Microsoft

Microsoft Cloud Compendium

Fragen und Antworten

Compliance in der Microsoft Enterprise Cloud

Veröffentlicht von Microsoft Legal and Corporate Affairs (LCA) Deutschland
Stand: Februar 2015

Compliance in der Microsoft Enterprise Cloud

Veröffentlicht von Microsoft Legal and Corporate Affairs (LCA) Deutschland
Stand: Februar 2015

Wo werden Daten in der Microsoft Enterprise Cloud gespeichert?

Für deutsche 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 personenbezogene Daten 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 vor allem keine personenbezogenen Daten verarbeitet werden, beispielsweise wenn Designdaten eines Modeherstellers in Azure gespeichert werden.

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

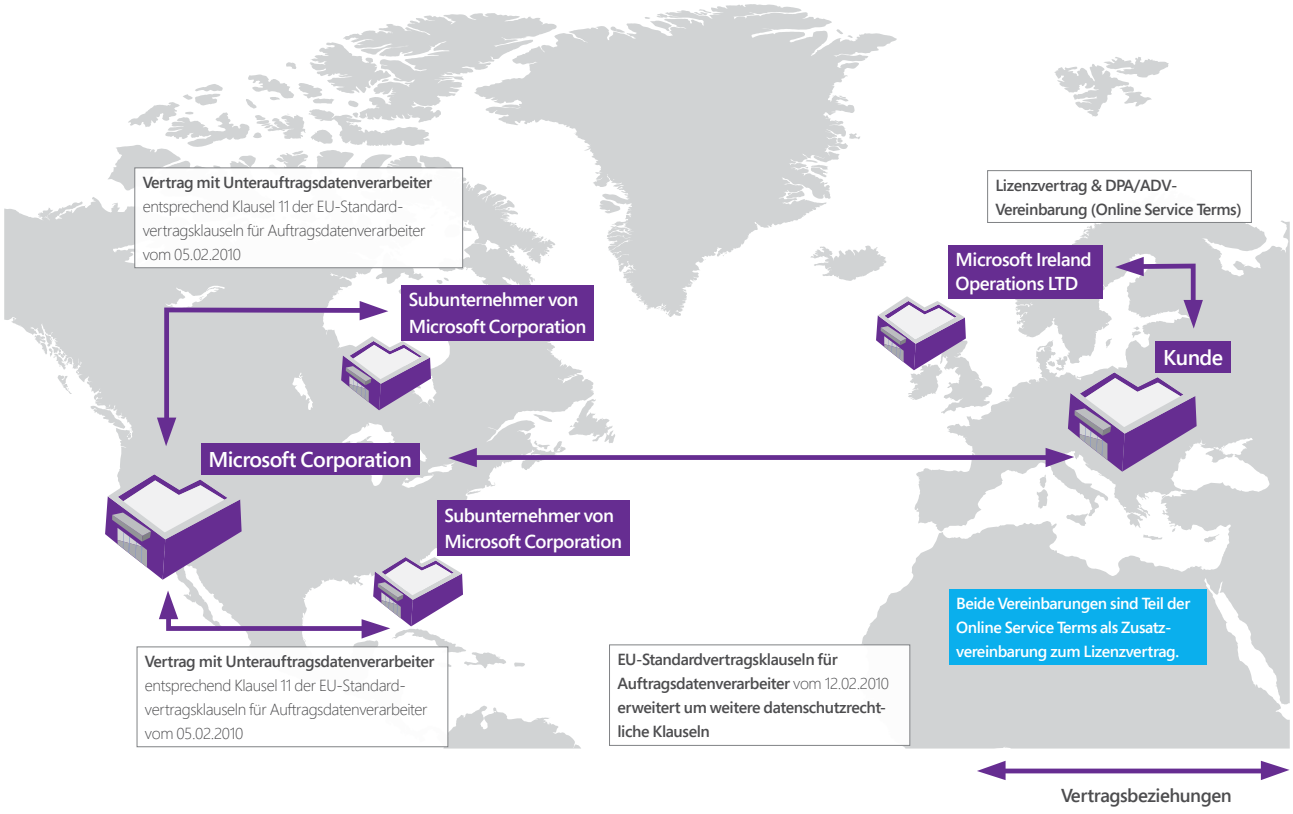
Ja. Rechenzentren in anderen EU-Ländern sind Rechenzentren in Deutschland datenschutzrechtlich gleichgestellt. Datenschutzrechtlich ist es also unerheblich, wo sich ein Rechenzentrum in der EU befindet. Dies folgt aus der Waren- und Dienstleistungsfreiheit in der Europäischen Union. Die Dienstleistungsfreiheit ist eine der vier Grundfreiheiten des Europäischen Binnenmarktes. Sie ermöglicht Anbietern den freien Zugang zu den Dienstleistungsmärkten aller Mitgliedsstaaten der Europäischen Union. Ein Rechenzentrum in Deutschland ist datenschutzrechtlich demnach nicht vorteilhafter als ein Rechenzentrum in einem anderen Mitgliedsstaat 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 verbindlicher Entscheidung der EU-Kommission hierfür eine adäquate datenschutzrechtliche Lösung.

Auf welcher rechtlichen Grundlage verarbeitet Microsoft personenbezogene Daten 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 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 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, die 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 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, http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/index_en.htm) ist ein Abstimmungsgremium aller 28 nationalen Datenschutzaufsichtsbehörden der EU-Mitgliedstaaten. Diese 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 hat damit festgestellt, dass das Vertragswerk alle Inhalte aufweist, die für eine weisungsgebundene Beauftragung von Dienstleistern außerhalb der EU erforderlich sind. Microsoft ist derzeit der einzige 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.

Die letzte Änderung, die Microsoft mit der Artikel 29-Datenschutzgruppe abgestimmt hat, ist in die Microsoft-Standardverträge zum 1.7.2014 aufgenommen worden. Altverträge können aktualisiert werden.

Welche Rolle spielt vor dem Hintergrund dieser Bestätigung noch die Safe Harbor Zertifizierung der Microsoft Corporation für deutsche Kunden?
Es gibt weiterhin Enterprise Cloud Services, für die die EU-Standardvertragsklauseln noch nicht gelten (z.B. Yammer). Für diese Services ist die Safe Harbor Zertifizierung weiterhin von Bedeutung. Die EU-Kommission hat festgestellt, dass Unternehmen, die sich den Safe Harbor Regime unterwerfen, ein angemessenes Datenschutzniveau bieten und dass personenbezogene Daten an diese Unternehmen übermittelt werden dürfen.

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 EU-Rechenzentren gespeicherten Inhaltsdaten verlangen, wird Microsoft hiergegen gerichtlich vorgehen, weil die US-Gesetze nach Auffassung von Microsoft nicht für solche Sachverhalte außerhalb der EU gelten. Microsoft hat in diesem Zusammenhang ein Anfechtungsverfahren gegen die von einem erstinstanzlichen 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.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 die NSA von Microsoft die Herausgabe von Daten von deutschen 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?

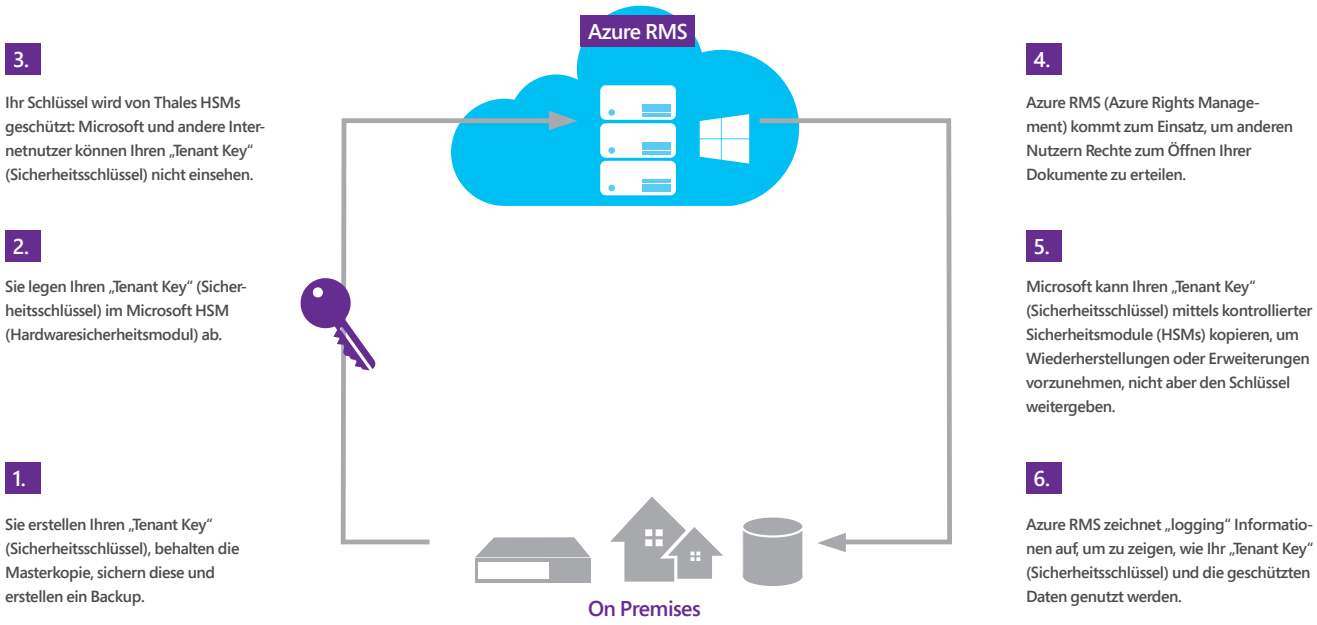
Ja. Sensitive Daten sind gemäß § 3 Absatz 9 BDSG Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. Diese unterliegen einem besonderen Schutz und dürfen grundsätzlich nur mit Einwilligung des Betroffenen oder auf Basis einer Auftragsdatenverarbeitung 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 Datenschutzniveau bestehen muss – bei einer Auftragsdatenverarbeitung keinen Unterschied zwischen den Anforderungen für die Beauftragung von Dienstleistern in der EU und außerhalb der EU. Der deutsche Gesetzgeber darf unseres Erachtens insofern auch keine strengeren Anforderungen stellen. Insoweit hat auch der Europäische Gerichtshof 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, die Microsoft in sein Vertragswerk standardmäßig integriert hat.

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 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:



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 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 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.

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.

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 personenbezogenen Daten (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/IEC 27018-Standard ab 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 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. In der Praxis können beispielsweise sektorspezifische Anforderungen wie im Finanzdienstleistungsbereich einschlägig sein. Nach den allgemeinen handels- und steuerrechtlichen Grundsätzen zur Buchführung bedarf es insbe-

sondere der Einhaltung einer ordnungsgemäßen Behandlung elektronischer Dokumente (GoBS). 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 der Microsoft Enterprise Cloud speichert, muss er sich dies außerdem vom zuständigen Finanzamt genehmigen lassen.

Weitere aktuelle Informationen finden Sie hier:

- Office 365 Trustcenter
  http://trust.office365.de

- Microsoft Azure Trustcenter
  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