 Trustcenter
  http://trust.office365.de
- Microsoft Azure Trustcenter
  http://azure.microsoft.com/de-de/support/trust-center/
- Dynamics Trust Center
  https://www.microsoft.com/de-ch/dynamics/crm-trust-center.aspx
- Häufig gestellte Fragen zu den Standardvertragsklauseln der EU
  http://office.microsoft.com/de-de/business/redir/ FX104033856.aspx
- Transparenzberichte (englisch)
  http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/
- Microsoft's Challenge to U.S. Search Warrant / NSA (englisch)
  http://blogs.technet.com/b/microsoft_on_the_issues/archihttp://blogs.technet.com/b/microsoft_on_the_issues/archive/2014/04/25/one-step-on-the-path-to-challenging-search-warrant-jurisdiction.aspxve/2014/04/25/one-step-on-the-path-to-challenging-sehttp://blogs.technet.com/b/microsoft_on_the_issues/archive/2014/04/25/one-step-on-the-path-to-challenging-search-warrant-jurisdiction.aspxarch-warrant-jurisdiction.aspx

  http://blogs.microsoft.com/on-the-issues/2014/06/04/unfihttp://blogs.microsoft.com/on-the-issues/2014/06/04/unfinished-business-on-government-surveillance-reform/nished-business-on-government-surveillance-reform/

  http://blogs.microsoft.com/blog/2014/12/15/business-media-civil-society-speak-key-privacy-case/

Diese Übersicht erhebt keinen Anspruch auf Vollständigkeit. Sie stellt keine Rechts- oder Steuerberatung dar.

Bildquelle: eigene, shutterstock_78032764, bartzuza