BAKER & MCKENZIE

Datenschutzrecht

RA Dr. Lukas Feiler, SSCP, CIPP/E

Technische Universität Wien
14. März 2016

TOPICS

- Einführung in das Thema Datenschutz aus rechtsvergleichender Sicht
- Anwendbares Recht
- Regulatorische Anforderungen
- Outsourcing
- Aktuelle IT-Trends: BYOD, Cloud Computing & Big Data
- Datenschutzgrundverordnung

©2016 Baker & McKenzie

Datenschutz als Grundrecht in der EU

- Europäische Menschenrechtskonvention
  - Schützt Privatsphäre (Artikel 8)
- EU Grundrechtecharta
  - Schützt das Grundrecht auf Datenschutz (Artikel 8)
- Österreich: § 1 Datenschutzgesetz 2000
- Deutschland: Grundrecht auf informationelle Selbstbestimmung

©2016 Baker & McKenzie

Data Privacy nach U.S.-Recht

- Verfassungsrecht
  - 1st Amendment: Freedom of association schützt auch die Vertraulichkeit von Mitgliederlisten (NAACP v. Alabama, 357 U.S. 449 (1958)
  - 4th Amendment: Schutz vor unreasonable searches & seizures; gilt aber nur wenn “reasonable expectation of privacy” (Katz v. United States, 389 U.S. 347 (1967)) → secrecy paradigm

©2016 Baker & McKenzie

Data Privacy nach U.S.-Recht #2

- Federal law
  - Nur sektor-spezifischer Schutz in Reaktion auf konkrete Vorfälle
    - Health Insurance Portability and Accountability Act: health care providers
    - Gramm-Leach-Bliley Act: financial institutions
    - Fair Credit Reporting Act: credit reporting agencies
    - Video Privacy Protection Act: video tape service providers
  - Hauptsächlich: self-regulation
- Common law / privacy torts
  - intrusion upon seclusion → secrecy paradigm
  - public disclosure of private facts → secrecy paradigm

©2016 Baker & McKenzie

Datenschutz-Compliance

- Datenschutz-Compliance gewinnt an Wichtigkeit
  - Rechtliche Risiken: Strafen von bis zu EUR 25.000 pro Verstoß
  - Image-Risiken: Compliance-Defizite & Security Breaches gefährden Image des Unternehmens
  - Wirtschaftliche Risiken durch verlorenes Kundenvertrauen
- Jüngere Entwicklungen
  - Sicherheitsrisiken durch Geheimdienste
  - Datenschutz-Aktivisten prangern Compliance-Defizite an (zB Europe v. Facebook)
  - Datenverarbeitungsregister ist seit 1.9.2012 online

©2016 Baker & McKenzie

Der Rechtsrahmen in Österreich und der EU

- Datenschutz-Richtlinie (RL 95/46/EG)
  - nicht nur Mindeststandard, sondern Vollharmonisierung
  - unmittelbar anwendbar sofern im Einzelfall hinreichend bestimmt
- Datenschutzgesetz 2000
- Am Horizont:
  - Neue Datenschutz-Grundverordnung (KOM (2012) 11)
  - Richtlinie über die Datenverarbeitung durch Strafverfolgungsbehörden (KOM (2012) 10)

©2016 Baker & McKenzie

Was sind "personenbezogene Daten"?

Personenbezogene Daten

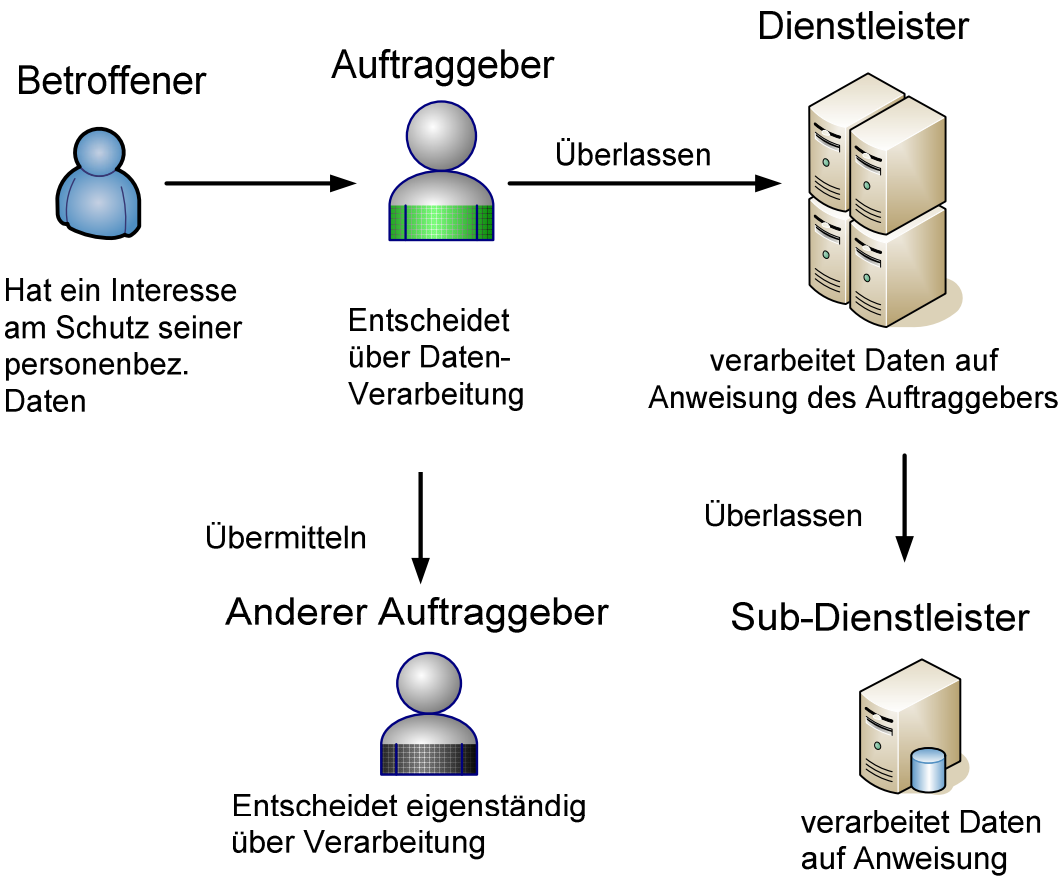
- Informationen über eine bestimmte oder bestimmbare Person
  - Es ist ausreichend, dass irgendjemand einen Personenbezug herstellen kann

Indirekt personenbezogene Daten

- wenn der Auftraggeber die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann

©2016 Baker & McKenzie

Akteure im Bereich des Datenschutzes



©2016 Baker & McKenzie

Regulierungsbehörden

- Datenschutzbehörde
- “Artikel 29-Arbeitsgruppe”
  - Besteht aus Vertretern der nationalen Behörden
  - Berät die Europäische Kommission und die nationalen Behörden

©2016 Baker & McKenzie

Nationale Datenschutz-rechte differieren – Welches Recht gilt? (Art 4)

Grundsatz: Ort der Niederlassung des Auftraggebers entscheidend

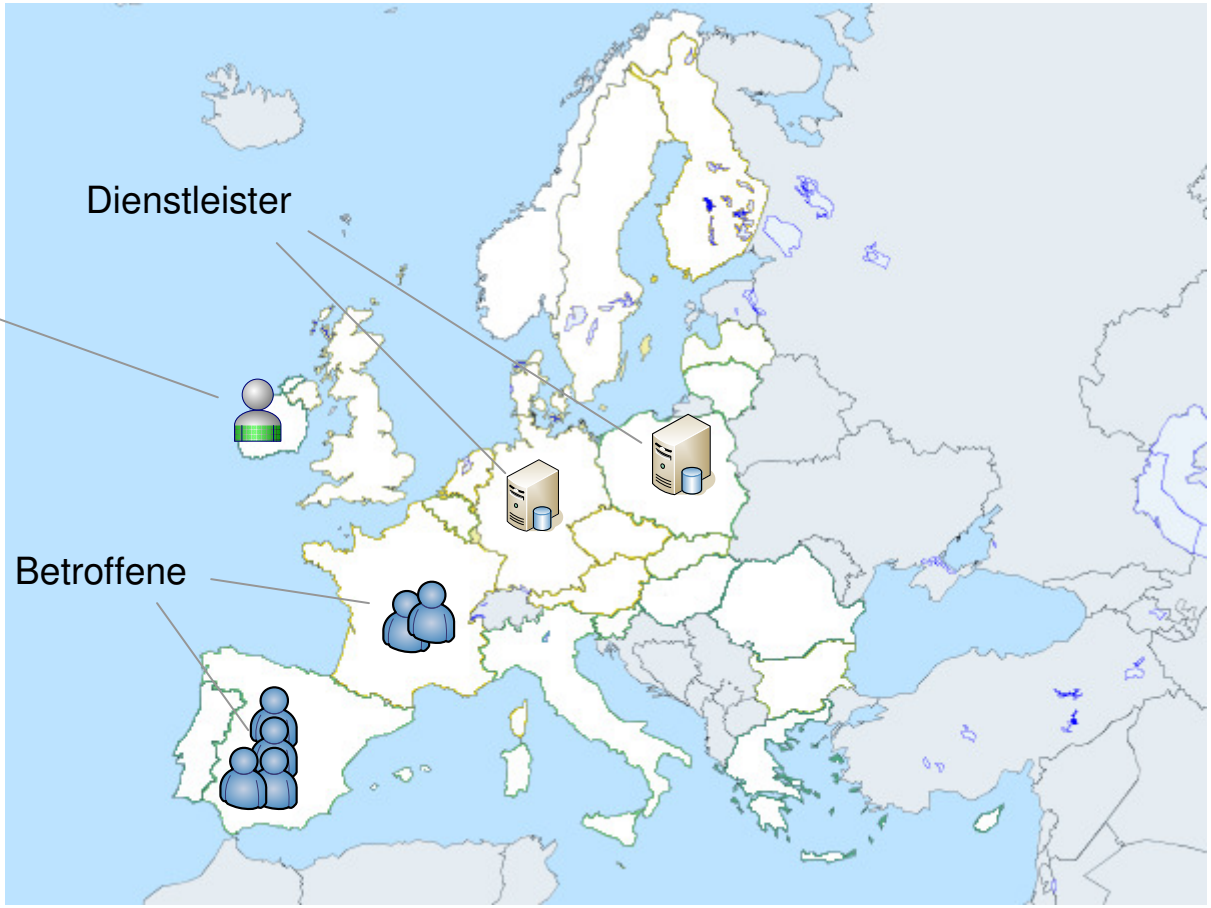
- Wenn Aufraggeber nur eine Niederlassung in der EU hat
  - zB wenn X GmbH Internet-Dienste in der ganzen EU anbietet aber nur in Österr. eine Niederlassung hat: österr. Recht gilt.
- Wenn Auftraggeber mehrere Niederlassungen in der EU hat:
  - Wenn Datenverarbeitung im Rahmen der Tätigkeiten aller Niederlassung → jede Niederlassung muss sich an lokales Recht halten
- Wenn der Auftraggeber keine Niederlassung in der EU hat:
  - Muss das Recht jener EU-Mitgliedstaaten befolgen, in denen Mittel zur Datenverarbeitung verwendet werden

©2016 Baker & McKenzie

Welches Recht gilt?
Nur eine Niederlassung in der EU

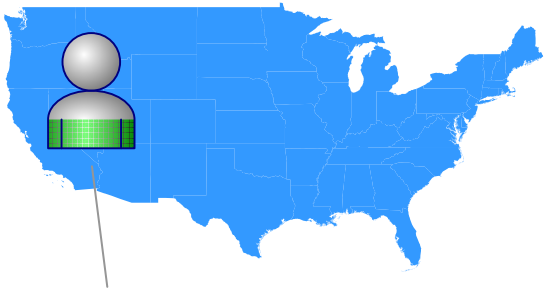
Auftraggeber
ohne sonst.
Niederlassungen

z.B.: Facebook
Ireland Ltd.

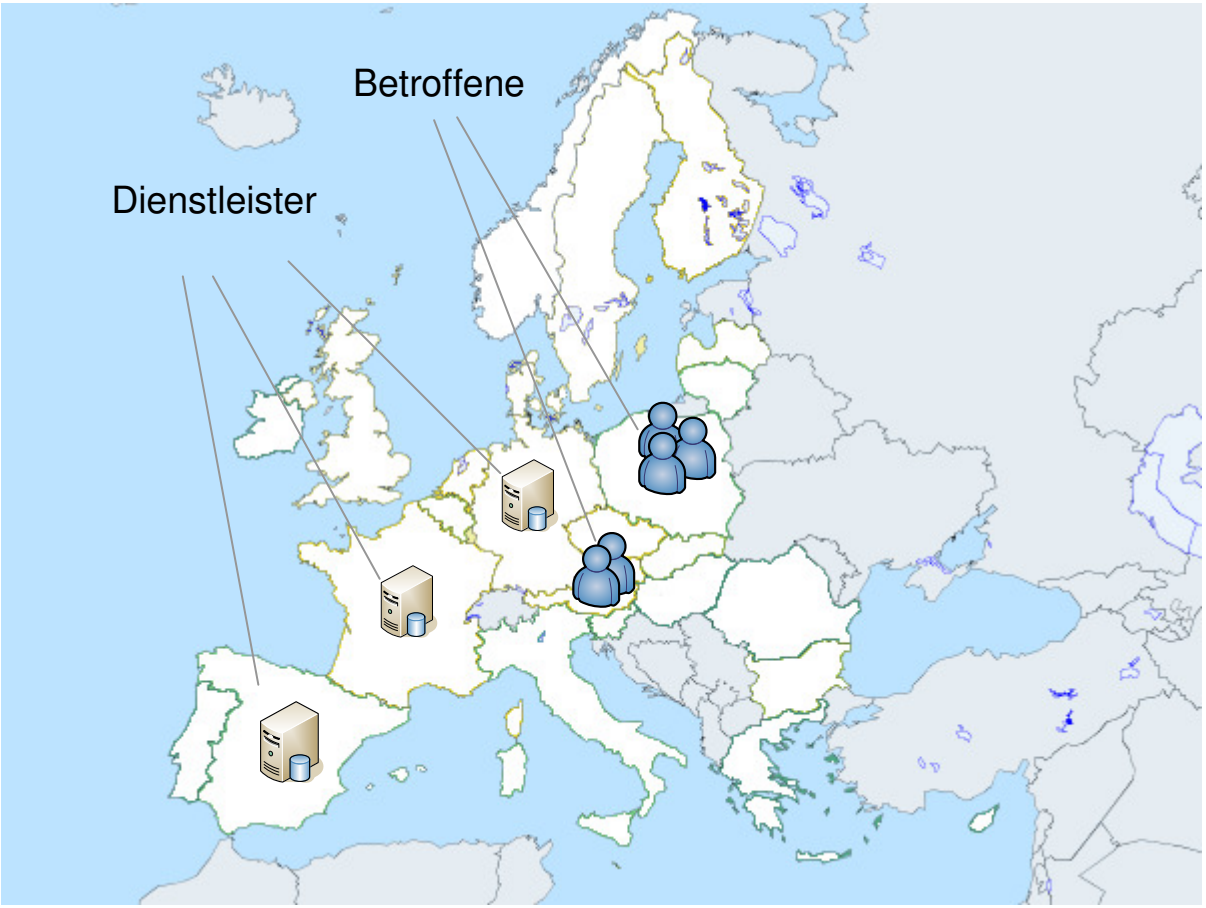


©2016 Baker & McKenzie

Welches Recht gilt?
Keine Niederlassung in der EU



Auftraggeber ohne Niederlassung in der EU



©2016 Baker & McKenzie

Zulässigkeit der Datenverarbeitung

Grundsätze:

1) Auf rechtmäßige Weise & nach Treu und Glauben
   - Erfordert arbeitsrechtliche Compliance
2) Zweckbindung: Verarbeitung nur für festgelegte eindeutige Zwecke
3) Datenminimierung: erhobene Daten müssen für die festgelegten Zwecke relevant sein
4) Richtigkeit und Aktualität: Pflicht zur Aktualisierung
5) Begrenzte Dauer: nur solange, wie für Zwecke erforderlich

©2016 Baker & McKenzie

Zulässigkeit der Datenverarbeitung #2

Personenbez. Daten dürfen nur verarbeitet werden, wenn (§ 8):

1) der Betroffene zugestimmt hat
   - Zustimmung ist widerruflich (“Right to be forgotten”)
2) zulässigerweise veröffentlichte Daten
3) indirekt personenbezogenen Daten
4) gesetzliche Ermächtigung oder Verpflichtung
5) lebenswichtige Interessen des Betroffenen
6) überwiegende berechtigte Interessen des Auftraggebers

©2016 Baker & McKenzie

Meldepflichten gegenüber nationalen Datenschutzbehörden

- AG hat Datenanwendung vor Inbetriebnahme bei der DSB zu melden (§ 18 Abs 1 DSG)
- Alle Meldungen sind öffentlich einsehbar: https://dvr.dsb.gv.at
- Meldepflicht entfällt, wenn (§ 17 Abs 2 DSG)
  - nur veröffentlichte oder nur indirekt personenbezogene Daten
  - Standard-Datenanwendung gemäß Standard- und Musterverordnung 2004; zB
    - Rechnungswesen und Logistik
    - Personalverwaltung für privatrechtliche Dienstverhältnisse

©2016 Baker & McKenzie

Vorabkontrolle

- Datenanwendung darf erst nach erfolgter Genehmigung in Betrieb genommen werden, wenn (§ 18 Abs 2 DSG)
  - Sensible Daten
  - Strafrechtlich relevante Daten
  - Auskunftserteilung über die Kreditwürdigkeit der Betroffenen
  - Informationsverbundsystems
  - Videoüberwachung (§ 50c DSG)

©2016 Baker & McKenzie

Rechte des Betroffenen

- Auskunftsrecht (§ 26 DSG)
  - Schriftlich geltend zu machen
  - über Daten, ihre Herkunft, Empfängerkreise, Zweck & Rechtsgrundlage, Namen und Adressen von Dienstleistern
  - Kein Recht auf Datenportabilität
- Recht auf Richtigstellung oder Löschung (§ 27 DSG)
  - Löschung zB wenn Zustimmung widerrufen (vgl Right to be Forgotton)
- Recht Widerspruch (§ 28 DSG)
  - Wenn Datenverwendung nicht auf Zustimmung basiert

©2016 Baker & McKenzie

Verpflichtende Datensicherheitsmaßnahmen (§ 14 DSG)

- Daten sind zu schützen vor
  - Verlust
    → Verfügbarkeit
  - zufälliger oder unrechtmäßiger Zerstörung od. Änderung
    → Integrität
  - Zugang durch Unbefugte
    → Vertraulichkeit
  - Nicht ordnungsgemäße Verwendung
    → Rechtmäßigkeit
- Sicherheitsmaßnahmen müssen unter Berücksichtigung der Kosten risikoadäquat sein

©2016 Baker & McKenzie

Verpflichtende Datensicherheitsmaßnahmen (§ 14 DSG) #2

- Jedenfalls erforderlich sind (§ 14 Abs 2 DSG)
  - Aufgabenverteilung festlegen (vgl NIST SP 800-53, AC-5)
  - Datenverwendung nur bei Anordnung des zuständigen MA
  - Belehrung aller Mitarbeiter über datenschutzrechtliche Pflichten (vgl ISO 27002, Pkt 8.2.2)
  - Regelung physischer Zutrittsberechtigung (ISO 27002, § 9.1.2)
  - Regelung der Zugriffsberechtigung auf Daten & Datenträger (vgl ISO 27002, § 11.6.1)
  - Zugriffskontrolle bei Maschinen oder Programmen (aaO)
  - Protokollierung von Zugriffen/Änderungen (ISO 27002, § 10.10)
  - Dokumentation obiger Maßnahmen (vgl ISO 27002, § 4.3)

©2016 Baker & McKenzie

Data Security
Breach Notification

- *Die Pflicht betroffene Personen von der Kompromittierung ihrer personenbezogenen Daten zu informieren.*
- Eine „Erfindung“ aus Kalifornien:
  - California Senate Bill 1386 (2002)
- Zweck:
  - Betroffene sollen reaktive Maßnahmen ergreifen können
  - Markt-Transparenz hinsichtlich Daten-Sicherheit
- Rechtsquellen in Österreich:
  - Gesetz: § 24 Abs 2a DSG 2000; § 95a TKG 2003
  - Verträge

©2016 Baker & McKenzie

Breach Notification nach DSG 2000

- § 24 Abs 2a DSG 2000: Notifikations-Pflicht, wenn:
  - Unternehmen bekannt wird, dass personenbezogene Daten „systematisch und schwerwiegend“ unrechtmäßig verwendet wurden und
  - den Betroffenen Schaden droht
- Ausnahme: wenn Notifikation nicht im Verhältnis zum geringfügigen drohenden Schaden steht
- Form der Notifikation: „in geeigneter Form“
- Zeitpunkt der Notifikation: „unverzüglich“
- Rechtsfolge der Verletzung:
  - Verwaltungsstrafe: bis zu EUR 10.000 (§ 52 Abs 2 DSG 2000)
  - Haftung für Vermögensschäden nach allgem. Zivilrecht

©2016 Baker & McKenzie

Breach Notification nach dem Vertrag

- Wenn Breach Notification in einem Vertrag nicht geregelt ist, gilt:
  - Wenn ohne Notifikation Schaden droht (sog. nebenvertragliche Schutzpflicht)
  - Betroffene sind unverzüglich zu informieren
- Rechtsfolge der Verletzung:
  - Vertragliche Haftung für Vermögensschäden

©2016 Baker & McKenzie

Outsourcing – Datenüberlassung an Dienstleister

- Auftraggeber kann sich eines Dienstleisters bedienen (§ 10 DSG)
  - Dienstleister muss ausreichende Gewähr für rechtmäßige und sichere Datenverwendung bieten → zB: ISO/IEC 27001-Zertifizierung
  - Vereinbarung muss folgende Pflichten enthalten:
    - Daten nur im Rahmen der Aufträge des AG verwenden
    - Datensicherheitsmaßnahmen gem § 14 DSG sind zu treffen
    - Sub-Dienstleister nur mit Billigung des Auftraggebers
    - Voraussetzungen für Erfüllung d. Pflichten gegenüber Betr.
    - nach Beendigung: Daten an AG übergeben oder vernichten
    - AG Informationen zur Verfügung zu stellen, die zur Kontrolle notwendig sind

©2016 Baker & McKenzie

Outsourcing an ausländische Dienstleister

- Auftragsverarbeiter in der EU
  - Keine Meldung/Genehmigung erforderlich
- Auftragsverarbeiter außerhalb der EU
  - Nur Genehmigungsfrei, wenn Drittstaat angemessenen Datenschutz bietet
    - Lt. Europ. Kommission zB Kanada, Schweiz, Israel
    - früher die USA:
      - früher Safe Harbor Program → “angemessener” Datenschutz, wenn Selbstzertifizierung des Unternehmens
      - seit 6.10.2015: Safe Harbor aufgehoben (EuGH C-362/14)
      - Ungewisse Zukunft: „Privacy Shield“

©2016 Baker & McKenzie

Outsourcing an ausländische Dienstleister #2

- Outsourcing an Auftragsverarbeiter in Drittland ohne angemessenen Datenschutz
  - Genehmigungsfrei, wenn (u.a.; § 12 Abs 3 DSG)
    - im Inland zulässigerweise veröffentlichte Daten;
    - für Empfänger nur indirekt personenbezogene Daten od.
    - Zustimmung der Betroffenen
  - Ansonsten besteht grds ein Genehmigungsvorbehalt
    - Genehmigung ist zu erteilen, wenn Dienstleister-Vertrag Standardvertragsklauseln der Europ. Kommission enthält

©2016 Baker & McKenzie

Herausforderungen durch aktuelle IT-Trends

- Bring Your Own Device (BYOD)
- Cloud Computing
- Big Data

©2016 Baker & McKenzie

Bring Your Own Device

- BYOD verringert Sicherheitsniveau erheblich:
  - Authentifizierung der Nutzer am Endgerät?
  - Patch Management?
  - Datenverschlüsselung?
- Sicherheitsniveau häufig nicht angemessen (§ 14 DSG)
  - Kompensatorische Maßnahmen nötig
  - z.B. Remote Wiping und/oder Usage Monitoring

©2016 Baker & McKenzie

Bring Your Own Device – Remote Wiping

- Szenario: Dienstnehmer verlegt (verliert?) sein Gerät mit
  - Privaten Daten (Urlaubsfotos etc.)
  - Geschäftsgeheimnissen/Kundendaten
- Darf der Arbeitgeber ohne Zustimmung des Dienstnehmers ein Remote Wiping vornehmen?
  - Problem: Datenbeschädigung strafbar (§ 126a StGB):

    Wer einen anderen dadurch schädigt, dass er Daten, über die er nicht oder nicht allein verfügen darf, löscht …

©2016 Baker & McKenzie

Bring Your Own Device – Remote Wiping #2

- Zustimmung des Dienstnehmers erforderlich
- Sollte vorab von allen Dienstnehmern schriftlich eingeholt werden
- Inhalt der Vereinbarung
  - Informationspflicht des Dienstnehmers an den Dienstgeber, wenn Endgerät verlegt/verloren
  - Voraussetzungen des Remote Wiping sind genau zu definieren

©2016 Baker & McKenzie

Cloud Computing - Zentrale Herausforderungen

- Internationale Datentransfers
  - Cloud Provider befindet sich oft in anderem Staat
  - Typischerweise sind Sub-Auftragsverarbeiter involviert
    - Software-Wartung
    - Support-Techniker
    - Zugriffsmöglichkeit durch Support-Personal gilt grds ebenso als Datentransfer

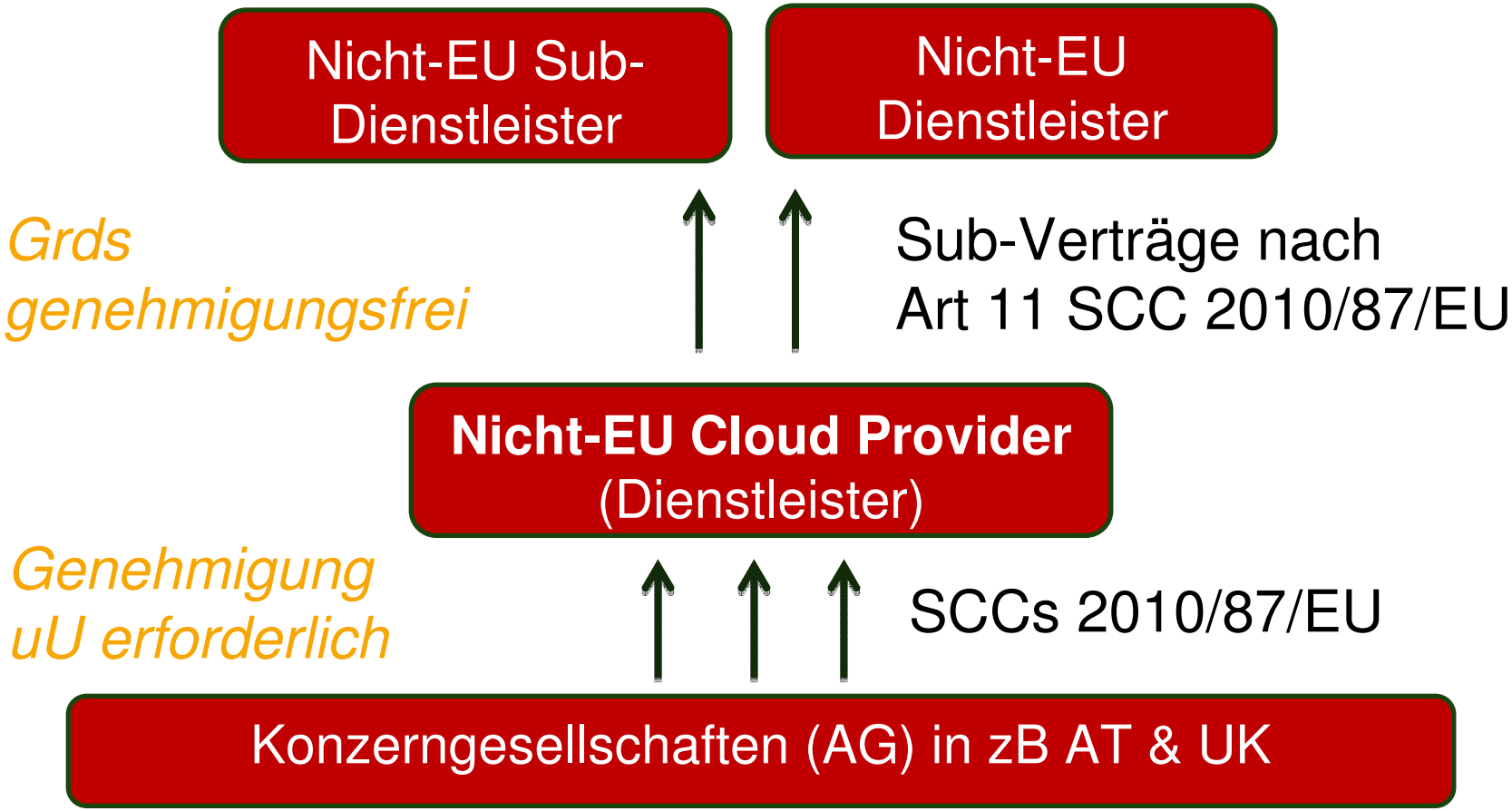
©2016 Baker & McKenzie

Cloud Computing - Zentrale Herausforderungen #2

- Vertragsstruktur bei Konzern-weiter Cloud-Nutzung
  - Zivilrechtlich: nur eine Konzerngesellschaft ist Vertragspartner
  - Datenschutzrechtlich:
    - Jede Konzerngesellschaft ist Auftraggeber nach ihrem nationalen Recht
    - Jede Konzerngesellschaft muss ein Data Processing/Transfer Agreement mit dem Cloud Provider schließen

©2016 Baker & McKenzie

Compliance-Lösung for Nicht-EU Cloud Provider & Sub-DL



©2016 Baker & McKenzie

Big Data – Big Liability?

- Big Data ist gekennzeichnet durch:
  - Die automatisierte Analyse (Data Mining) von
  - idR unstrukturierten
  - großen Datenmengen
- Anwendungsgebiete von Big Data
  - Analyse und „Vorhersage“ des Kundenverhaltens
    - Personenbezogene Werbung
    - Preisdiskriminierung
  - Optimierung betrieblicher Prozesse
    - zB Planung des Personalbedarfs
  - Risiko- und Finanzmanagement

©2016 Baker & McKenzie

Big Data – Zentrale Herausforderungen

- Anonymisierung
- Grundsatz der Zweckbindung: Verarbeitung nur für festgelegte eindeutige Zwecke & dürfen nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden

  → Speicherung auf Vorrat für undefinierte Zwecke unzulässig

  → Jede Zweckänderung kann neue Registrierungs- und Zustimmungspflichten begründen (neue Datenanwendung)
- Vollautomatisierte Entscheidungen grds unzulässig, wenn
  - rechtliche Folgen oder erhebliche Beeinträchtigung des Betroffenen &
  - Bewertung einzelner Aspekte der Person (zB Leistungsfähigkeit, Kreditwürdigkeit, Zuverlässigkeit)

©2016 Baker & McKenzie

Good News!
You're Not Paranoid - PRISM & Tempora

- Tempora – UK GCHQ
  - Total-Auswertung des Internet-Backbone-Traffics in UK
  - Rechtsgrundlage: Regulation of Investigatory Powers Act (RIPA)
  - Schranken?
    - Art 15 Abs 1 E-Privacy-RL (2002/58/EC) & Art 8 EMRK
- PRISM – U.S. NSA
  - Direkter Zugang zu Facebook, Google, Microsoft, Skype, …
  - Rechtsgrundlage: Foreign Intelligence Surveillance Act
  - Schranken?
    - 1st & 4th Amendment to the U.S. Constitution?

©2016 Baker & McKenzie

Battle of Compliance: EU- vs. U.S.-Recht

- Internationale Konzerne unterliegen meist mehreren Rechtsordnungen
- USA PATRIOT Act § 505: Mit National Security Letters kann das FBI von jedermann Auskunft begehren
  - über sämtliche Transaktionsdaten
  - ohne gerichtliche Kontrolle
  - ohne Verhältnismäßigkeitsprüfung
  - Plus: Verpflichtung zur Geheimhaltung
- Datenschutzrecht der Mitgliedstaaten
  - Eingriffe müssen verhältnismäßig sein
  - Erfordernis eines effektiven Rechtsschutzes (Art 6 EMRK)

©2016 Baker & McKenzie

Battle of Compliance: EU- vs. U.S.-Recht #2

Zum Beispiel

- Internationaler IT-Service Provider betreibt Data Center in der EU
  - EU-Datenschutzrecht gilt
- Mit Sitz in den USA unterliegt er USA PATRIOT Act § 505

→ U.S.-Recht verpflichtet zur Verletzung von EU-Recht

→ EU-Recht verpflichtet zur Verletzung von U.S.-Recht

©2016 Baker & McKenzie

Ausblick - DSGV

- Datenschutz-Grundverordnung der EU
  - Vision: Vollharmonisierung des Datenschutzrechts
  - Realität: mehr 20 Regelungszuständigkeiten für Mitgliedstaaten
  - Interne Dokumentations- und Prüfpflichten statt behördliche Meldepflichten
  - Betrieblicher Datenschutzbeauftragter
  - Strafen von bis zu 4% des Jahresumsatzes
  - Hoch komplexe Zuständigkeitsordnung (kein Konzernprivileg)
  - Keine Regelung zum anwnedbaren Recht

©2016 Baker & McKenzie

Kontakt

Baker & McKenzie
Schottenring 25
1010 Vienna
Tel.: +43 (0) 1 24 250
Fax: +43 (0) 1 24 250 600

RA Dr. Lukas Feiler, SSCP, CIPP/E
lukas.feiler@bakermckenzie.com

Die Baker & McKenzie - Partnerschaft von Rechtsanwälten, Wirtschaftsprüfern, Steuerberatern und Solicitors ist eine im Partnerschaftsregister des Amtsgerichts Frankfurt/Main unter PR-Nr. 1602 eingetragene Partnerschaftsgesellschaft nach deutschem Recht mit Sitz in Frankfurt/Main. Sie ist assoziiert mit Baker & McKenzie International, einem Verein nach Schweizer Recht. Mitglieder von Baker & McKenzie International sind die weltweiten Baker & McKenzie-Anwaltsgesellschaften. Der allgemeinen Übung von Beratungsunternehmen folgend, bezeichnen wir als "Partner" einen Freiberufler, der als Gesellschafter oder in vergleichbarer Funktion für uns oder ein Mitglied von Baker & McKenzie International tätig ist. Als "Büros" bezeichnen wir unsere Büros und die Kanzleistandorte der Mitglieder von Baker & McKenzie International.

© Baker & McKenzie