Microsoft

Microsoft Cloud Compendium
Fragen und Antworten

Compliance in der Microsoft Enterprise Cloud

Veröffentlicht von Microsoft Corporate, External and Legal Affairs (CELA) Deutschland
Stand: Januar 2016

Compliance in der Microsoft Enterprise Cloud

Veröffentlicht von Microsoft Corporate, External and Legal Affairs (CELA), Deutschland
Stand: Januar 2016

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, CRM Online und Windows Intune („data at rest"). Für deutsche Kunden werden daher standardmäßig die wesentlichen Kundendaten („Core Customer Data") der Microsoft Enterprise Services (Office 365, CRM Online 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 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 hat angekündigt, in Kürze Cloud Services aus Rechenzentren in Deutschland anzubieten. Heißt das, dass ein deutscher Kunde Microsoft Enterprise Cloud Services außerhalb Deutschlands nicht mehr datenschutzkonform nutzen kann?

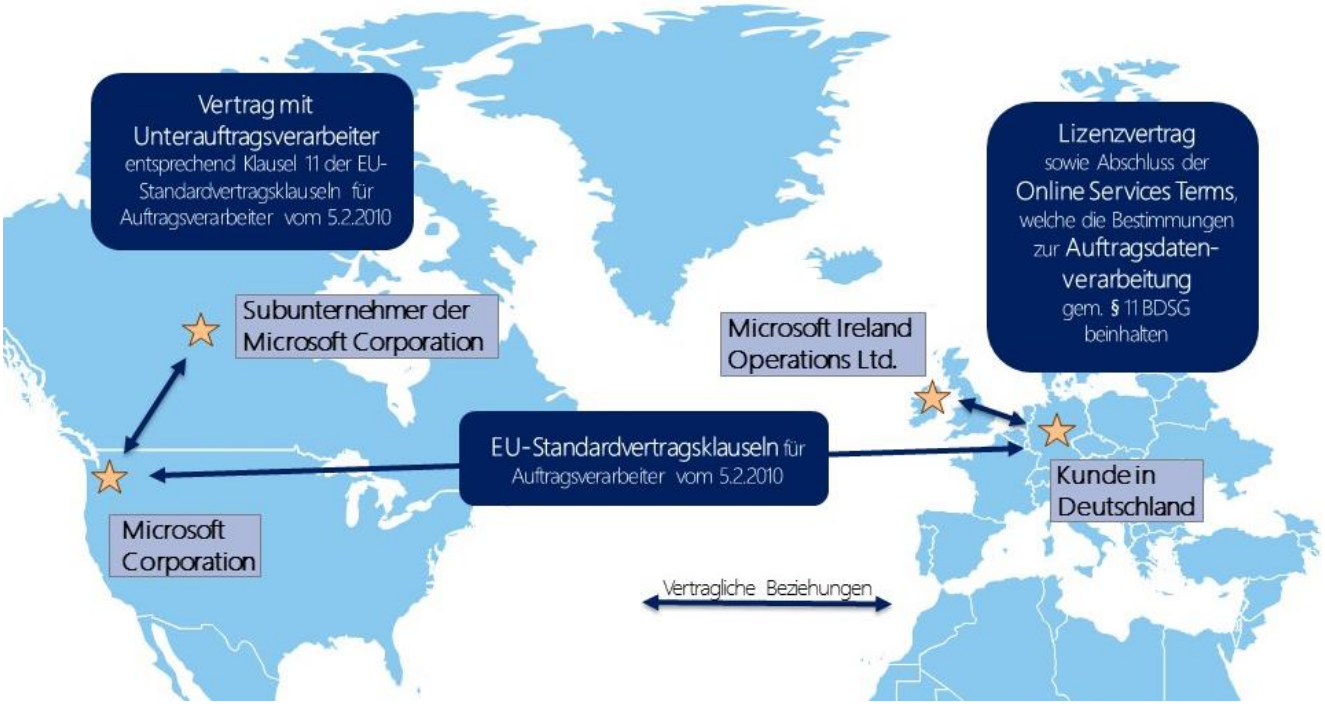
Nein. Rechenzentren in anderen EU-Ländern sind Rechenzentren in Deutschland datenschutzrechtlich gleichgestellt. Datenschutzrechtlich ist es also unerheblich, wo sich ein Rechenzentrum in der EU bzw. im EWR befindet. Dies folgt aus der Waren- und Dienstleistungsfreiheit in der Europäischen Union. Die 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, CRM Online, 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 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 Bestimmungen beinhalten auf Seite 10 im Abschnitt „Bestimmungen für die Datenverarbeitung" unter anderem die gesetzlich vorgeschriebenen Regelungen für eine Auftragsdatenverarbeitung (gemäß § 11 Bundesdatenschutzgesetz (BDSG) bzw. den jeweiligen Landesdatenschutzvorschriften: auch Auftragsdatenverarbeitungsvereinbarung (ADV-Vereinbarung oder Data Processing Agreement (DPA)) genannt.

Die Online Services Terms beinhalten 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.

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. Auftragsdatenverarbeitungsvereinbarung und EU-Standardvertragsklauseln sollten auf Kundenseite alle nutzenden Konzerngesellschaften 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 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?
Ja. Die Artikel 29-Datenschutzgruppe (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). Die Artikel 29 Datenschutzgruppe ist ein Abstimmungsgremium aller 28 nationalen Datenschutzaufsichtsbehörden der EU-Mitgliedstaaten. Sie hat damit festgestellt, dass das Microsoft-Vertragswerk alle Inhalte aufweist, die für eine weisungsgebundene Beauftragung von Dienstleistern außerhalb der EU erforderlich sind. Microsoft ist der erste große Cloud Anbieter, der eine solche Bestätigung der EU-Datenschutzaufsicht erhalten hat. 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.

Welchen Einfluss hat das Urteil des Europäischen Gerichtshofs (EuGH) vom 6. Oktober 2015 zu Safe Harbor auf die Microsoft Cloud Services?
Für die Microsoft Enterprise Services Office 365, Microsoft Azure Core Services, CRM Online und Windows Intune hat das Urteil keine Auswirkung. Der EuGH hat nur das Safe Harbor-Abkommen für ungültig erklärt. Damit ist ein US-Datentransfer nicht per se unzulässig, sondern bleibt aufgrund anderer Rechtsgrundlagen weiterhin möglich. Der EuGH hat festgestellt, dass nur er allein die Kompetenz besitzt, Rechtsakte der Unionsorgane für nichtig oder ungültig zu erklären. Ein solcher, weiterhin verbindlicher Rechtsakt für den Transfer von personenbezogenen Daten an Empfänger außerhalb der EU sind die EU-Standardvertragsklauseln, auf die Microsoft den Datentransfer in den vorgenannten Enterprise Cloud Services stützt. Seit dem 1. Januar 2016 bietet Microsoft auch für Yammer die Standardvertragsklauseln an.

Bedarf der Einsatz der Microsoft Cloud nach dem Safe Harbor-Urteil des EuGH nunmehr der Genehmigung durch die Datenschutzaufsichtsbehörden?
Nein. Zwar hat der Düsseldorfer Kreis, das Abstimmungsgremium der Datenschutzbeauftragten des Bundes und der Länder in Deutschland, am 26. Oktober 2015 erklärt, für sog. Binding Corporate Rules und individualisierte Datenexportverträge ab sofort keine neuen Genehmigungen für Datentransfers in die USA mehr zu erteilen. Microsoft ist mit seinen Enterprise Cloud Services hiervon jedoch nicht betroffen, weil es die Cloud Services weder auf Basis von Binding Corporate Rules noch auf Basis individualisierter Datenexportverträge erbringt, sondern auf Basis der EU-Standardvertragsklauseln.

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 verlangen, wird Microsoft hiergegen gerichtlich vorgehen, weil die US-Gesetze nach Auffassung von Microsoft nicht für solche Sachverhalte innerhalb der EU gelten. Microsoft hat in diesem Zusammenhang ein Anfechtungsverfahren gegen die von einem New Yorker Gericht angeordnete Herausgabe von Daten, die in der EU gespeichert sind, initiiert. Das Verfahren ist zur Zeit vor dem US Second Circuit Court of Appeals anhängig. Mit einem Urteil wird in Kürze gerechnet. Microsoft wurde bezüglich der Herausgabe gerichtlich ein Aufschub gewährt, so dass Microsoft die Daten bislang nicht herausgeben musste. Nähere Einzelheiten hierzu finden Sie hier:

http://blogs.technet.com/b/microsoft_on_the_issues/archive/2014/04/25/one-step-on-the-path-to-challenging-search-warrant-jurisdiction.aspx

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

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

Bis zur Erstellung dieses Dokuments gab es im Übrigen noch nie den Fall, dass Microsoft die Daten von deutschen Unternehmenskunden herausgeben musste.

Als Reaktion auf die Berichte über Zugriffe auf Datenleitungen durch Geheimdienste verschiedener Länder übermittelt Microsoft im Übrigen Daten zwischen seinen Rechenzentren nunmehr ausschließlich verschlüsselt. Microsoft hat Ende 2014 auch die Verschlüsselung der Daten auf seinen Servern bei einzelnen Enterprise Cloud Services eingeführt.

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.

https://blogs.microsoft.com/eupolicy/2015/06/03/microsoft-transparency-center-opens-in-brussels/

Können sog. sensitive Daten (wie beispielsweise

Gesundheitsdaten) verarbeitet werden?
Ja. Sensitive Daten sind gemäß § 3 Absatz 9 BDSG Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. Diese unterliegen einem besonderen Schutz und dürfen grundsätzlich nur mit Einwilligung des Betroffenen oder auf Basis einer Auftragsdaten-verarbeitung weitergegeben werden. Dies gilt entgegen anderer Meinungen auch, wenn der Dienstleister außerhalb der EU tätig wird. Denn die europäische Datenschutzrichtlinie macht – ungeachtet der Tatsache, dass beim Dienstleister ein angemessenes Datenschutz-niveau bestehen muss – bei einer Auftragsdaten-verarbeitung keinen Unterschied zwischen den Anforderungen für die Beauftragung von Dienstleistern in der EU und außerhalb der EU. Der deutsche Gesetzgeber darf insofern auch keine strengeren Anforderungen stellen. Der europäische Gerichtshof hat mit Urteil vom 24. November 2011 ausdrücklich entschieden, dass die Mitgliedsstaaten keine Regelungen erlassen dürfen, die die Maßgaben der Datenschutzrichtlinie über- oder unterschreiten. Schließlich sieht die EU-Kommission ja auch gerade in den EU-Standardvertragsklauseln für Auftragsdatenverarbeiter die Möglichkeit der Verarbeitung sensitiver Daten vor. Dass deutsches Recht nicht strenger als europäisches Datenschutzrecht sein darf, hat auch der Bundesgerichtshof in einem Urteil vom 4. Juni 2013 bereits wiederholt.

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 personenbezogener Daten. 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 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 Datenschutz-recht 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 CRM Online 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 wird ab der zweiten Jahreshälfte 2016 die Microsoft Dienste Azure, Office 365 sowie Dynamics CRM Online aus einem deutschen Rechenzentrum anbieten. Was bedeutet das für die Kunden?

Sofern Kunden – aus welchen Gründen auch immer – Bedenken wegen der Speicherung in EU-Rechenzentren haben, können sie ab Herbst 2016 auch die Microsoft Cloud Technologie aus einem deutschen Rechenzentrum 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 Ausgang des vorstehend genannten US-Gerichtsverfahrens 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, gültig seit dem 1. Januar 2015, ersetzt die GoBS sowie die GDPdU). 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

- Häufig gestellte Fragen zu den Standardvertragsklauseln der EU
  http://office.microsoft.com/de-de/business/redir/FX104033856.aspx

- Transparenzberichte
  http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/

- Die deutsche Microsoft Rechtsabteilung veranstaltet in regelmäßigen Abständen Cloud Workshops mit einem Schwerpunkt auf rechtlichen Themen. Weitere Informationen hierzu, insbesondere zu den nächsten Terminen, finden Sie unter folgender Internetadresse: **www.mscloudevent.de.**