Cloud Computing rechtskonform einkaufen und verkaufen.

Klaus Foitzick
Vorstand
activeMind AG

Fragen

- Was müssen Unternehmen wissen, wenn sie Aufträge für Cloud-Services vergeben?
- Welche Anforderungen müssen Cloud-Anbieter sicherstellen?
- Was bringen welche Zertifizierungen für Anbieter und Kunden?
- Erkaufen sich die Kunden das Mehr an Effizienz und Flexibilität durch einen Verlust an Informations- und Datenschutz?

Ein paar Grundlagen vorab…

Das Datenschutzrecht schützt Menschen

- Datenschutzgesetze sind nur bei Daten von Menschen zu beachten
  (z.B. Kontaktdaten und diesen zugeordnete Daten von Mitarbeitern, Lieferanten und Kunden)

- Daten von Menschen dürfen nur mit Erlaubnis verarbeitet werden
  Daten von Menschen dürfen nur verarbeitet werden, wenn ein Gesetz dies erlaubt oder der Betroffene eingewilligt hat.

Ist Cloud Computing alles was unklar ist?

Cloud-Dienste werden u.a. danach unterschieden, von wem sie angeboten werden.

Public Cloud

- Externer Anbieter (lokal / landesweit / weltweit)

Private Cloud

- Firmeneigenes – meist auf Virtualisierungstechnologie basierendes – Rechenzentrum welches um Sicherheits- und Managementdienste erweitert wurde.

Hybrid Cloud

- Kombination von Public und Private Clouds. Bei einer solchen Cloud werden sowohl die klassischen Rechenzentren eingesetzt, als auch die Skalierbarkeit öffentlicher Clouds genutzt.

Datenweitergabe an einen Dienstleister

Datenweitergabe an einen Dienstleister bedarf einer Rechtsgrundlage
(Public Clouds und Hybrid Clouds)

- Die Rechtsgrundlage leitet sich durch den Auftraggeber ab.
  Ein Vertrag zur Auftragsdatenverarbeitung § 11 BDSG erforderlich.
  (typisch bei IT-Dienstleistern)
- Rechtsgrundlage aus Vertragszweck
  Die Weitergabe an den Dienstleister ist Vertragsgegenstand.
  (typisch bei Vermittlungsgeschäften oder Vertrag mit mehreren Partnern)

Cloud ist auch nichts neues, oder?

- Wird ein Vertrag zur Auftragsdatenverarbeitung abgeschlossen, ist der Cloudanbieter nicht “Dritter”; damit ist keine rechtliche Grundlage für die Weitergabe an ihn erforderlich, sondern die Rechtsgrundlage des Auftraggebers gilt auch für ihn.
- Aber: Auftragsdatenverarbeitung ist nur innerhalb Mitgliedstaat der EU oder innerhalb des Europäischen Wirtschaftsraumes möglich.
- Und: Für Auftragsdatenverarbeitung muss ein vorgeschriebener Vertrag geschlossen werden und eine dokumentierte Erstkontrolle erfolgt.

Pflichten der Geschäftsführung bei einem Cloud-Einsatz

Hier besteht die Gefahr der persönlichen Haftung

- Korrekte Lizenzierung (Nutzung welcher Lizenzen?)
- Ausreichende Datensicherung
- Virenschutz
- Auswertungen von Sicherheitsmeldungen
- Sicherheitsupdates
- Datenschutz, Urheberrechte, Wettbewerbsrecht…

1. Frage

Was müssen Unternehmen wissen, wenn sie Aufträge für Cloud-Services vergeben?

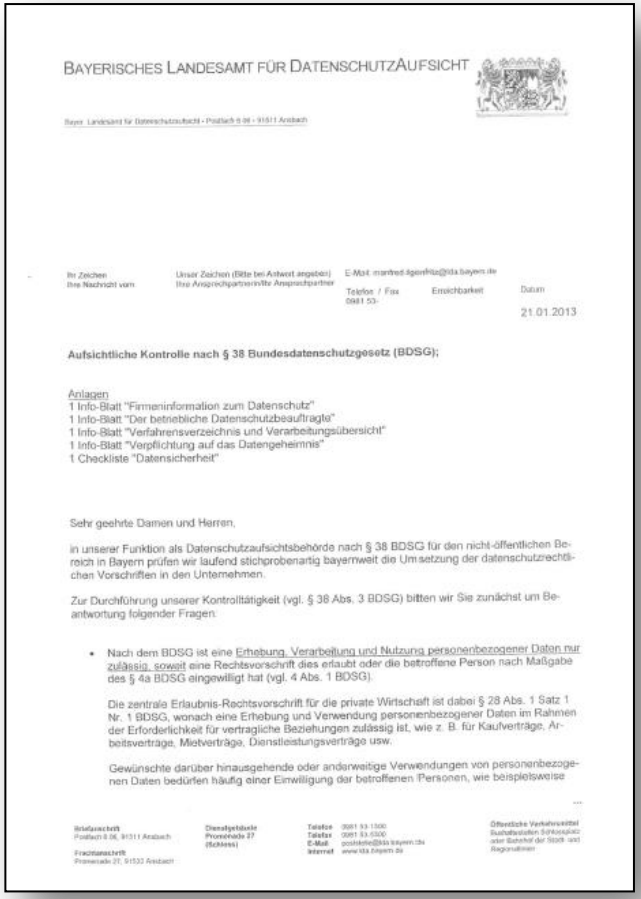
Welche Punkte sind durch <u>Auftraggeber</u> zu beachten?

Der Auftraggeber bleibt für die Verarbeitung der Daten beim Dienstleister verantwortlich

- Schriftlicher Vertrag mit gesetzlich definierten Inhalten
- Anweisung techn. und org. Maßnahmen
  (Zutritt, Zugang, Zugriff, Auftrag, Weitergabe, Eingabe, Auftrag, Verfügbarkeit, Zwecke)
- Erstkontrolle der Einhaltung der Vereinbarungen und deren Dokumentation mit laufender Aktualisierung

http://www.activemind.de/auftragsdatenverarbeitung-vorlage-erstkontrolle

Kontrolle der Auftraggeber durch Aufsichtsbehören



BAYERISCHES LANDESAMT FÜR DATENSCHUTZAUFSICHT

21.01.2013

Aufsichtliche Kontrolle nach § 38 Bundesdatenschutzgesetz (BDSG);

Anlagen
1 Info-Blatt "Firmeninformation zum Datenschutz"
1 Info-Blatt "Der betriebliche Datenschutzbeauftragte"
1 Info-Blatt "Verfahrensverzeichnis und Verarbeitungsübersicht"
1 Info-Blatt "Verpflichtung auf das Datengeheimnis"
1 Checkliste "Datensicherheit"

Sehr geehrte Damen und Herren,

in unserer Funktion als Datenschutzaufsichtsbehörde nach § 38 BDSG für den nicht-öffentlichen Bereich in Bayern prüfen wir laufend stichprobenartig bayernweit die Umsetzung der datenschutzrechtlichen Vorschriften in den Unternehmen.

Zur Durchführung unserer Kontrolltätigkeit (vgl. § 38 Abs. 3 BDSG) bitten wir Sie zunächst um Beantwortung folgender Fragen:

- Nach dem BDSG ist eine Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, soweit eine Rechtsvorschrift dies erlaubt oder die betroffene Person nach Maßgabe des § 4a BDSG eingewilligt hat (vgl. 4 Abs. 1 BDSG).

  Die zentrale Erlaubnis-Rechtsvorschrift für die private Wirtschaft ist dabei § 28 Abs. 1 Satz 1 Nr. 1 BDSG, wonach eine Erhebung und Verwendung personenbezogener Daten im Rahmen der Erforderlichkeit für vertragliche Beziehungen zulässig ist, wie z. B. für Kaufverträge, Arbeitsverträge, Mietverträge, Dienstleistungsverträge usw.

  Gewünschte darüber hinausgehende oder anderweitige Verwendungen von personenbezogenen Daten bedürfen häufig einer Einwilligung der betroffenen Personen, wie beispielsweise

Sehr detaillierte Fragen zu:

- Rechtsgrundlagen für die Verarbeitung
- Datenschutzbeauftragten
  - Bestellung, Zeitaufwand
  - Tätigkeitsberichte
  - Richtlinien
  - Verpflichtung der Mitarbeiter / Doku
- Verfahrensverzeichnis / Vorabkontrolle
- **Auftragsdatenverarbeitung / Verträge**
- Videoüberwachung
- Private Mailnutzung / BYOD / USB
- Technische Maßnahmen / Verschlüsselung / Notfallplan

http://www.activemind.de/landesamt-datenschutz-aufsicht-anlasslose-kontrolle/

2. Frage

Welche Anforderungen müssen Cloud-Anbieter sicherstellen?

Welche Auftragnehmer gibt es im Cloud Umfeld?

- IT-Infrastruktur-Anbieter (IaaS)
- Software-as-a-Service Anbieter (SaaS)
- Plattform-as-a-Service Anbieter mit Kundenbezug (PaaS)
- Systemhäuser, die Installation / Wartung übernehmen
- Programmierer der Lösung, soweit Zugriff auf Livedaten
- Freie Mitarbeiter, der oben genannten

http://www.activemind.de/cloud-computing-und-datenschutz/

Anforderungen an Cloud-Anbieter?

- Angebot innerhalb eines Mitgliedstaates der EU / EWR
- Nachweisbarkeit der Einhaltung der Datenschutzgesetze und Nachweis der technischen Umsetzung
- Qualifizierte Vertriebsmitarbeiter und Betreuer
- Bereitschaft, sich kontrollieren zu lassen
- Transparenz der Verarbeitungen

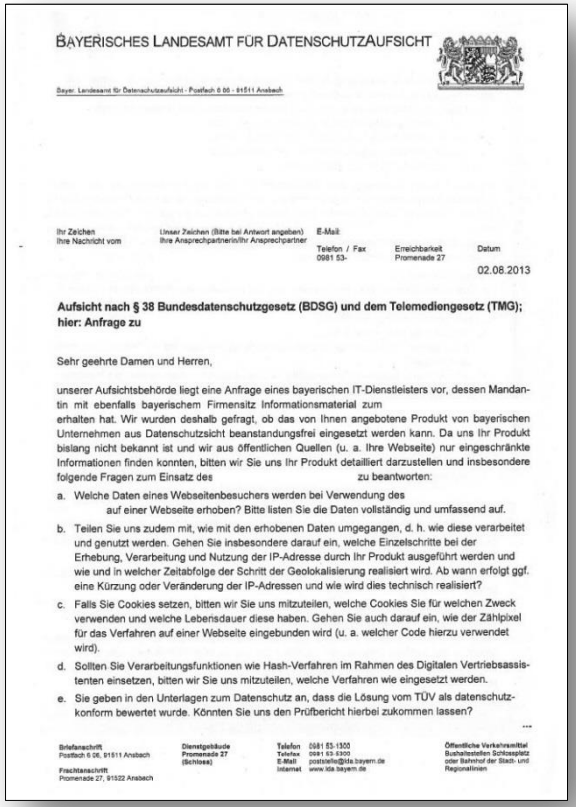
http://www.activemind.de/datenschutzkonzept-muster/

Ein Highlight aus den AGB eines Cloudanbieters

…soweit Daten an uns übermittelt werden, stellt der Kunde Sicherheitskopien her. … Für den Fall eines dennoch auftretenden Datenverlustes ist der Kunde verpflichtet, die betreffenden Datenbestände nochmals unentgeltlich an uns zu übermitteln…

Drum prüfe, wer sich ewig bindet

Kontrolle der Cloud durch Aufsichtsbehören



BAYERISCHES LANDESAMT FÜR DATENSCHUTZAUFSICHT

Bayer. Landesamt für Datenschutzaufsicht - Postfach 6 06 - 91511 Ansbach

Ihr Zeichen
Ihre Nachricht vom

Unser Zeichen (Bitte bei Antwort angeben)
Ihre Ansprechpartnerin/Ihr Ansprechpartner

E-Mail:
Telefon / Fax
0981 53-

Erreichbarkeit
Promenade 27

Datum
02.08.2013

Aufsicht nach § 38 Bundesdatenschutzgesetz (BDSG) und dem Telemediengesetz (TMG); hier: Anfrage zu

Sehr geehrte Damen und Herren,

unserer Aufsichtsbehörde liegt eine Anfrage eines bayerischen IT-Dienstleisters vor, dessen Mandantin mit ebenfalls bayerischem Firmensitz Informationsmaterial zum
erhalten hat. Wir wurden deshalb gefragt, ob das von Ihnen angebotene Produkt von bayerischen Unternehmen aus Datenschutzsicht beanstandungsfrei eingesetzt werden kann. Da uns Ihr Produkt bislang nicht bekannt ist und wir aus öffentlichen Quellen (u. a. Ihre Webseite) nur eingeschränkte Informationen finden konnten, bitten wir Sie uns Ihr Produkt detailliert darzustellen und insbesondere folgende Fragen zum Einsatz des zu beantworten:

a. Welche Daten eines Webseitenbesuchers werden bei Verwendung des auf einer Webseite erhoben? Bitte listen Sie die Daten vollständig und umfassend auf.
b. Teilen Sie uns zudem mit, wie mit den erhobenen Daten umgegangen, d. h. wie diese verarbeitet und genutzt werden. Gehen Sie insbesondere darauf ein, welche Einzelschritte bei der Erhebung, Verarbeitung und Nutzung der IP-Adresse durch Ihr Produkt ausgeführt werden und wie und in welcher Zeitabfolge der Schritt der Geolokalisierung realisiert wird. Ab wann erfolgt ggf. eine Kürzung oder Veränderung der IP-Adressen und wie wird dies technisch realisiert?
c. Falls Sie Cookies setzen, bitten wir Sie uns mitzuteilen, welche Cookies Sie für welchen Zweck verwenden und welche Lebensdauer diese haben. Gehen Sie auch darauf ein, wie der Zählpixel für das Verfahren auf einer Webseite eingebunden wird (u. a. welcher Code hierzu verwendet wird).
d. Sollten Sie Verarbeitungsfunktionen wie Hash-Verfahren im Rahmen des Digitalen Vertriebsassistenten einsetzen, bitten wir Sie uns mitzuteilen, welche Verfahren wie eingesetzt werden.
e. Sie geben in den Unterlagen zum Datenschutz an, dass die Lösung vom TÜV als datenschutzkonform bewertet wurde. Könnten Sie uns den Prüfbericht hierbei zukommen lassen?

...

Briefanschrift
Postfach 6 06, 91511 Ansbach

Dienstgebäude
Promenade 27
(Schloss)

Telefon 0981 53-1300
Telefax 0981 53-5300
E-Mail poststelle@lda.bayern.de
Internet www.lda.bayern.de

Öffentliche Verkehrsmittel
Bushaltestellen Schlossplatz oder Bahnhof der Stadt- und Regionallinien

Frachtanschrift
Promenade 27, 91522 Ansbach

Sehr detaillierte Fragen zu:

- Welche Daten werden erhoben?
- Technische Implementierung
  - Nutzung von Coocies
  - Eingesetzte HASH Verfahren
- Prüfberichte erfolgter externer Audits
- Auskunfts und Widerspruchsmöglichkeiten
- Datenschutzrechtliche Rechtsgrundlagen der Verarbeitung
- Mustervertragstexte
- Bestehende Auftragsdatenverarbeitungen als Auftraggeber

3. Frage

Was bringen welche Zertifizierungen für Anbieter und Kunden?

Eine Zertifizierung ist so wertvoll, wie die Anerkennung der zertifizierenden Stelle.

Ableitung eines international anerkannten Zertifikats

- IAF (weltweite Anerkennung der Zertifizierung)
- EA European co-operation for Accreditation (europäische Anerkennung)
- DAkkS Deutsche Akkreditierungsstelle
- Beispiel einer Zertifizierungsstelle TÜV Hessen

Beispiel Zertifikat der activeMind AG

TÜV PROFI CERT

ZERTIFIKAT

für das Managementsystem nach

DIN EN ISO 9001:2008

Der Nachweis der regelkonformen Anwendung wurde erbracht
und wird gemäß TÜV PROFICERT-Verfahren bescheinigt für

activeMind · AG
Technologie und Management Beratung
Potsdamer Straße 3
D-80802 München

Geltungsbereich

Schulungs-, Beratungs- und Prüfungsleistungen im Bereich
Datenschutz, Qualitätsmanagement und Datensicherheit

Zertifikat-Registrier-Nr. 73 100 4026-7
Auditbericht-Nr. 4252 1279
Zertifikat gültig bis 2015-09-30

IAF
TGA-ZM-05-07-00

TÜV HESSEN

Darmstadt, 2012-10-01
Zertifizierungsstelle des TÜV Hessen
Der Zertifizierungsstellenleiter

SEITE 1/2. Nur gültig in Verbindung mit dem Hauptzertifikat.
Diese Zertifizierung wurde gemäß TÜV PROFICERT-Verfahren durchgeführt und wird regelmäßig überwacht.
Die aktuelle Gültigkeit ist nachprüfbar unter www.tuev-club.de. Originalzertifikate enthalten ein aufgeklebtes Hologramm.
TÜV Technische Überwachung Hessen GmbH, Rüdesheimerstr. 119, D-64285 Darmstadt, Tel. +49 6151/600311

- Norm
- Geltungsbereich
  Wichtig! Prüfen!

- Akkreditierung
- Zertifizierungsstelle

Zertifizierungen für Cloudanbieter

- **ISO/IEC 27001:2013**
  Durch die Zertifizierung wird der Nachweis erbracht, dass das zertifizierte Unternehmen ein Informationssicherheitsmanagement betreibt.
  - Kein Nachweis der Umsetzung konkreter technischer Anforderungen.
  - Rechtskonforme Leistungserbringung wird nicht geprüft.
- Angesehene Norm, die eine gute Aussage über das bestehende Managementsystem gibt. Wird von Aufsichtsbehörden oft als ausreichender Nachweis der techn. und org. Maßnahmen angesehen.
- Derzeit ca. 800 in Deutschland zertifiziert, ca. 17.000 weltweit

Zertifizierungen für Cloudanbieter


Deutsches IT-Sicherheitszertifikat

BSI-IGZ-0143-2013

ISO 27001-Zertifikat auf der Basis von IT-Grundschutz

Betrieb der Leistungen: Virtual Server, Security as a Service, Datacenter, MPLS VPN Internet Access

der Global Access Internet Services GmbH

gültig bis: 5. März 2016

- **ISO 27001 auf Basis IT-Grundschutz**
  Durch die Zertifizierung wird der Nachweis erbracht, dass das zertifizierte Unternehmen ein Informationssicherheitsmanagement betreibt und die technischen Anforderungen der IT-Grundschutzkataloge einhält.
  - Nachweis der Umsetzung konkreter technischer Anforderungen
  - Rechtskonforme Leistungserbringung wird nicht geprüft.
- In Deutschland sehr angesehene Norm, die eine sehr gute Aussage über das bestehende Managementsystem und die technische Umsetzung gibt. Wird von Aufsichtsbehörden immer als ausreichender Nachweis der techn. und org. Maßnahmen angesehen.
- Derzeit „weltweit“ 63 zertifiziert

Andere „Zertifizierungen“

- Selbstverpflichtung **Safe Harbor**
  US-Unternehmen können dem Safe Harbor beitreten und sich auf der entsprechenden Liste des US-Handelsministeriums eintragen lassen, wenn sie sich verpflichten, die Safe Harbor Principles und die dazugehörenden – verbindlichen – Frequently Asked Questions (FAQ) zu beachten. Kosten 200 $
  - Selbstverpflichtung ohne Prüfung und Nachweis
  - Keine Aussage über technische oder organisatorische Maßnahmen
- Der Düsseldorfer Kreis, das **Gremium in der Konferenz der Datenschutzbeauftragten des Bundes und der Länder**, hat im April 2010 erklärt, dass sich Datenexporteure in Deutschland **nicht auf die Behauptung einer Safe-Harbor-Zertifizierung von US-amerikanischen Unternehmen verlassen dürfen.**
- Derzeit haben sich ca. 2500 Firmen eintragen lassen.

Ein Highlight aus den AGB eines Cloudanbieters

… auf Grund der Safe Harbor Zertifizierung und laut der EU-Datenschutzrechtlinie ist die Übermittlung von Daten aus Ihrem Unternehmen an XXX rechtlich zulässig…

4. Frage

Erkaufen sich die Kunden das Mehr an Effizienz und Flexibilität durch einen Verlust an Informations- und Datenschutz?

Datenschutz versus Effizienz

- Bei Infrastrukturanbietern Gesamtkosten vergleichen
  (korrekte Lizenzierung, Datensicherung, Einbindung in Infrastruktur, Monitoring, Virenschutz, Berechtigungsvergabe, Datenschutz, Kosten für Kontrolle und Vertrag)
- Bei Software-as-a-Service deren Integration beachten
  (Oft sind SaaS Lösungen leistungsfähige Monolithen, die schwer in Prozesse mit anderen Anwendungen eingebunden werden können)
- Verfügbarkeit, Vertraulichkeit und Integrität beachten
- Migration in beide Richtungen planen
- Notfallkonzept erstellen

Gibt es Fragen?

Vielen Dank für die Aufmerksamkeit

Kontaktdaten

Klaus Foitzick
Vorstand

activeMind AG
Management und Technologieberatung

Potsdamer Straße 3
80802 München
Tel: **+49 89 418 56 01 - 70**
Fax: **+49 89 418 56 01 - 79**
Web: **www.activemind.de**
E-Mail: **foitzick@activemind.de**

- **Volljurist**
- **MCSE, VCP, ITIL v3 Manager**
- **ISO 9001 / 27001 Auditor des TÜV Hessen**
- **Auditorteamleiter der Bundesamtes für Sicherheit in der Informationstechnik (BSI) ISO 27001 auf Basis IT Grundschutz.**
- **Akkreditierter Prüfstellenleiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD)**

Was macht die activeMind AG?

- **Datenschutzbeauftragte für (IT-) Dienstleister**
- **Implementieren der ISO 27001 Norm und den BSI-Grundschutz (techn. und org.)**
- **Auditieren ISO 27001 / BSI / Datenschutz für das BSI / TÜV / ULD und Auftraggeber**

Mitarbeiter

- **3 Rechtsanwälte, 3 ISO 27001 Auditoren (TÜV), 2 BSI Auditoren, 1 ISO 9001 Auditor (TÜV), 1 ULD Prüfstellenleiter (Recht und Technik), 1 VCP, 1 MCSE**