Datenschutz und Datensicherheit rechtliche Aspekte

13. OSL-Technologietage

24. September 2015

PENTAHOTEL Berlin-Köpenick

Überblick

- Grundlagen Datenschutz
- Grundlagen Datensicherheit
- Clouds
  - In EU/EWR
  - In Drittländer
  - (Rechts-)Folgen

Grundlagen Datenschutz I

Daten nach dem Bundesdatenschutzgesetz (BDSG)

§ 1 Abs. 2 Nr. 3 BDSG

„…soweit sie Daten […] unter Einsatz von Datenverarbeitungs-anlagen […] oder die Daten in oder aus nicht automatisierten Dateien […],…“

+

§ 3 Abs. 1 BDSG

Personenbezogene Daten (pb Daten) :

- *Einzelangaben*
- *Persönliche oder sachliche Verhältnisse*
- *Einer bestimmten oder bestimmbaren natürlichen Person*

§ 3 Abs. 9 BDSG

Besondere Arten personenbezogener Daten (bes. pb Daten)

„…Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschafts-zugehörigkeit, Gesundheit oder Sexualleben.“

Grundlagen Datensicherheit

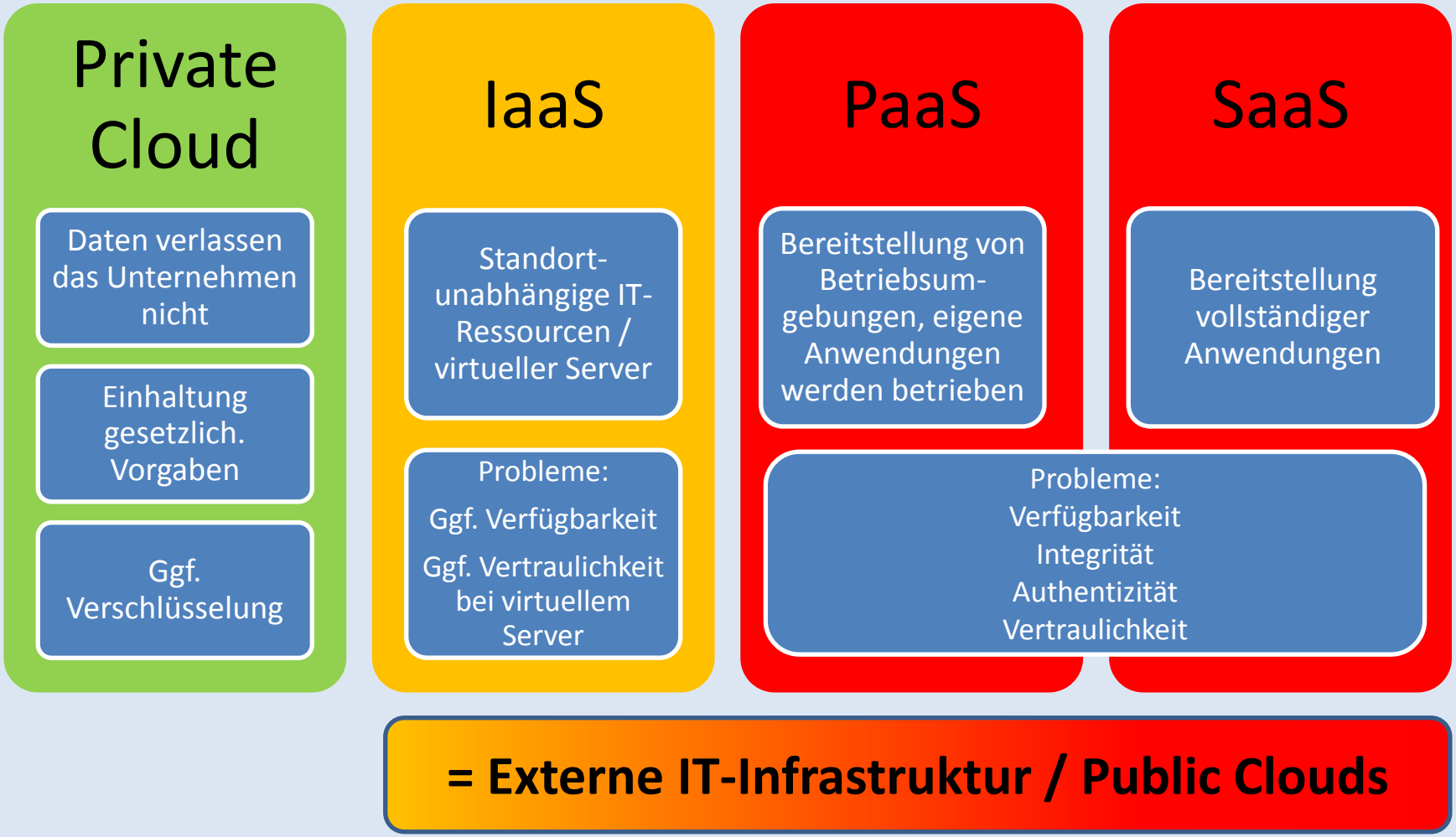
§ 9 BDSG: „technischen und organisatorischen Maßnahmen […), wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht."

→ Anlage zu § 9 BDSG

1. Zutrittskontrolle
2. Zugangskontrolle
3. Zugriffskontrolle
4. Weitergabekontrolle
5. Eingabekontrolle
6. Auftragsdatenkontrolle
7. Verfügbarkeitskontrolle
8. Trennungsgebot

„…insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren."

Cloud


Private Cloud
Daten verlassen das Unternehmen nicht
Einhaltung gesetzlich. Vorgaben
Ggf. Verschlüsselung
IaaS
Standort-unabhängige IT-Ressourcen / virtueller Server
Probleme:
Ggf. Verfügbarkeit
Ggf. Vertraulichkeit bei virtuellem Server
PaaS
Bereitstellung von Betriebsum-gebungen, eigene Anwendungen werden betrieben
SaaS
Bereitstellung vollständiger Anwendungen
Probleme:
Verfügbarkeit
Integrität
Authentizität
Vertraulichkeit
= Externe IT-Infrastruktur / Public Clouds

Voraussetzung für die Datenverarbeitung in der Cloud

„für eigene Geschäfts-zwecke“ (§§ 28 ff. BDSG)

Wirksame Einwilligung

Vertragliche Regelungen

- In der EU/EWR
  - Auftragsdaten-verarbeitung (ADV)
- In Drittländer
  - Angemessenes Datenschutzniveau

Clouds in der EU/EWR

Auftragsdatenverarbeitung (ADV) nach § 11 BDSG

- Schriftliche Festlegung der Essentialia Negotii
- Beachtung der TOM gemäß der Anlage zu § 9 BDSG
- Cloudbetreiber ist weisungsgebunden
- Datenschutzverstöße müssen gemeldet werden
- Ggf. Regelung zu Unterauftragnehmern

Auftraggeber muss regelmäßig insb.
die Einhaltung der TOM kontrollieren!

Clouds in Drittländern

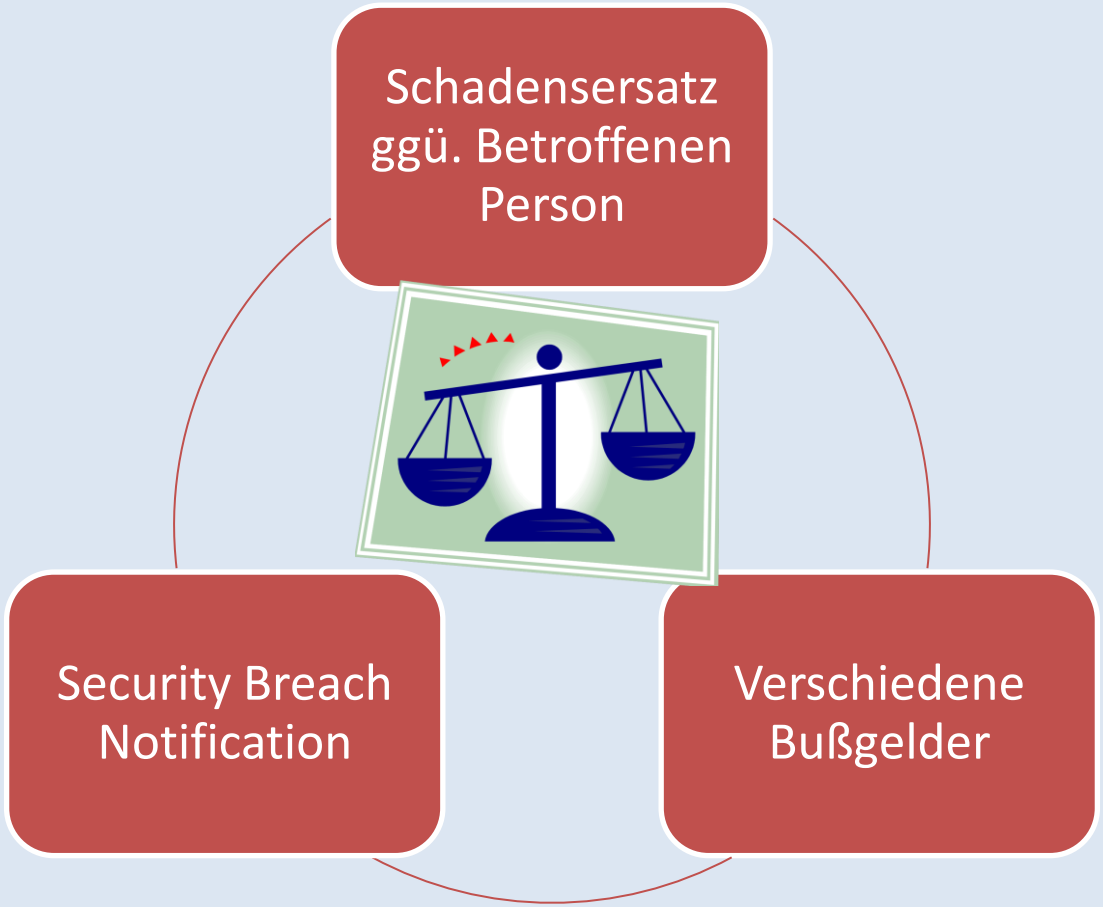
BDSG gilt außerhalb EU nicht

→ Übermittlung nur, wenn angemessenes DS-Niveau gewährleistet! (§ 4b Abs. 2 BDSG)

Voraussetzung für Datenverarbeitung in Drittländern

1. Läge nach deutschen Recht eine gültige Rechtsgrundlage für die Datenübermittlung vor?
2. Ist ein angemessenes DS-Niveau im Empfängerland garantiert?
   - EU-Standard-Vertragsklauseln
   - Binding Corporate Rules
   - Für USA: Safe Harbour  Patriot Act

(Rechts-)Folgen



Zusammenfassung datenschutzkonforme Cloud

Personenbezogene Daten

Pb Daten:
-bes. pb Daten
-Berufsgeheimnis
-Kreditkarten- und Kontodaten

Daten, die hochverfügbar sein müssen

Geschäftsgeheimnisse

Cloud in EU/EWR

„für eigene Geschäftszwecke“ (§§ 28 ff. BDSG)

Wirksame Einwilligung

ADV

Cloud in Drittland

angemessenes DS-Niveau garantiert?

Vielen Dank!

Rechtsanwältin Julia Hesse, LL.M.

office@juliahesse.eu

Anhang: Zertifikate

- Liste der Anbieter von Datenschutzzertifikaten der Stiftung Datenschutz
- Datenschutzstandard DS-BVD-GDD-01 (Anforderungen an Auftragnehmer nach § 11 BDSG)
- ISO 27001
- ISO 27001 auf Basis IT-Grundschutz
- ISO 27018

Anhang: Vertragsentwürfe

- GDD: Muster zur ADV nach § 11 BDSG
- Überblick Standardvertragsklauseln der EU
  - Binding Corporate Rules i. S. v. Art. 25 Abs. 1, 2 bzw. Art. 26 Abs. 2 RL 95/46/EG
  - Standardvertragsklauseln der Europäischen Kommission i. S. v. Art. 26 Abs. 2, 4 RL 95/46/EG
  - Safe-Harbour-Regelungen i. S. v. Art. 25 Abs. 1, 2 RL 95/46/EG

Anhang: Ratgeber

- GDD-Ratgeber "Datenschutzprüfung von Rechenzentren“ & Checkliste
- Bitkom: Leitfaden Cloud Computing
- BSI: Cloud Computing Dossiers