TeleTrusT
Pioneers in IT security.

Informationstag "IT-Sicherheit im Arbeitsrecht"

Berlin, 15.04.2014

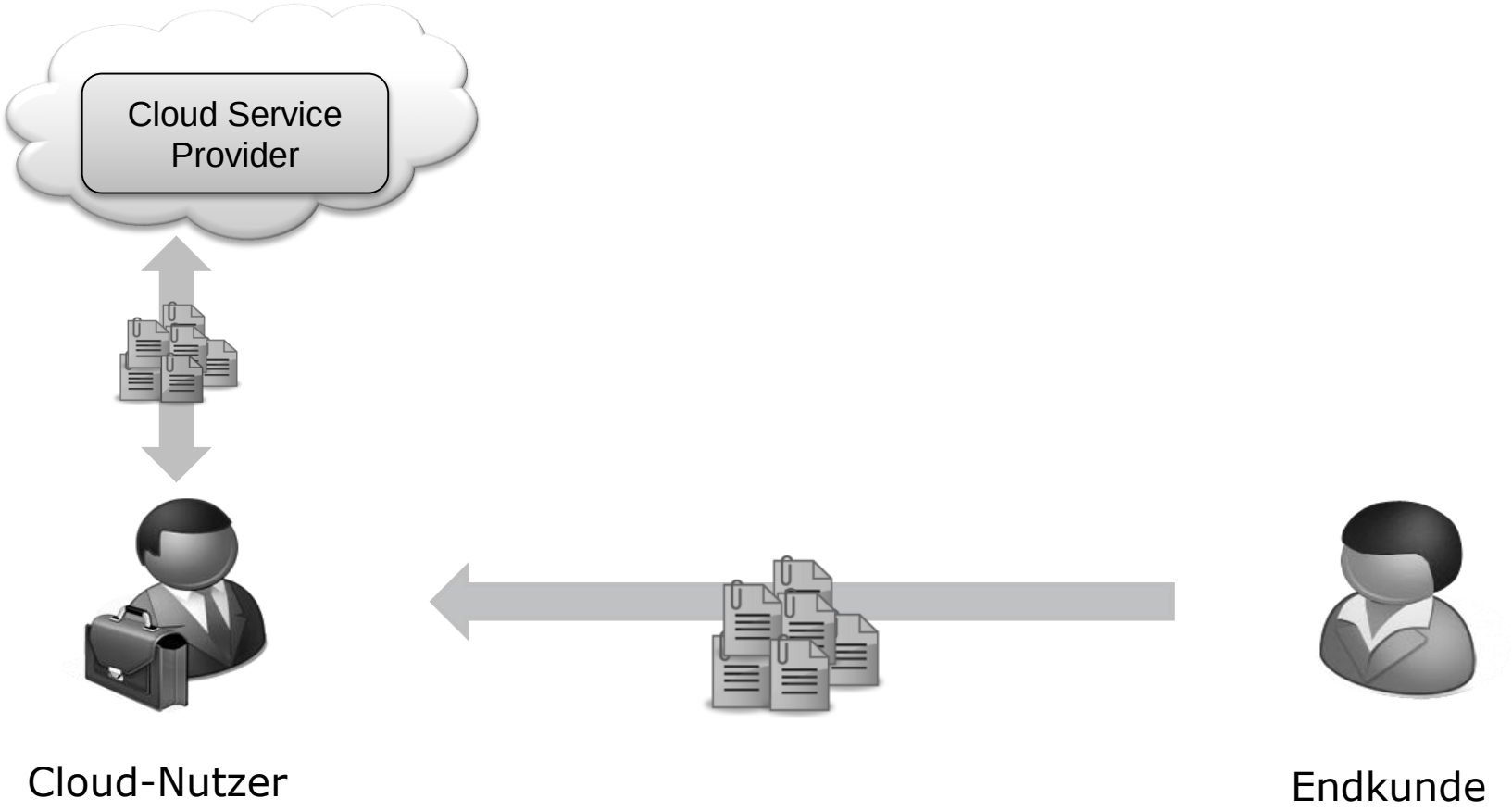
Sicherheit in Cloud-Diensten

Karsten U. Bartels LL.M.
Rechtsanwalt, HK2 Rechtsanwälte

HK2
Rechtsanwälte

- Rechtsanwalt
- Lehrbeauftragter der TH Wildau
- Zertifizierter Datenschutzbeauftragter (TÜV)
- Sachverständiger für IT-Produkte beim ULD S-H
- Auditor datenschutz cert GmbH
- Leiter AG Recht, TeleTrusT
- Stellv. Vorsitzender der davit.de
- Schlichter IT-Recht der IHK Berlin

Worum geht es?



HK2
Rechtsanwälte

Leistungsvereinbarung

+

Vereinbarung zum Datenschutz

Leistungsvereinbarung

- Prüfbare Leistungsbeschreibung
- Change Management
- Back-Up / Archivierung
- Nutzungsrechte
- Subunternehmer / back-to-back
- Mitwirkungspflichten/ Nebenpflichten
- Variable Abrechnung
- Service Level Agreement
- Exit

Re-Insourcing / Datenportabilität

- Kein Cloud-Vertrag ohne Exit
- Portierung
  - Umfang der Daten
  - Format und Medien
  - Transportrisiko
  - Prüfung der Daten
  - Schnittstellen
  - Informationspflichten
  - Fristen
  - Zielsystem
- Recht auf Portierungen/ Portierungsfall

Nicht zu verwechseln mit …

HK2 Rechtsanwälte

Art. 18 EU DSGVO-Entwurf, KOM(2012) 11

bzw.

Entschließung EP, 12.03.14, 1. Lesung
Art. 15, Abänderung 111

HK2
Rechtsanwälte

SLA

1. Time to repair, MeanTTR
2. Abgrenzung Fehler-/ Anwender-Support
3. Service Requests
4. Monitoring

Technische Skalierbarkeit

≠

Anspruch auf Skalierbarkeit

SLA: Verfügbarkeit

- Leistungsbeschreibung vs. Haftungsbegrenzung
- Übergabepunkte
- Verantwortlichkeit für IT
- Verfügbarkeit
  - Problem: 99,xx % im Monatsmittel + Scheduled Downtime
  - Problem: Messung

SLA: Messung der Verfügbarkeit

- Objekt der Verfügbarkeit
- Was wird gemessen?
- Wie wird gemessen?
- Wo wird gemessen?
- Wer misst?
- Auskunftspflichten
- Sanktionsregime

Leistungsvereinbarung: Allgemeines

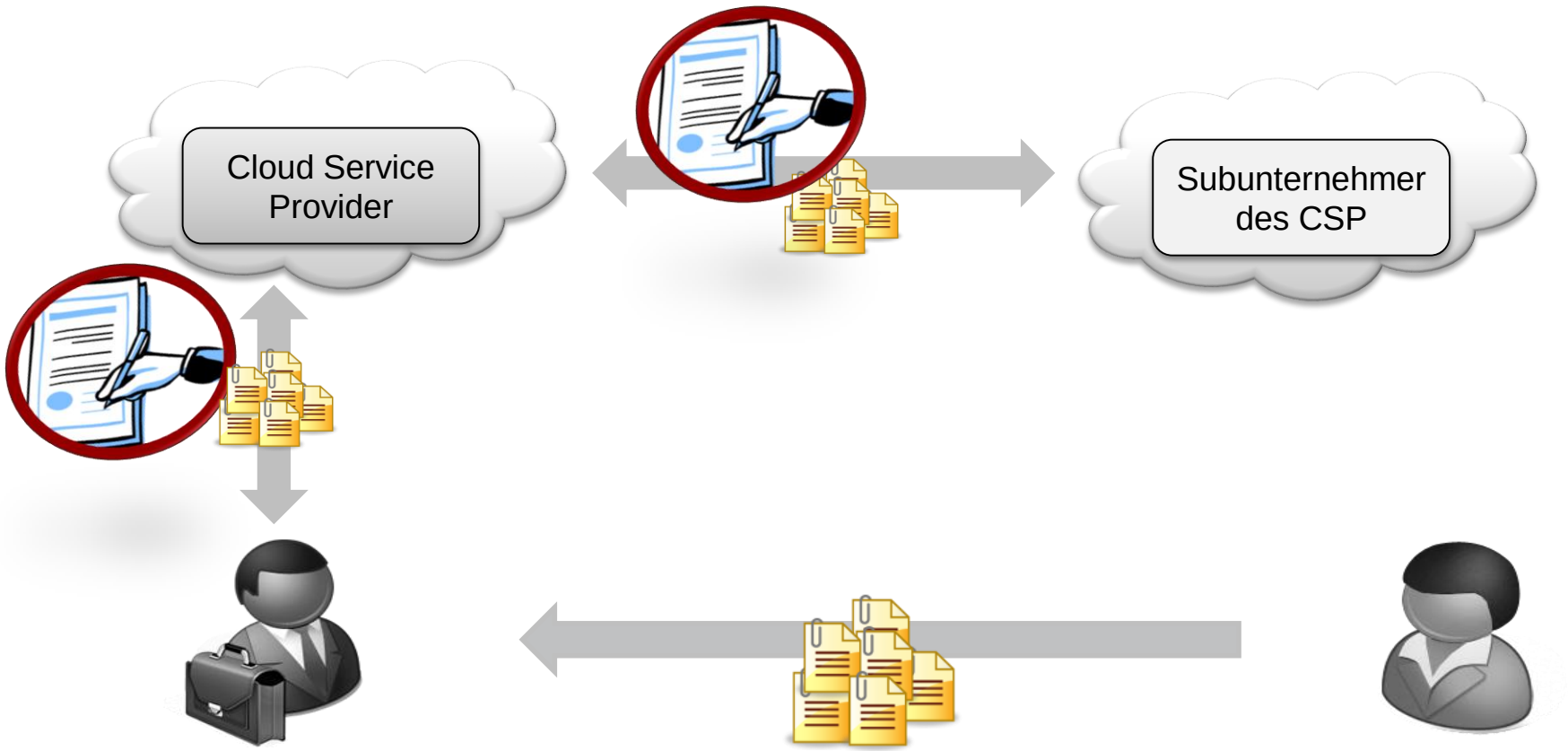
HK2 Rechtsanwälte

- AGB-Kollision
- Haftungsbeschränkung
- Geheimhaltung (know how)
- Mindestvertragslaufzeiten + Kündigungsregelungen
- Eskalationsregime / ADR
- Rechtswahl + zwingendes Recht
- Gerichtsstand

HK2
Rechtsanwälte

ADV-Vereinbarung
(Auftragsdatenverarbeitung)

HK2
Rechtsanwälte



Auftragsdatenverarbeitung
§ 11 BDSG

HK2 Rechtsanwälte

- Erforderliche Regelungen in Schriftform
  - Gegenstand und die Dauer des Auftrags
  - Umfang, Art und Zweck der vorgesehenen Datenverwendung
  - Weisungsrechte des Auftraggebers
  - Kontrollrechte des Auftraggebers
  - Regelungen von Subunternehmerverhältnissen
  - Festlegung der „TOM“, § 9 BDSG
  - Datenrückgabe, Löschungspflichten

Technische und organisatorische Maßnahmen (TOM)

HK2 Rechtsanwälte

- § 9 BDSG, Anlage zu § 9 S. 1 BDSG
  - Zutrittskontrolle
  - Zugangskontrolle
  - Zugriffskontrolle
  - Weitergabekontrolle
  - Eingabekontrolle
  - Auftragskontrolle
  - Verfügbarkeitskontrolle
  - „Trennungskontrolle“

Kontrollpflicht / Prüfung durch Dritte

HK2 Rechtsanwälte

- Prüfung
  - Auditoren, Sachverständige, Rechtsanwälte, IT-Sicherheitsbeauftragte, Wirtschaftsprüfer

- Auditierung / Zertifizierung
  - EuroCloud SaaS Star Audit
  - BSI IT-Grundschutz, ISO 27001
  - ULD Schleswig-Holstein
  - datenschutz cert, DEKRA, TÜV

// Risikoabwägung und Nebenziele //

HK2
Rechtsanwälte

Cloud-Verträge

- grenzüberschreitend -

Cloud - grenzüberschreitend

Anforderungen an die Datenübermittlung aus EU-Mitgliedstaat in Nicht-Mitglied der EU/ des EWR

1. Kein bereichsspezifisches Verbot
2. Gesetzlicher Erlaubnistatbestand oder Einwilligung des Betroffenen
3. Angemessenes Schutzniveau
   - Sicheres Drittland (z.B. Kanada, Schweiz)
   - EU Standardvertragsklauseln (EU-Model Clauses)
   - Binding Corporate Rules (BCRs)
   - *„Safe Harbor“ (nur USA) in 2014 ?!*

HK2
Rechtsanwälte

Risiken

- Vertragliche Ansprüche!
- Betroffener
  - Vertragliche Ansprüche
  - § 6 BDSG
- Datenschutzbehörden
  - § 42a BDSG Informationspflicht
  - § 43 BDSG Ordnungswidrigkeit
  - § 44 BDSG Straftat
- Imageverlust

Praxistipps

1. Prüfen: ADV oder Funktionsübertragung
2. Nutzen: Muster-ADV-Vereinbarung
3. Implementieren: Workflow zur Prüfung
4. Synchron verhandeln: AGB + ADV-Vereinbarung

HK2
Rechtsanwälte

Ausblick

HK2
Rechtsanwälte

EU Datenschutzgrundverordnung
EU NIS Richtlinie

DE Änderung des UKlaG

HK2
Rechtsanwälte

BMJ Heiko Maas
11.02.2014

„ … Auf nationaler Ebene werden wir das Gesetz über Unterlassungsklagen ändern. **Künftig bekommen Verbraucherorganisationen das Recht, bei Verstößen gegen den Datenschutz, Klage zu erheben.** […] Bis Ende April wird mein Ministerium dazu einen Referentenentwurf vorlegen. Diejenigen, die den Datenschutz und die Privatsphäre ihrer Kunden verletzen, können dann nicht länger darauf hoffen, einfach davonzukommen. Mit dem neuen Verbandsklagerecht stellen wir sicher, dass die Regeln des Datenschutzes nicht nur auf dem Papier stehen, sondern auch eingehalten werden…“

Lesetipp: Praxisleitfaden

HK2 Rechtsanwälte

Sichere Nutzung von Cloud-Anwendungen

am Beispiel des TeleTrusT – Bundesverband IT-Sicherheit e.V.

HK2
Rechtsanwälte

Karsten U. Bartels LL.M.

- Rechtsanwalt
- Leiter AG Recht, Bundesverband IT-Sicherheit e.V. – TeleTrusT
- Lehrbeauftragter der TH Wildau zum IT-Recht, Fachbereich Wirtschaft, Informatik, Recht
- Zertifizierter Datenschutzbeauftragter (TÜV)
- Externer Auditor für Managementsysteme IT Security und Datenschutz (TÜV SÜD Management Service GmbH)
- Auditor der datenschutz cert GmbH
  - Datenschutz-Gütesiegel *ips* - internet privacy standards
  - Zertifikat zur Auftragsdatenverarbeitung
  - Zertifikat für Datenschutz-Management *priventum*
- Beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein anerkannter Sachverständiger für IT-Produkte (rechtlich)
- Stellv. Vorsitzender Arge Informationstechnologie, Deutscher Anwaltverein e.V.
- Schlichter IT-Recht der IHK Berlin Schlichtungsstelle

Hausvogteiplatz 11 A
10623 Berlin
bartels@hk2.eu