Ihr Cloudaufgaben-Heft

Datenschutz in der Cloud

Erfahren Sie, worauf es beim Datenschutz in der Cloud ankommt

Microsoft Dynamics

Inhalt

Cloud Services nutzen und zum Klassenprimus werden

Überlegen Sie gerade, eine Customer Relationship Management (CRM)-Lösung in Ihrem Unternehmen einzuführen und setzen dabei auf Cloud Computing? Sicherlich: CRM-Lösungen als Cloud Dienste bieten nicht nur modernste Technologien für Datenspeicherung, -verarbeitung und Kommunikation, sie erhöhen auch die Flexibilität der Geschäftsprozesse im Kundenmanagement. Auslastungsspitzen lassen sich leichter abfangen und auf die relevanten Daten kann von unterwegs aus zugegriffen werden. Damit ist schließlich eine verbesserte Produktivität verbunden. Und gerade Cloud-basierte Lösungen leisten noch mehr: IT-Kapazitäten, damit verbundene Service- und Wartungstätigkeiten und auch die Kosten für die IT-Infrastruktur können deutlich reduziert werden.

Kurz: Cloud Lösungen bieten Ihrem Unternehmen viele Vorteile. Ganz sorglos sollte man diese aber nicht nutzen. Denn wenn es um Cloud Computing geht, ist „Datenschutz" Pflichtfach – und das kann schnell kompliziert werden.

„Beim Cloud Computing erweist sich das Thema Datenschutz als einer der wichtigsten Faktoren, um überhaupt neue Services zu nutzen."

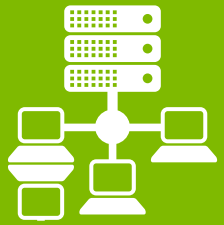
Hans-Jürgen Rose,
Leiter des Geschäftsbereichs
Microsoft Dynamics
Business Solutions,
Microsoft Deutschland GmbH

Wer sich nicht auskennt, kassiert im „Datenschutz“ schlechte Noten

Wenn es um das Fach Cloud Computing geht, melden sich besonders in Deutschland viele zum Thema Datenschutz und äußern ihre Fragen. Verständlich, denn bei der Speicherung und Verarbeitung von Nutzer- und Kundendaten in der Cloud – und damit meist in externen Rechenzentren – werden Datenschutz und Datensicherheit zu heiklen Themen.

Die wichtigste Frage lautet: Wer trägt die Verantwortung, wenn Kunden- und Unternehmensdaten in Speicher- und Analysesystemen zusammenlaufen, die nicht in Ihrem Unternehmen stehen, wenn Daten also einem Dritten anvertraut werden? Es geht dabei schließlich um sensible Kundeninformationen und -daten, die vor Missbrauch geschützt werden müssen.

Daher ist es für Unternehmen unabdingbar, sich mit dem Thema Datenschutz zu befassen. Nur was genau gilt es zu beachten und wie können Sie sich hier absichern?



„Für RWE ist Cloud Computing eine strategische Säule bei der Optimierung der Konzern-IT. Das Thema Datenschutz hat in diesem Kontext zentrale Bedeutung und bei unseren Cloud-Projekten hohe Priorität.“

Uwe Lachermund, Leiter IT Infrastructure, RWE IT GmbH

Rechtliche Vorgaben für die Speicherung sensibler Kunden-daten in der Cloud

Erste Adresse für Nachhilfe in Sachen Datenschutz und Cloud Computing ist der „Arbeitskreis Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder". Die Verantwortlichen haben sich intensiv mit der Nutzung personenbezogener Daten in der Cloud auseinandergesetzt und einen Leitfaden entwickelt, der auf die verschiedenen Anforderungen, die von Cloudkunden und Cloudanbietern umgesetzt werden müssen, eingeht.

Zu den zentralen Empfehlungen des Arbeitskreises zählen:

- Bei Clouds, die sich außerhalb des **Europäischen Wirtschaftsraums** (EWR) erstrecken, ist eine entsprechende Rechtsgrundlage für die Übermittlung personen-bezogener Daten in Drittstaaten erforderlich.
- Bei Kündigung des Cloud Services müssen alle Daten zuverlässig gelöscht werden. Dabei haben Transparenz, Integrität und Compliance-konforme Datenverarbeitung oberste Priorität.

Die vollständigen Empfehlungen des Arbeitskreises Technik und Medien der Konferenz der Datenschutzbeauftrag-ten des Bundes und der Länder finden Sie **über diesen Link**.

Der Arbeitskreis Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder thematisiert auch die Bedeutung der **EU-Standardvertragsklauseln** (auch „EU Model Clauses" genannt). Diese von der Europäischen Kommission vorgegebenen Vertragsklauseln reflektieren die Anforderungen, die mit der **Auftragsdatenverarbeitung** und der Speicherung sensibler Kundendaten in der Cloud verbunden sind.

Die Klauseln ermöglichen einen rechtlich abgesicherten Datentransfer zu Dienstleistern außerhalb der EU und legen genau fest, ob und wann Daten an Dritte weitergegeben werden dürfen, welche Voraussetzungen dafür in allen beteiligten Ländern – und bei den Cloudanbietern – gegeben sein müssen und welche Pflichten Cloudkunden und Dienstleister haben.

Die EU-Standardvertragsklauseln stellen gleichzeitig hohe Anforderungen an die Cloudanbieter. Um diese Klauseln als Standard in das Vertragswerk integrieren zu können, müssen sie bestimmte Auflagen erfüllen: Dazu zählen zum Beispiel ein ausdifferenziertes Auditrecht und die Offenlegung der Subunternehmerverträge, die Sie als Cloudkunde einfordern können.

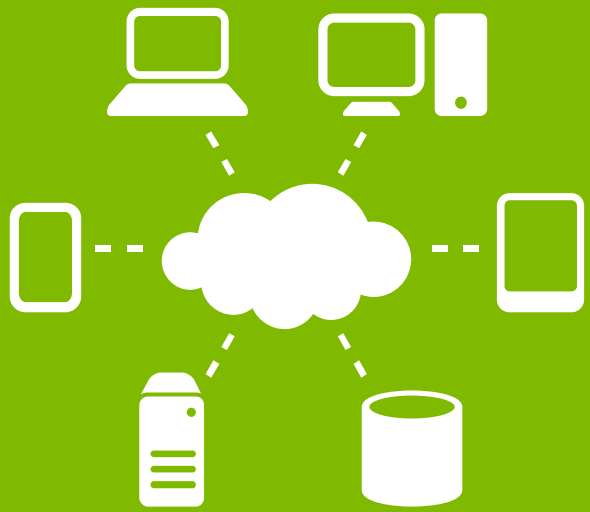
- **Online-Portal für Cloud Security-Themen von Fraunhofer AISEC: http://www.cloud-competence-center.com/home/**
- **Cloud Computing powered by BITKOM: http://www.cloud-practice.de**
- **Cloud-Aktionsprogramm des BMWI: http://www.bmwi.de/go/trusted-cloud**
- **Cloud Computing Grundlagen vom Bundesamt für Sicherheit in der Informationstechnik: https://www.bsi.bund.de/DE/Themen/CloudComputing/Grundlagen/Grundlagen_node.html**

Aber wer ist denn nun für den Schutz von Daten in der Cloud verantwortlich?

Generell gilt: Für die Einhaltung der gesetzlichen Bestimmungen hinsichtlich der Nutzung personenbezogener Daten ist derjenige in der Pflicht, der diese Daten erhebt und verarbeitet. Oder anders formuliert: Wenn Sie einen Cloud Service nutzen möchten, sind Sie dafür verantwortlich, was mit den Daten geschieht (wer darauf zugreift, wie sie genutzt werden, etc.). Sie können dafür auch haftbar gemacht werden.

Wer also keinen Strafaufsatz schreiben möchte, müsste sich als Cloudkunde theoretisch sogar beim Anbieter vor Ort von der Einhaltung der technischen und organisatorischen Maßnahmen überzeugen. Dies gilt sowohl vor Beginn als auch regelmäßig während der Auftragsdatenverarbeitung (ADV). In der Praxis ist dies natürlich kaum machbar. Dennoch liegt es letztlich in der Verantwortung des Cloudkunden, zu prüfen, ob der Cloudanbieter regelkonform und rechtssicher Daten verarbeitet. Und das kann ganz schön aufwändig sein.

Weitere Informationen zu den EU-Standardvertragsklauseln finden Sie **hier**.



Microsoft engagiert sich in Sachen Datenschutz

Wir haben schon mal vorgearbeitet und unterstützen Anwender und Kunden umfassend beim Thema Datenschutz in der Cloud: Microsoft übernimmt hier eine Vorreiterrolle, indem wir freiwillig die EU-Standardvertragsklauseln in unser Vertragswerk integriert haben. **Diese sogenannten EU Model Clauses** stehen für „Microsoft Business Dynamics CRM Online" zur Verfügung und gelten ebenfalls für Office 365. Voraussetzung dafür waren umfassende Audits und Zertifizierungen.

Doch mit unserem Angebot, die EU Model Clauses zu berücksichtigen, hört die Datenschutzinitiative bei Microsoft nicht auf: Um unsere Kunden umfassend über die Datenschutzmaßnahmen in Bezug auf unsere Cloudanwendungen zu informieren, haben wir das **Trust Center** eingerichtet. Dort finden Sie umfassend Hilfestellung zum Thema Datenschutz.

Das Trust Center bietet Ihnen eine zentrale Plattform mit allen relevanten Dokumenten und Informationen, die Sie benötigen, um sich über den Schutz Ihrer Daten, die in der Microsoft-Cloud gespeichert sind, zu informieren. Wir sorgen dadurch für mehr Transparenz und Sie haben die Möglichkeit, unterschiedliche Cloud-Produkte im Hinblick auf die Maßnahmen für Datenschutz und -sicherheit besser vergleichen zu können.

Datenschutz ist für uns mehr als ein reines Pflichtfach

Microsoft ist sich seiner Verantwortung bewusst und stellt sich den Herausforderungen, die mit dem Thema Datenschutz in der Cloud verbunden sind. Unseren Kunden bieten wir eine umfassende Vertragsstruktur für den Schutz ihrer Daten im Einklang mit den EU-Richtlinien.

Microsoft ist bisher einer der wenigen Service-Provider weltweit, der sich mit der Einbeziehung der **EU-Standardvertragsklauseln** seinen Kunden und Anwendern gegenüber verpflichtet hat. Sie ergänzen das **Safe Harbor-Abkommen** und gewährleisten eine pragmatische und rechtlich abgesicherte Umsetzung von deutschen und europäischen Datenschutzvorgaben. Darüber hinaus sorgt die **Auftragsdatenverarbeitungserklärung** (ADV/DPA) für Transparenz und Compliance-konformen Umgang bei der Verarbeitung der Kundendaten.

Und auch unsere anderen Cloud Services zeichnen sich durch umfassende und weitgehende Sicherheit aus. Derzeit erarbeiten wir eine einheitliche Regelung für unser gesamtes Cloud-basiertes Lösungsportfolio. Auf diese Weise erfüllen wir unsere **Corporate Technical Responsibility** (CTR). CTR bedeutet für uns die freiwillige Verpflichtung, Verantwortung für gesellschaftliche, wirtschaftliche und politische Veränderungen zu übernehmen, die durch unsere technischen Innovationen angestoßen werden.

Die wichtigsten Fragen und Antworten zum Thema Datenschutz

Bei Ihren Cloudaufgaben sind Sie wahrscheinlich schon häufiger über die Stichwörter „Safe Harbor-Abkommen" und „PATRIOT Act" gestolpert. Wenn Sie sich genauer darüber informieren möchten, welche Anforderungen und Konzepte für den Datenschutz damit verbunden sind, bieten Ihnen unsere FAQs dazu umfassend Gelegenheit:

Was hat es mit dem Safe Harbor-Abkommen auf sich?
Das **Safe Harbor-Abkommen** ist eine Datenschutzvereinbarung zwischen der EU und den USA. Ohne dieses Abkommen wäre es laut der Datenschutzrichtlinie 95/46/EG grundsätzlich verboten, personenbezogene Daten aus EG-Mitgliedsstaaten in Staaten zu übertragen, die über kein dem EG-Recht vergleichbares Datenschutzniveau verfügen. Dies trifft auch auf die USA zu. Im Jahr 2000 hat die EU anerkannt, dass bei den Unternehmen, die dem Safe Harbor-System beigetreten sind, ausreichende Datenschutzmaßnahmen bestehen. **Microsoft hat bereits 2001 dieses Abkommen unterzeichnet.**

Was bedeutet das Safe Harbor-Abkommen für meine Kundendaten, die in der Microsoft-Cloud gespeichert sind?
Als amerikanisches Unternehmen ist Microsoft dem Safe Harbor-Abkommen bereits 2001 beigetreten, um einen rechtlich abgesicherten Datentransfer zu ermöglichen. Wir haben uns damit frühzeitig den Anforderungen an den Datenschutz verpflichtet. Seit mehr als zehn Jahren garantieren wir darüber hinaus durch unsere **Trustworthy Computing-Initiative** unseren Kunden und Anwendern die weiterreichende Sicherheit und Verlässlichkeit.

Was ist mit dem PATRIOT Act? Sind meine Kundendaten davon betroffen?
Der USA PATRIOT Act ist ein US-Bundesgesetz, das 2001 im Zuge des Krieges gegen den Terrorismus verabschiedet wurde. Wichtig: Der **PATRIOT Act** schafft keinesfalls eine rechtsfreie Zone, in der US-Behörden beliebig Zugriff auf Daten von Unternehmen und Privatanwendern haben. Wann und unter welchen Bedingungen amerikanische Behörden auf sensible Daten zugreifen dürfen, ist juristisch genauestens definiert, stark reglementiert und damit sehr eingeschränkt.

Wie sicher sind die Microsoft-Rechenzentren und nach welchen ISO-Normen sind sie standardisiert?
Microsoft hat mehrere Milliarden US-Dollar in seine Rechenzentren investiert – hier auch gezielt in die Sicherheitsinfrastruktur und Sicherheitsmaßnahmen. Unsere Rechenzentren sind nach verschiedenen international geltenden Standards und Normen zertifiziert, z. B. nach der wichtigen ISO-/IEC-Norm 27001:2005, SAS 70 Type II, FISMA und PCI (ausführliche Informationen dazu finden Sie über diesen **Link**).

Cloudaufgaben – Glossar

SAFE HARBOR
Safe Harbor (englisch für „Sicherer Hafen") bezeichnet die Datenschutz-Vereinbarung zwischen den USA und der Europäischen Union. Die USA haben damit seit 2000 ein Reglement für die Übermittlung personenbezogener Daten aus den EU-Staaten in die USA geschaffen.

Hintergrund dafür ist, dass die Datenschutzrichtlinie der EU-Kommission (95/46/EC) es grundsätzlich verbietet, personenbezogene Daten aus EU-Mitgliedsstaaten in Staaten zu übertragen, die über kein dem EU-Recht vergleichbares Datenschutzniveau verfügen. Das ist beispielsweise in den USA der Fall, in denen es kaum allgemein verbindliche, rechtliche Vorschriften gibt, um insbesondere den Umgang mit persönlichen Nutzerdaten zu definieren oder zu regeln.

US-Unternehmen, die sich unter dem Safe Harbor Framework öffentlich zertifizieren, verpflichten sich die Safe Harbor-Prinzipien und die dazugehörenden, verbindlichen Hinweise zu weiteren Frequently Asked Questions (FAQ) einzuhalten. Auf dieser Grundlage erkennt die EU an, dass bei diesen Unternehmen ein ausreichendes, dem EU-Recht vergleichbares Schutzniveau besteht.

AUFTRAGSDATENVERARBEITUNG (ADV) (siehe: DatenschutzWiki)
Auftragsdatenverarbeitung im Sinne des Bundesdatenschutzgesetzes (BDSG), ist die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten durch einen Dienstleister im Auftrag der verantwortlichen Stelle. § 11 BDSG beschreibt im Detail, welche Rechte, Pflichten und Maßnahmen im Einzelnen durch einen Vertrag zwischen Auftraggeber (verantwortliche Stelle) und Auftragnehmer (Dienstleister) zu treffen sind.

Beispiele zur Auftragsdatenverarbeitung: Die Beauftragung eines Callcenters zur Kundenkommunikation oder auch die Ablage von personenbezogenen Daten auf extern gehosteten Servern.

EU MODEL CLAUSES
Die EU-Standardvertragsklauseln sind von der Europäischen Kommission vorgegebene Vertragsklauseln, die den Datentransfer zwischen Unternehmen innerhalb und außerhalb der Europäischen Union zum Gegenstand haben. Die verbindliche Vereinbarung dieser Klauseln ist ein weiterer Baustein eines zulässigen Datentransfers in Nicht-EU-Länder. Diese Vertragsklauseln stellen hohe Anforderungen an Anbieter Cloud-basierter Lösungen, dazu zählt beispielsweise auch ein sehr ausdifferenziertes Auditrecht oder die Offenlegung der Subunternehmerverträge.

Ergänzend zum Safe Harbor Abkommen stellt Microsoft mit den EU Model Clauses ein weiteres Standardvertragswerk für seine Cloud-Kunden zur Verfügung. Der Vorteil liegt in der Einfachheit des Prozesses, denn mit der Einführung der EU Standardvertragsklauseln-ADV-Konstruktion erfüllt Microsoft die Empfehlungen, wie sie vom „Arbeitskreis Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder" zur Nutzung von Cloud Services in der Orientierungshilfe „Cloud Computing" veröffentlicht worden sind.

PATRIOT ACT
Der USA PATRIOT Act (Apronym für Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, dt. etwa: „Gesetz zur Stärkung und Einigung Amerikas durch Bereitstellung geeigneter Instrumente, um Terrorismus aufzuhalten und zu blockieren") ist ein amerikanisches Bundesgesetz, das seit dem 25. Oktober 2001 in Kraft ist, als direkte Reaktion auf die Terroranschläge am 11. September 2001.

ISO/IEC 27001
ISO/IEC 27001 ist eine internationale Norm, die den Prozess und Verlauf, nach dem Informationssicherheitsmanagementsysteme implementiert, betrieben, geprüft, verwaltet und verbessert werden müssen, beschreibt und definiert. Cloud-Anbieter, deren Rechenzentren nach dieser ISO-Norm zertifiziert sind, gewährleisten einen hohen Sicherheitsstandard und belegen, dass sie sowohl die gesetzlichen Anforderungen als auch Anforderungen der Kunden an ein Informationssicherheitsmanagement umfassend erfüllen.

TRUST CENTER
Das Trust Center ist für Microsoft-Kunden das zentrale Portal für sämtliche Informationen rund um die Themen Datensicherheit und Compliance. Damit stellt das Unternehmen sicher, dass seine Kunden schnell und einfach alle Dokumente finden, die sie benötigen, um sich über Datensicherheit und Compliance zu informieren.