Datenschutzrechtliche Aspekte des Cloud Computing

Der Hessische Datenschutzbeauftragte
Gustav-Stresemann-Ring 1
65189 Wiesbaden
Telefon 0611 / 1408-0
http://www.datenschutz.hessen.de
E-Mail: poststelle@datenschutz.hessen.de

Definitionen

Cloud-Anwender

Cloud-Anwender ist jede natürliche oder juristische Person, die von Betroffenen personenbezogene Daten erhebt, verarbeitet oder nutzt und hierfür von anderen Stellen IT-Dienstleistungen für Cloud-Services in Anspruch nimmt.

Cloud-Anbieter

Cloud-Anbieter ist jede natürliche oder juristische Person, die einem Cloud-Anwender IT-Dienstleistungen für Cloud-Services bereitstellt. Fehlen dem Cloud-Anbieter hierfür die Ressourcen, so kann dieser zur Erfüllung seiner Verpflichtungen gegenüber dem Cloud-Anwender u. U. weitere Unter-Anbieter einbeziehen.

Definitionen

1. Von Cloud Computing wird dann gesprochen, wenn eine oder mehrere Dienstleistungen aufeinander abgestimmt, schnell und dem tatsächlichen Bedarf angepasst sowie nach tatsächlicher Nutzung abrechenbar über ein Netz bereit gestellt werden.

2. Cloud Computing ist eine dynamische allokierbare Infrastruktur, in der Kapazitäten und Services nach Bedarf bezogen werden können. Die Grundlage dieser Infrastruktur ist die Virtualisierung sowohl der Hardware, des Speichers als auch des Netzwerks sowie der Software

3. IT aus der Steckdose

Betriebsmodelle

Private Cloud	Public Cloud	Hybrid Cloud	Community Cloud
Dienste innerhalb einer Institution	am freien Markt angeboten	Mischung aus Public und Private Cloud	mehrere Cloud-Anbieter bieten Cloud-Services einem definierten Kundenkreis an
Cloud-Anbieter und Anwender sind identisch	für jedermann verfügbar	sinnvoll zur Lastverteilung	
	beliebige Zahl von Anwendern		

Services

IaaS	PaaS	SaaS
Infrastrukture as a Service	Platform as a Service	Software as a Service
Anwender nutzen virtualisierte Komponenten , benutzen aber eigene Betriebssysteme und Programme	Anwender nutzen eigene Programme auf der vom Dienstleister bereitgestellten Infrastruktur	Anwender nutzen vom Dienstleister bereitgestellte Programme meist über Web-Browser

Kontrolle über Ressourcen

Selbst	Hosting	IaaS	PaaS	SaaS
Anwendung	Anwendung	Anwendung	Anwendung	Anwendung
VM	VM	VM	Services	Services
Server	Server	Server	Server	Server
Speicher	Speicher	Speicher	Speicher	Speicher
Netz	Netz	Netz	Netz	Netz

Abnahme der Kontrollmöglichkeit

---------- →

Nutzer hat Kontrolle **Geteilte Kontrolle** **Anbieter hat Kontrolle**

Welche Chancen bietet diese Technologie und welche Gründe sprechen für die Nutzung?

Hier sind im Wesentlichen wirtschaftliche Aspekte zu nennen:

1. Flexibilität bei der Buchung, Nutzung und Stilllegung von Rechenkapazitäten je nach aktuellem und ggf. auch kurzfristigen Bedarf (Skalierbarkeit)

2. Einfacher Erwerb, verbrauchsabhängige Bezahlung

3. Einsparpotenzial im Bereich –Anschaffung, Betrieb und Wartung der IT-Systeme

4. Ubiquitäre Verfügbarkeit von Geschäftsanwendungen unabhängig on geographischen Standorten.

Welche Risiken stehen dem entgegen?

- keine eindeutige Rechtslage
- Unsicherheit bzgl. der Verträge und der Haftungsregelungen
- ggf. unzulässige Übermittlung personenbezogener Daten außerhalb der EU und des EWR
- Unvereinbarkeit mit unternehmensweiter IT-Compliance
- Sicherheit und Verfügbarkeit der Cloud-Systeme
- Betriebs- und Sicherheitskonzepte werden nicht offengelegt
- Standort der Rechenzentren und Speicherort der Daten ist unbekannt
- keine ortsbezogene Datenverarbeitung
- Anbieter von Cloud-Systemen sind an der Transparenz nicht interessiert
- Flexibilität und Skalierbarkeit bedingen eine gewisse Intransparenz

Zahlreiche betroffene Rechtsgebiete

- Haftung , Gewährleistung
- Urheberrecht
- Steuer- und Handelsrecht (Revisionsfähigkeit)
- Verbraucherrecht, AGBs
- Strafprozessrecht
- Sicherheitsrecht
- IT-Vertragsrecht
- Datenschutzrecht

Wie ist der grundrechtliche Schutz der Daten verankert?

- Das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i V m. Art.1 Abs. 1 GG) umfasst das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.“

- Ein Eingriff auf dieses Grundrecht ist zudem dann anzunehmen, wenn die Integrität des geschützten informationstechnischen Systems angetastet wird, indem auf das System so zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können.

Was ist aus der Sicht der DSBs zu schützen, was sind personenbezogene Daten?

- Personenbezogene Daten sind Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (§ 2 Abs. 1 HDSG, §3 Abs. 1 BDSG).

- Darunter fallen Daten, die der Identifizierung der Person dienen, etwa der Name, die Anschrift oder das Geburtsdatum und alle sonstigen Informationen, die auf eine Person beziehbar sind. Bestimmt und bestimmbar ist eine Person, wenn sich aus den Daten unmittelbar oder mittelbar, also mit verfügbarem Zusatzwissen, aber ohne unverhältnismäßigen Aufwand die betroffene Person identifizieren lässt. Die Daten müssen eine natürliche Person, also einen Menschen, betreffen.

Verantwortung in der Cloud (1)
Verantwortliche Stelle

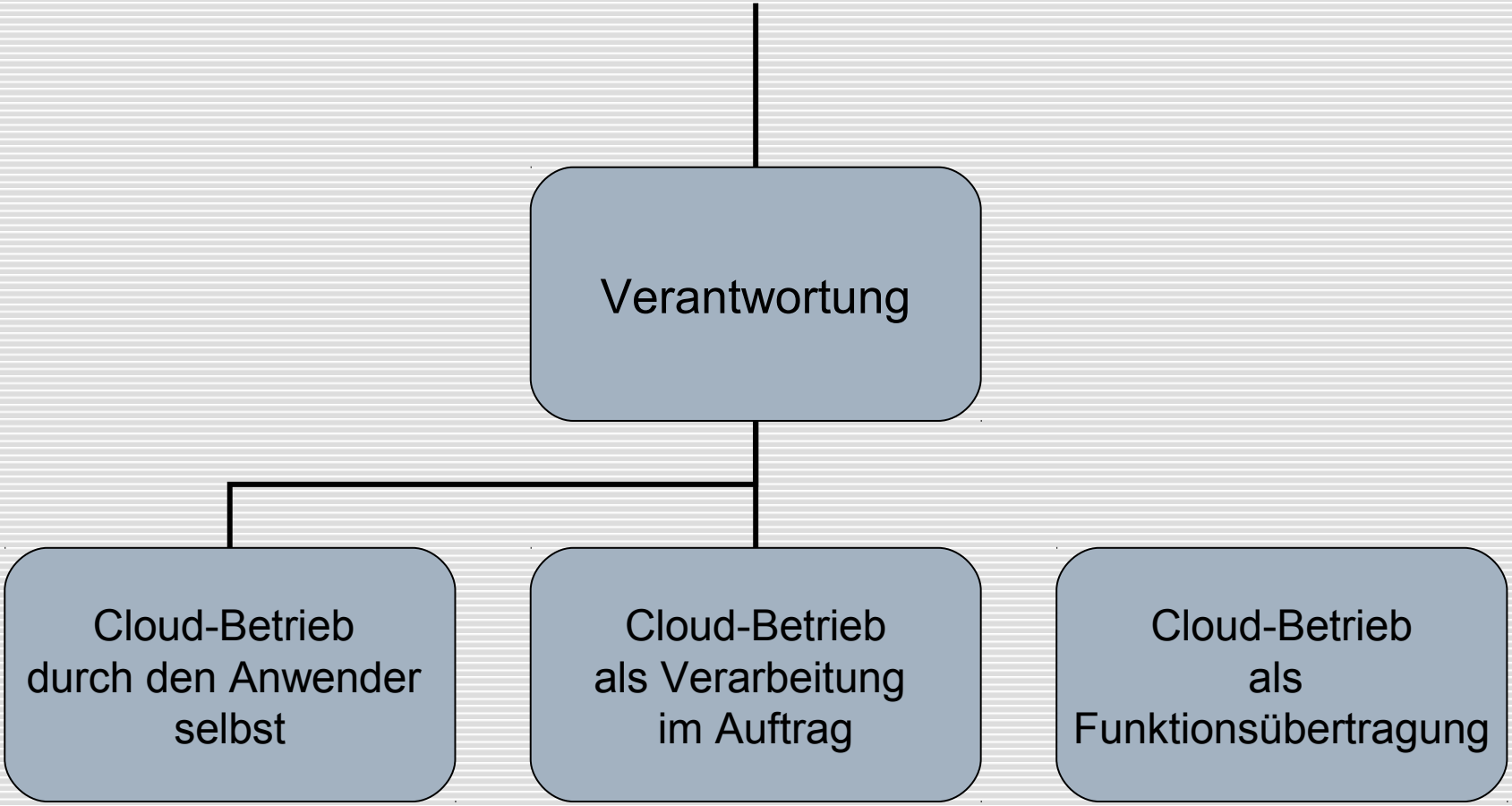
Das europäische Datenschutzrecht knüpft die rechtliche Verantwortung für die Datenverarbeitung personenbezogener Daten an die inhaltliche Verantwortung über die Entscheidung des Umgangs mit den Daten.

Wer ist verantwortliche Stelle?

§ 3 Abs. 7 BDSG: Verantwortliche Stelle ist jede Person, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder die durch andere vornehmen lässt.

Art. 2d EU-DS-RL: Verantwortlich ist, wer über Zwecke und Mittel der Datenverarbeitung entscheidet.

Verantwortung in der Cloud (2)
Betriebsmodelle



Verantwortung in der Cloud (3)
Betriebsmodell 1

Betrieb durch den Anwender selbst

- alleinige Verantwortung beim Cloud-Anwender, der gleichzeitig Cloud-Anbieter ist

- Cloud-Anwender (Private Cloud) ist der Adressat von
  - Verfügungen
  - Betroffenenansprüchen
  - Schadensersatzansprüchen
  - Bußgeldsanktionen

Verantwortung in der Cloud (4)
Betriebsmodell 2

Betrieb als Datenverarbeitung im Auftrag

Zulässigkeitsvoraussetzung:

Auftragnehmer müssen Personen und Stellen

- im Inland
- in einem Mitgliedsstaat der Europäischen Union
- in einem Mitgliedsstaat des Europäischen Wirtschaftsraums

Auftragnehmer:

- Bestimmungen des § 11 BDSG

Verantwortung in der Cloud (5)
Betriebsmodell 2

Betrieb als Datenverarbeitung im Auftrag

Grundsatz:

- Der Auftragnehmer bleibt für die Einhaltung der Datenschutzvorschriften verantwortlich

Pflichten Auftraggeber:

- Auftragnehmer muss unter Berücksichtigung der Eignung für die Gewährleistung der technischen und organisatorischen Maßnahmen ausgewählt werden
- Auftrag ist schriftlich zu erteilen

Pflichten Auftragnehmer:

- Daten dürfen nur nach Weisung des Auftraggebers verarbeitet werden
- Auftraggeber ist auf datenschutzwidrige Weisungen hinzuweisen

Verantwortung in der Cloud (6)
Betriebsmodell 2

Im Auftrag ist detailliert fest zu halten(Vgl. § 11 Abs. 2 BDSG)

- Gegenstand und Dauer des Auftrags
- Umfang, Art und Zweck der Erhebung, Verarbeitung und Nutzung von Daten
- Kreis der Betroffenen
- Technische und organisatorische Maßnahmen nach § 9 BDSG
- Berichtigung, Sperrung und Löschung von Daten
- Pflichten des Auftragnehmers und dessen Kontrollen
- Unterauftragsverhältnisse
- Kontrollrechte des Auftragnehmers und Mitwirkungspflichten des Auftragnehmers
- Mitzuteilende Verstöße des Auftragnehmers gegen Datenschutzvorschriften
- Umfang der Weisungsbefugnisse des Auftraggebers
- Rückgabe von Datenträgern bzw. Löschung von Daten nach Auftragsbeendigung

Verantwortung in der Cloud (7)
Betriebsmodell 2

Kontroll- und Dokumentationspflichten nach BDSG

Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.

Das Ergebnis ist schriftlich fest zu halten.

Verantwortung in der Cloud (8)
Betriebsmodell 3

Betrieb als Funktionsübertragung

DV im Auftrag ist nicht zulässig, wenn

- Auftragnehmer Dritter im Sinne des BDSG ist(§ 3 Abs. 8 S 2), insbesondere
  - jede Stelle außerhalb der Europäischen Union (EU)
  - außerhalb des Europäischen Wirtschaftsraums (EWR)

Folge:

- Bestimmungen des § 11 BDSG sind nicht anwendbar
- rechtliche Voraussetzungen für eine Datenübermittlung müssen gegeben sein (bspw. §§ 4b, 4c BDSG)

Verantwortung in der Cloud (9)
Betriebsmodell 3

Zulässigkeit der Datenübermittlung in die Cloud

Vertrag (§ 28 Abs. 1 Nr. 1 BDSG)

- Übermittlung muss zur Erfüllung eines Vertrages mit dem Betroffenen erforderlich sein

Aber:

- Wer hat solche Verträge mit den Betroffenen?

Erforderlichkeit (§ 28 Abs. 1 Nr. 2 BDSG)

- Übermittlung muss zur Wahrung berechtigter Interessen des Cloud-Nutzers erforderlich sein und die Interessen der Betroffenen dürfen nicht überwiegen

Aber:

- Wann ist eine Datenverarbeitung außerhalb der EU/EWR erforderlich?
- Wie können die Interessen der Betroffenen gesichert werden?

Verantwortung in der Cloud (10)
Vergleich

Cloud-Betrieb für die öffentliche Verwaltung

- nur private Cloud

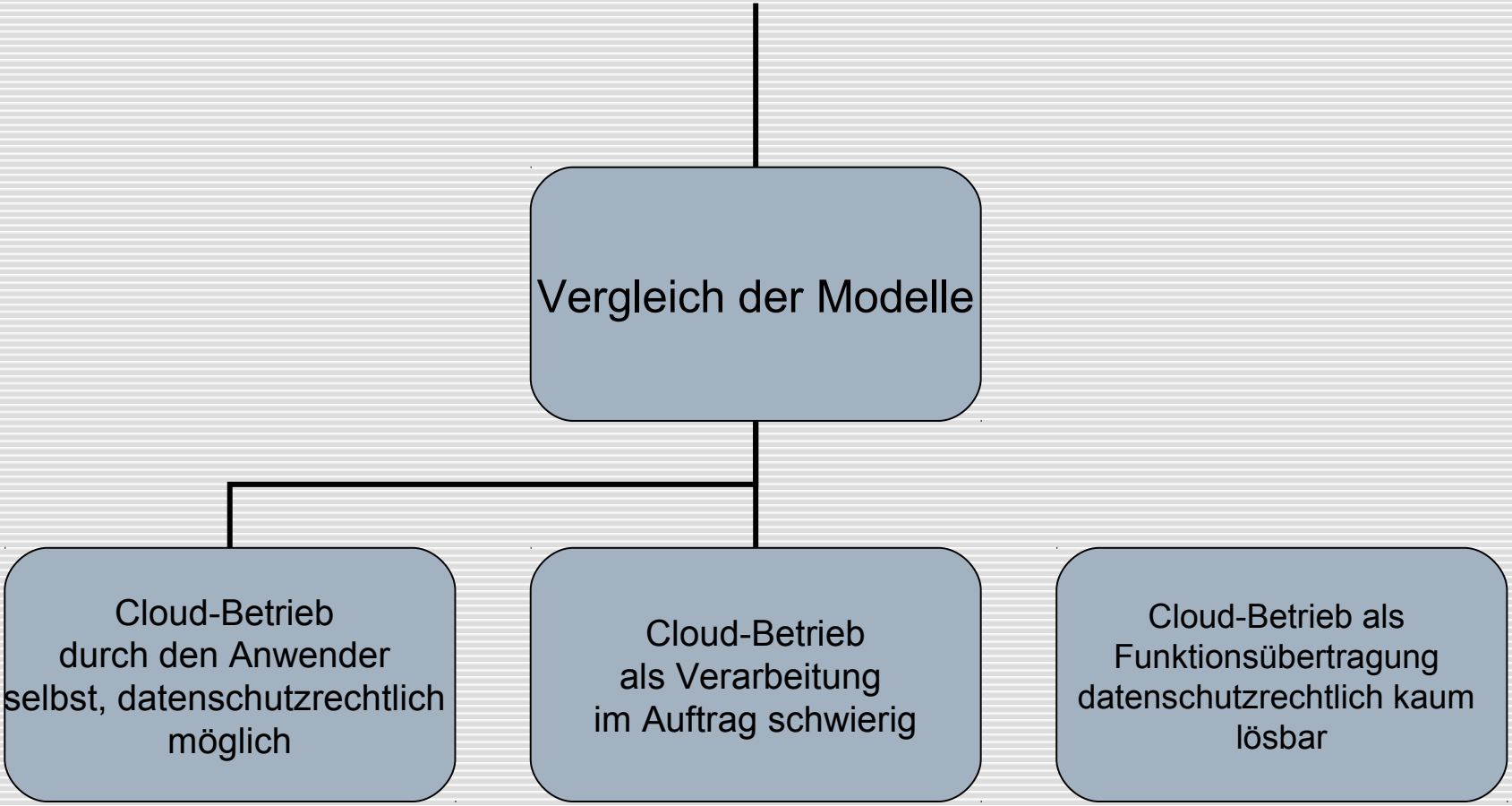
Cloud-Betrieb als ADV

- rechtlich grundsätzlich möglich
- Anzahl der möglichen Auftragnehmer stark eingeschränkt
- Pflichten des Auftraggebers praktisch kaum wahrnehmbar
- Grenzüberschreitende Kontrollen faktisch schon im EU-Raum unrealistisch

Cloud-Betrieb als Funktionsübertragung

- außerhalb der EU und des EWR-Raums problematisch
- Schutz der Betroffenenrechte praktisch nicht realisierbar
- Grenzüberschreitende Kontrollen unrealistisch
- Rechtlich allenfalls denkbar durch Vertrag mit Betroffenen

Verantwortung in der Cloud (11)
Fazit



Forderungen und Empfehlungen
Schutz der Grundwerte

Verfügbarkeit	Vertraulichkeit	Integrität	Revisionssicher-heit	Transparenz
Personenbezo-gene Daten stehen zeitgerecht zur Verfügung und können ordnungsgemäß von autorisierten Benutzern verarbeitet werden	Nur Befugte können personenbezoge ne Daten zur Kenntnis nehmen.	Personenbezo-gene Daten bleiben während der Verarbeitung unversehrt, vollständig und aktuell. Die Funktionsweise der Systeme ist vollständig gegeben.	Es kann festgestellt werden, wer wann welche personenbezogene Daten in welcher Weise verarbeitet hat.	Die Verfahrensweise bei der Verarbeitung personenbezoge ner Daten ist vollständig, aktuell und in einer Weise dokumentiert, dass sie in zumutbarer Zeit nachvollzogen werden kann.

Risiken in der Cloud

Cloudspezifische Risiken

- Löschung von Daten
- Nachvollziehbarkeit durch Protokollierung
- Vervielfältigung und Verteilung der Daten
- Sorgfältige Einführung von Cloud-Lösungen

Klassische Risiken

- Datentrennung
- Transparenz
- Verfügbarkeit

Forderungen und Empfehlungen

§ 9 BDSG

Technische und organisatorische Maßnahmen

- Maßnahmen, die erforderlich sind, um die Ausführung der Vorschriften des BDSG einzuhalten
- Aufwand muss im angemessenen Verhältnis zum Schutzzweck stehen
- Details sind in Anlage zu § 9 BDSG

Forderungen und Empfehlungen

Informationssicherheit beim Cloud-Anwender

- Management von Risiken, die mit der Auslagerung von Geschäftsprozessen einhergehen
- Etablierung eines Informationssicherheitsmanagement nach BSI-Standard 100-1
- Eigenes Sicherheitskonzept gemäß BSI-Standard 100-2 und 100-3
- Abstimmung des Sicherheitskonzeptes mit dem des Cloud Anbieters
- Risikoanalyse in Bezug auf
  - Sicherheit von Web-Anwendungen
  - Authentifikationsverfahren
  - Verschlüsselung bei der Übertragung und ggf. bei der Speicherung
  - Web-Service-Standards
  - Malware

Forderungen und Empfehlungen

Klare Regelung der Zugriffsrechte

- Abschottung der einzelnen Auftragsverhältnisse

- Differenziertes Zugriffsrechte - System insbesondere beim Einsatz von Virtualisierungstechniken
  - welcher Nutzer verwaltet welche Maschine
  - welche Dateiberechtigungen werden in virtuellen Maschinen eingerichtet
  - Welchr Rechte sind für das Gastbetriebssystem erforderlich

Forderungen und Empfehlungen

Informationssicherheit beim Cloud-Anbieter

- vollständige Transparenz der Cloud gegenüber dem Cloud-Nutzer
- Etablierung eines Informationssicherheitsmanagement nach BSI-Standard 100-1
- Sicherheitskonzept gemäß BSI-Standard 100-2 und 100-3
- Abstimmung des Sicherheitskonzeptes mit dem des Cloud-Anwenders
- Ereignismanagement (z.B. gemäß BSI-Baustein 1.8 Behandlung von Sicherheitsfällen)
- Datenschutzstandards durch Erarbeitung von Protection-Profiles
- Transparente Auditierung

  (Zertifizierung nach Common Criteria, ISO 27001, FISMA-Zertifikat, SAS-70-Typ II-Zertifikat, Gütesiegel der künftigen Stiftung Datenschutz dem des §9a BDSG oder des ULD S-H)

Forderungen und Empfehlungen

Außereuropäische Clouds

- Datenübermittlung außerhalb des EU/EWR-Raums unzulässig, es sei denn, ein angemessenes Datenschutzniveau existiert (§ 4b Abs. 2,3 BDSG)
- Gilt bspw. für Schweiz, Kanada und Argentinien
- Bei Datenverkehr an Drittstaaten können die Standard-Klauseln nach der Richtlinie 95/46/EG vom 05.02.2010 greifen
- Safe-Harbour-Selbstzertifizierungen in den USA reichen allein nicht aus
- Nachweis der Vertrauenswürdigkeit mit einem SAS-70-TYPII-Zertifikat genügen den Anforderungen nur teilweise
- Möglich sind verbindliche Unternehmensregelungen (Binding Corporate Rules), die ein angemessenes Datenschutzniveau per Vertrag garantieren und durch die Datenschutz-Aufsichtsbehörden genehmigt werden müssen (§4 c BDSG)

Ausblick

Was erfordert datenschutzgerechtes Cloud-Computing?

- transparente, detaillierte und eindeutige vertragliche Regelungen der cloud-gestützten ADV, insbesondere zum Ort der Datenverarbeitung und zur Benachrichtigung über eventuelle Ortswechsel, zur Portabilität und Interoperabilität
- Transparente und detaillierte Informationen der Anbieter über die technischen , organisatorischen und rechtlichen Rahmenbedingungen einschließlich der Sicherheitskonzeption
- Abgestimmte Sicherheitsmaßnahmen zwischen Cloud-Anbietern und Cloud-Anwendern
- Spezielle Auditierungsverfahren und aktuelle Zertifikate, die die Infrastruktur betreffen, die bei der Auftragserfüllung in Anspruch genommen wird
- Weiterentwickelte Standardvertragsklauseln speziell für Cloud Computing

Ausblick

Noch Fragen ?

Literatur

- BSI-Mindestsicherheitsanforderungen an Cloud-Computeranbieter
- Orientierungshilfe Cloud-Computing
- Cloud-Computing für die öffentliche Verwaltung
  ISPRAT-Studie 11/2010 des Fraunhofer Instituts für offene Kommunikationssysteme
- Materialien der ENISA zum Thema Cloud Computing
- Cloud Computing - Was Entscheider wissen müssen
  Bitkom-Leitfaden