Software as a Service und Datenschutz – Die Erfahrungen der UB Mannheim bei der Einführung von Alma

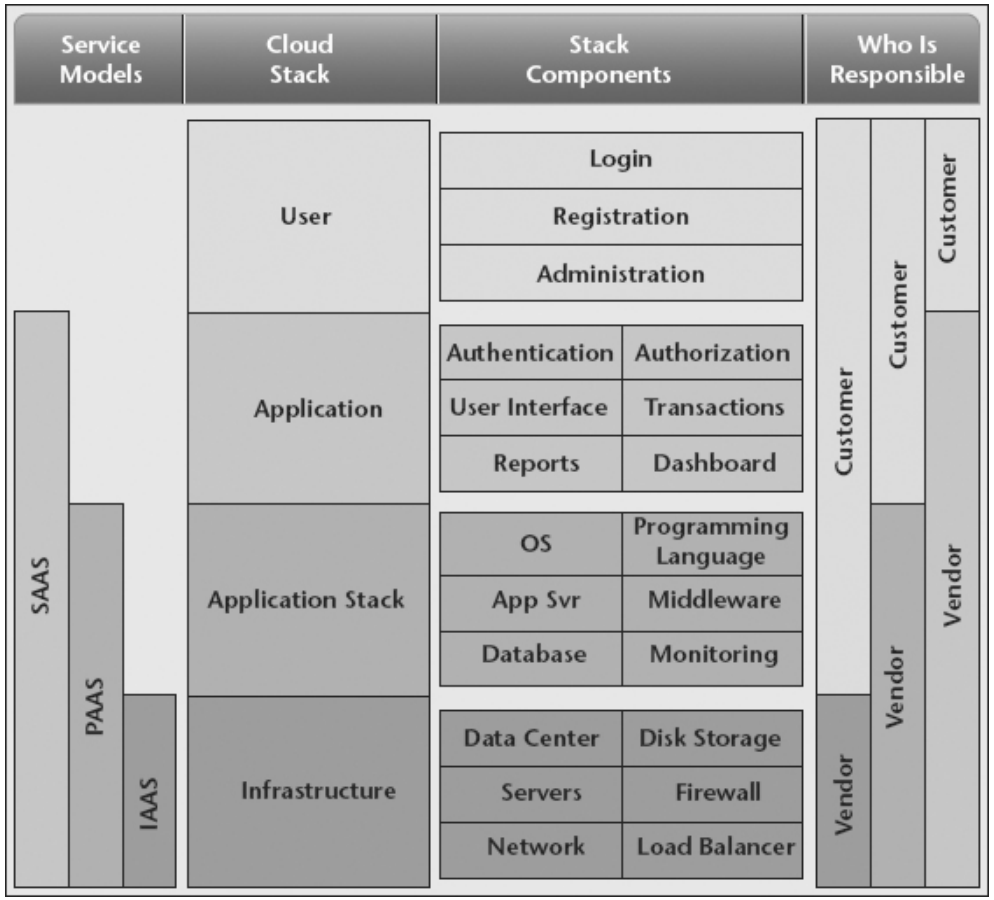
13. InetBib-Tagung, 12.02.2016

Dr. Marion von Francken-Welz, Dr. Christian Hänger

Themen

1. Alma als Software as a Service (SaaS)
2. Auftragsdatenverarbeitung
3. Personenbezogene Daten
4. Sorgfältige Auswahl des Auftragnehmers
5. Housing als Auftragsdatenverarbeitung?
6. Support durch Ex Libris Ltd. (Israel)
7. Fazit

1. Alma als Software as a Service (SaaS)



Quelle: Kavis, Michael J.: Architecting the Cloud Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS), Hoboken : Wiley 2014.

1. Alma als Software as a Service (SaaS)

- **Situation**
  Die Ex Libris GmbH stellt eine Applikation und Supportleistungen für die Universität Mannheim auf einer Serverfarm in Amsterdam zur Verfügung. Die Server stehen in den Räumen des niederländischen Unternehmens Equinix. In Ausnahmefällen greift das israelische Unternehmen Ex Libris - a ProQuest Company auf die Applikation zu.
- **Beratung durch ZENDAS**
  Zentrale Datenschutzstelle der baden-württembergischen Universitäten

2. Auftragsdatenverarbeitung

§ 7 LDSG BW, § 11 BDSG

- Beauftragung Dritter mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten
- Auftragnehmer verarbeitet Daten in der EU (§ 3 Abs. 5 LDSG BW; vgl. § 3 Abs. 8 S. 3 BDSG)
- Der Auftraggeber bleibt für die Einhaltung des Datenschutzes verantwortlich (§ 7 Abs. 1 S. 1 LDSG BW; § 11 Abs. 1 S. 1 BDSG).
- Weisungsgebundenheit des Auftragsnehmers (§ 7 Abs. 3 S. 2 LDSG BW, § 11 Abs. 3 S. 1 BDSG)

2. Auftragsdatenverarbeitung

- Der Auftragnehmer ist sorgfältig auszuwählen (§ 7 Abs. 2 S. 1 LDSG BW; § 11 Abs. 2 S. 1 BDSG) und zu überwachen (§ 7 Abs. 2 S. 6 LDSG BW; § 11 Abs. 2 S. 4 BDSG).
  - Kontrolle vor Ort nicht zwingend
  - Veröffentliche Informationen, Zertifizierungen, Prüfberichte, Referenzen (vgl. *Plath*, in: Plath, BDSG, § 11 BDSG Rn. 55, 92)
- Gesetzliche Mindestanforderungen an Vertragsinhalt (§ 7 Abs. 2 S. 4 LDSG BW; § 11 Abs. 2 S. 2 BDSG)
  - Weisungsbefugnis (§ 7 Abs. 2 S. 4 LDSG BW; § 11 Abs. 2 S. 2 Nr. 9 BDSG)
  - Kontrollrechte (§ 11 Abs. 2 S. 2 Nr. 7 BDSG)
  - Regelung über mögliche Unteraufträge (§ 7 Abs. 2 S. 4 LDSG BW; § 11 Abs. 2 S. 2 Nr. 6 BDSG)

3. Personenbezogene Daten

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener) (§ 3 Abs. 1 LDSG BW; § 3 Abs. 1 BDSG).

- Nutzerdaten
- Lieferantendaten
- Daten von MitarbeiterInnen
- Katalogdaten (z. B. Angaben über noch lebende Autoren oder Herausgeber)
- Administrationsvorgänge in der Applikation und im Webserver (Systemnutzer)

4. Sorgfältige Auswahl des Auftragnehmers

Der Auftragnehmer ist sorgfältig auszuwählen (§ 7 Abs. 2 S. 1 LDSG BW; § 11 Abs. 2 S. 1 BDSG).

Übernahme der Ex Libris Group durch ProQuest

- Die Server befinden sich weiterhin in den Niederlanden, Ex Libris (Deutschland) GmbH bleibt rechtlich selbständig (→ Auftragsdatenverarbeitung).
- Eine Übermittlung personenbezogener Daten an US-amerikanische Behörden ist datenschutzrechtlich unzulässig.
- Laut Ex Libris dürfen weder die europäischen Tochtergesellschaften noch Ex Libris Ltd. Daten europäischer Kunden an US-amerikanische Behörden herausgeben.
- Keine Anhaltspunkte für ein zu erwartendes rechtswidriges Verhalten.

4. Sorgfältige Auswahl des Auftragnehmers

… insbes. im Hinblick auf die technischen und organisatorischen Maßnahmen (§ 7 Abs. 2 S. 2, § 9 LDSG BW; § 11 Abs. 2 S. 1, § 9 BDSG)

- Wird idealerweise **durch Datenschutz- und Sicherheitskonzept** gewährleistet
- Zertifizierung nach ISO 27.001
- Referenzkunden in EU
- Technische und organisatorische Maßnahmen wie im Verfahrensverzeichnis beschrieben

4. Sorgfältige Auswahl des Auftragnehmers

Technische und organisatorische Maßnahmen

- Server der Ex Libris GmbH in durch Zutrittskontrolle und Kameras gesichertem Raum und dort in abgeschlossenen Schränken
- Verschlüsselung der Daten nach AES 128 Bit
- Keine externen Laufwerke oder USB-Ports der Server
- Zugang zum System ausschließlich für autorisierte Personen
- Verschlüsselte Kommunikation zwischen Applikation und Client (HTTPS, stunnel)

5. Housing als Auftragsdatenverarbeitung?

Technisches Konzept

- Rechenzentrum der Firma Equinix NL mit folgenden Infrastrukturleistungen: Standort, Elektrizität, Klimatisierung etc.
- Administration der Server-Hardware, Netzwerk- oder Speicherkomponenten durch Ex Libris GmbH
- Verhinderung des unrechtmäßigen Zugangs zu personenbezogenen Daten durch geeignete Schutzmaßnahmen

5. Housing als Auftragsdatenverarbeitung?

- Wartungsarbeiten und vergleichbare Hilfstätigkeiten gelten als Datenverarbeitung im Auftrag (§ 7 Abs. 5 LDSG BW; vgl. § 11 Abs. 5 BDSG).
- „Hintergrund der Regelung [in § 11 Abs. 5 BDSG] ist, dass bei der Wartung von IT-Systemen […] die Gefahr besteht, dass der Dienstleister **im Rahmen seiner Tätigkeit** Kenntnis von personenbezogenen Daten erhält“ (*Plath*, in: Plath, BDSG, 2012, § 11 Rn. 121).
- Der Housing-Betreiber könnte sich allenfalls widerrechtlich Zugriff auf personenbezogene Daten verschaffen.

6. Support durch Ex Libris Ltd. (Israel)

Übermittlung (§§ 18, 20 LDSG BW; §§ 16, 4b BDSG)

- Erforderlichkeit der Übermittlung (§ 18 Abs. 1 Nr. 1, § 15 Abs. 1 Nr. 1 LDSG; § 16 Abs. 1 Nr. 1, § 14 Abs. 1 S. 1 BDSG)

→ Support durch Fernzugriff nur im Ausnahmefall

- Keine zweckändernde Nutzung bei Prüfung und Wartung (§ 18 Abs. 1 Nr. 1, § 15 Abs. 1 Nr. 2, Abs. 3 LDSG)
- Kein überwiegendes schutzwürdiges Interesse des Betroffenen (§ 20 Abs. 3 S. 1 Nr. 2 LDSG BW; § 4b Abs. 2 S. 2 BDSG)

→ Israel verfügt über ein angemessenes Datenschutzniveau (Beschluss der EU-Kommission vom 31. Januar 2011, 2011/61/EU).

→ Interesse der UB an Wiederherstellung des störungsfreien Systembetriebs

7. Fazit

- Erarbeitung einer praktikablen Lösung in Zusammenarbeit mit Ex Libris und ZENDAS bei hohen datenschutzrechtlichen Anforderungen
- Datenschutz verhindert nicht den Softwarebetrieb, sondern führt zur Standardisierung und gewährleistet Datensicherheit