BAKER & MCKENZIE

# Datenschutzrecht in der internationalen Unternehmenspraxis

Dr. Lukas Feiler, SSCP
Baker & McKenzie

9. Dezember 2013

# TOPICS

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


©2013 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


©2013 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


©2013 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


©2013 Baker & McKenzie

# Is Privacy Dead?

- “You have zero privacy anyway, get over it”
- Milliarden von Usern haben Facebook-Profile, viele sind öffentlich
- Schätzen Konsumenten Privatsphäre?
  - Hängt vom Kontext ab!
  - “Privacy in Context”: Konsumenten sind bereit, ihre Daten in einem Kontext zu teilen, verweigern es aber in einem anderen
    - manche teilen Informationen über ihre religiösen Ansichten mit ihren Freunden, nicht aber mit Kollegen
    - Während sie Informationen über ihr Gehalt mit ihren Kollegen, nicht aber mit ihren Freunden teilen
  - Facebook: privater Kontext (Familie, Freunde, Bekannte)
  - Google+: circles replizieren “Lebenssphären”


©2013 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
- Jüngste Entwicklungen
  - “Hacktivists” machen Security Breaches publik (zB Anonymous)
  - Datenschutz-Aktivisten prangern Compliance-Defizite an (zB Europe v. Facebook)
  - Datenverarbeitungsregister ist seit 1.9.2012 online


©2013 Baker & McKenzie

# Der Rechtsrahmen in der EU

- Datenschutz-Richtlinie (DS-RL; RL 95/46/EG)
  - EuGH (C-468/10 und C-469/10):
    - nicht nur Mindeststandard, sondern Vollharmonisierung
    - unmittelbar anwendbar sofern im Einzelfall hinreichend bestimmt
- ePrivacy Directive (2002/58/EG) – gilt grundsätzlich nur für Telekommunikationsunternehmen
- Am Horizont:
  - Neue Datenschutz-Grundverordnung (KOM (2012) 11)
  - Richtlinie über die Datenverarbeitung durch Strafverfolgungsbehörden (KOM (2012) 10)


©2013 Baker & McKenzie

# Was sind “personenbezogene Daten”?

Personenbezogene Daten

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

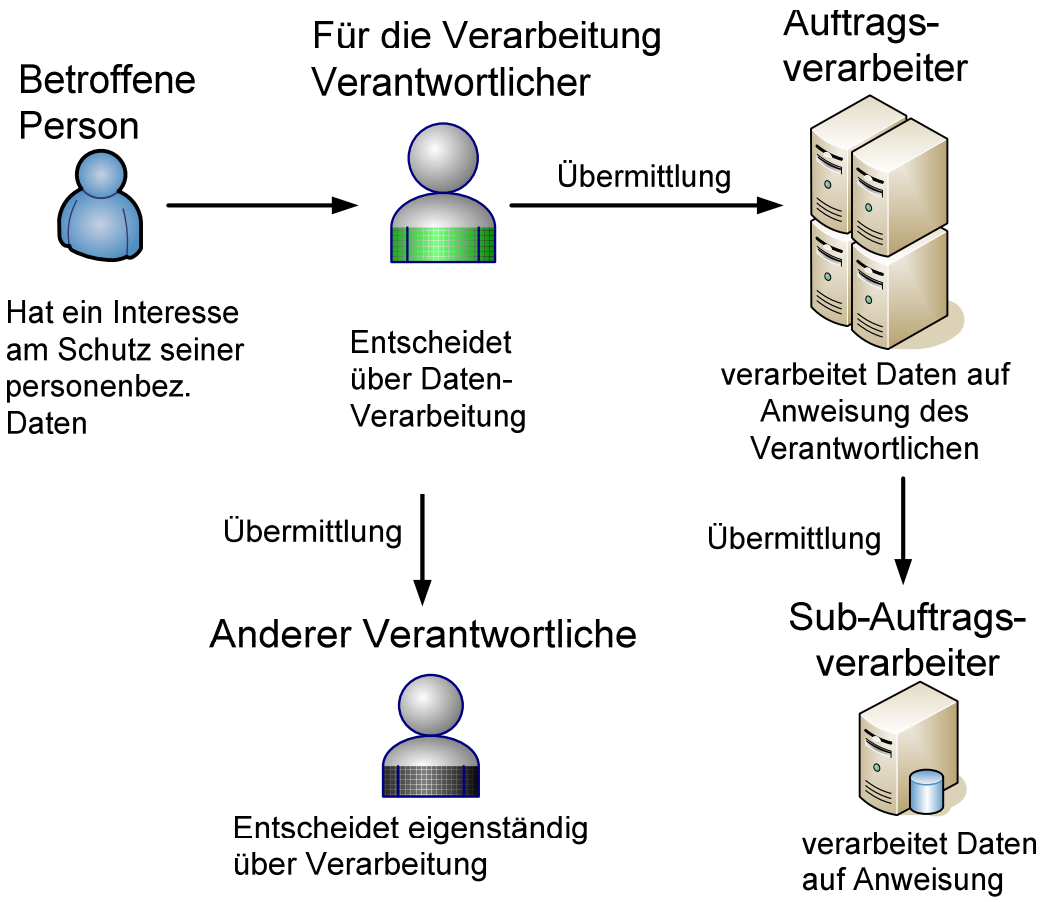

©2013 Baker & McKenzie

# Akteure im Bereich des Datenschutzrechts (Art 4 DS-RL)

- Betroffene Person (Betroffener)
  - natürliche Personen, deren Daten verwendet werden (in Ö: auch juristische Personen)
- Für die Verarbeitung Verantwortlicher (Verantwortlicher)
  - Personen, die allein oder gemeinsam über Zwecke und Mittel der Datenverarbeitung entscheiden
  - unabhängig davon, ob sie die Daten selbst verarbeiten oder damit einen Auftragsverarbeiter beauftragen
- Auftragsverarbeiter
  - Personen, die Daten im Auftrag des Verantwortlichen verarbeiten → Service Provider


©2013 Baker & McKenzie

# Akteure im Bereich des Datenschutzes





©2013 Baker & McKenzie

# Regulierungsbehörden

- Nationale Aufsichtsbehörden
  - EU-Datenschutzrecht wird ausschließlich von nationalen Behörden vollzogen (Art 28 DS-RL)
- European Data Protection Supervisor (EDPS)
  - Überwacht Einhaltung des Datenschutzes durch EU-Institutionen
  - Berät EU-Institutionen in legislativen Angelegenheiten
- “Art 29 Working Party”
  - Besteht aus Vertretern der nationalen Behörden
  - Berät die Europäische Kommission und die nationalen Behörden


©2013 Baker & McKenzie

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

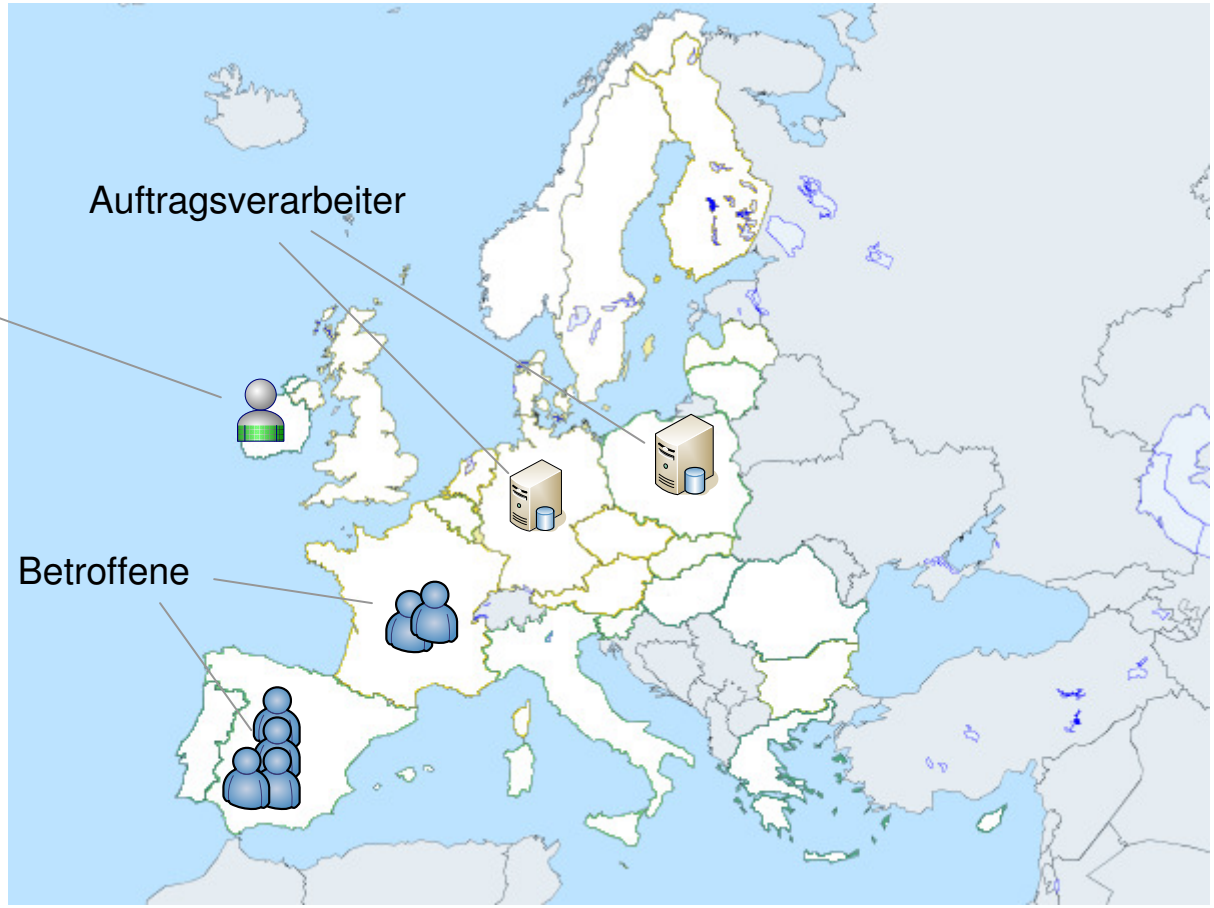
- Grundsatz: Ort der Niederlassung des Verantwortlichen ist entscheidend
  - zB wenn X GmbH Internet-Dienste in der ganzen EU anbietet aber nur in Österr. eine Niederlassung hat: österr. Recht gilt.
- Wenn Verantwortlicher mehrere Niederlassungen in der EU hat:
  - Im Rahmen der Tätigkeiten welcher Niederlassung erfolgt die Datenverarbeitung?
  - zB EU-weit operierendes Unternehmen implementiert eine CRM-Lösung für alle seine Niederlassungen in der EU → jede Niederlassung muss sich an lokales Recht halten
- Wenn der Verantwortliche keine Niederlassung in der EU hat:
  - Muss das Recht jener EU-Mitgliedstaaten befolgen, in denen Mittel zur Datenverarbeitung verwendet werden


©2013 Baker & McKenzie

# Welches Recht gilt?
# Nur eine Niederlassung in der EU

Verantwortlicher ohne sonst. Niederlassungen

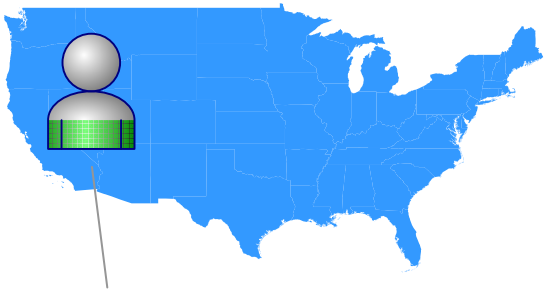
z.B.: Facebook Ireland Ltd.



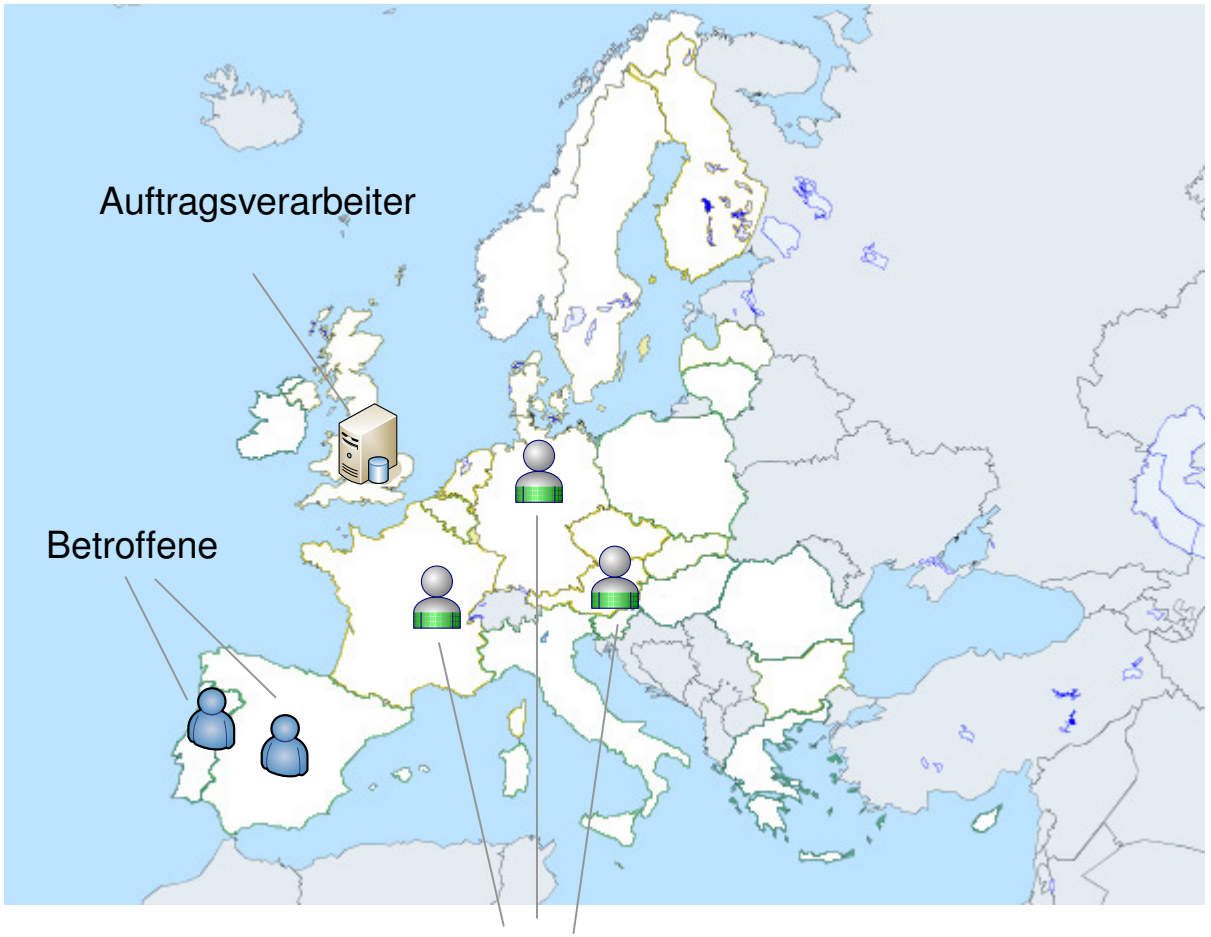


©2013 Baker & McKenzie

# Welches Recht gilt?
# Mehrere Niederlassungen in der EU



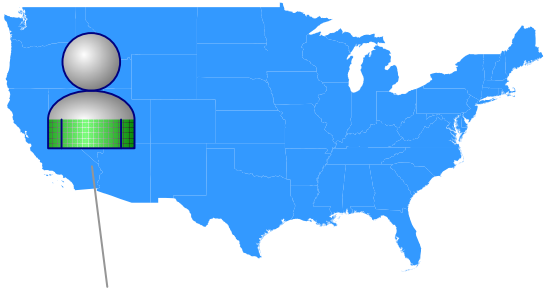
Verantwortlicher mit 3 Niederlassungen in der EU



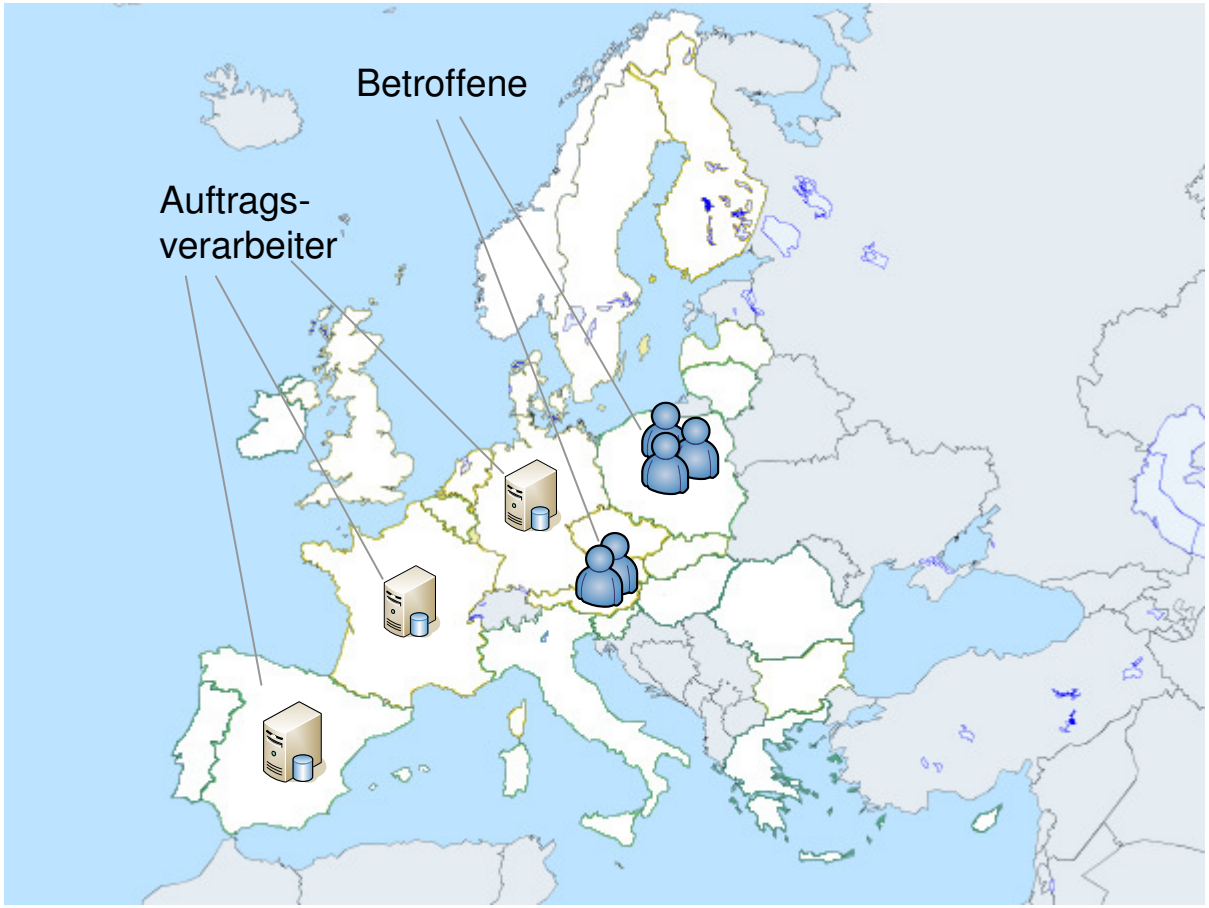


©2013 Baker & McKenzie

# Welches Recht gilt?
# Keine Niederlassung in der EU



Verantwortlicher
ohne Niederlassung
in der EU





©2013 Baker & McKenzie

# Zulässigkeit der Datenverarbeitung

Grundsätze:

1) Auf rechtmäßige Weise & nach Treu und Glauben
   - Erfordert in manchen Mitgliedstaaten zB 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


©2013 Baker & McKenzie

# Zulässigkeit der Datenverarbeitung #2

Personenbez. Daten dürfen nur verarbeitet werden, wenn (Art 7):

1) der Betroffene zugestimmt hat
   - Ist Zustimmung widerruflich? (“Right to be forgotten”)
2) für Vertragserfüllung erforderlich
3) Erfüllung rechtlicher Verpflichtungen des Verantwortlichen
4) Lebenswichtige Interessen des Betroffenen
5) Erforderlich für Wahrnehmung im öffentlichen Interesse
6) überwiegende berechtigte Interessen des Verantwortlichen


©2013 Baker & McKenzie

# Zulässigkeit der Verarbeitung sensibler Daten

Besondere Kategorien personenbezogener Daten (sensible Daten)

- rassische und ethnische Herkunft,
- politische Meinung,
- Gewerkschaftszugehörigkeit,
- religiöse oder philosophische Überzeugung,
- Gesundheit
- Sexualleben

Eingeschränkte Zulässigkeit der Verarbeitung; insb:

- „überwiegende berechtigte Interessen des Verantwortlichen“ nicht ausreichend
- Zustimmung des Betroffenen muss in vielen MS ausdrücklich sein


©2013 Baker & McKenzie

# Meldepflichten gegenüber nationalen Datenschutzbehörden

- Verantwortlicher hat Verarbeitung der Datenschutzbehörde vor Inbetriebnahme zu melden (Art 18)
- Meldung muss enthalten (Art 19)
  - Name und Anschrift des Verantwortlichen
  - Zweck der Datenverarbeitung
  - Kreis der Betroffenen & Datenkategorien
  - Kreise der Übermittlungsempfänger
  - Allgemeine Beschreibung der Datensicherheitsmaßnahmen
- Meldungen sind öffentlich einsehbar
  - zB in Österreich: https://dvr.dsk.gv.at


©2013 Baker & McKenzie

# Ausnahmen von der Meldepflicht

Mitgliedstaaten *können* Ausnahmen vorsehen für

- Bestimmte Datenkategorien & Verarbeitungszwecke
  → zB in Österr gem Standard- und Musterverordnung 2004
- Sofern der Verantwortliche einen betrieblichen Datenschutzbeauftragten bestellt
  - dieser muss Einhaltung des Datenschutzrechts überwachen und internes Register führen
  - Datenschutzbeauftragter genießt vollständige Unabhängigkeit

  → zB in Deutschland gem § 4f BDSG


©2013 Baker & McKenzie

# Vorabkontrolle

- Besonders riskante Datenverarbeitungen dürfen erst nach erfolgter Genehmigung in Betrieb genommen werden (Art 20)
  - Welche Datenverarbeitungen das sind, bestimmt jeder Mitgliedstaat
  - zB in Österreich insb:
    - Sensible Daten
    - Strafrechtlich relevante Daten


©2013 Baker & McKenzie

# Rechte des Betroffenen

- Auskunft (Art 12 lit a)
  - darüber, ob Daten des Betroffenen verarbeitet werden
  - welche Datenkategorien für welche Zwecke verarbeitet werden
  - Empfänger oder Kategorien von Empfängern
  - über die tatsächlichen Daten selbst „in verständlicher Form“
    → data portability?
  - über die Herkunft der Daten
- Berichtigung, Löschung oder Sperrung (Art 12 lit b)
  - Wenn unrichtig bzw. rechtswidrig gespeichert
- Widerspruch (Art 14)
  - Wenn Verarbeitung nicht auf Zustimmung beruht


©2013 Baker & McKenzie

# Verpflichtende Datensicherheitsmaßnahmen (Art 17)

- 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


©2013 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 der EU:
  - ePrivacy Directive
  - Nationales Recht: AT: § 24 DSG; DE: § 42a BDSG
  - Verträge


©2013 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


©2013 Baker & McKenzie

# Breach Notification nach BDSG

- § 42a BDSG: Notifikations-Pflicht, wenn:
  - Dritten unrechtmäßig zur Kenntnis gelangt sind
  - es drohen schwerwiegende Beeinträchtigungen
  - Gilt nur für:
    - Sensible Daten
    - Daten, die einem Berufsgeheimnis unterliegen
    - Daten, die sich auf strafbarer Handlungen beziehen
    - Daten zu Bank- oder Kreditkartenkonten
- Aufsichtsbehörde ist unverzüglich zu informieren
- Betroffene sind  unverzüglich zu informieren; wenn unverhältnismäßig: in mindestens zwei bundesweit erscheinenden Tageszeitungen


©2013 Baker & McKenzie

# Outsourcing – Datenübermittlung an Auftragsverarbeiter

- Verantwortlicher kann sich zur Datenverarbeitung eines Auftragsverarbeiters bedienen
  - Auftragsverarbeiter muss ausreichende Gewähr für rechtmäßige und sichere Datenverwendung bieten (Art 17 Abs 2) → zB: ISO/IEC 27001-Zertifizierung
  - Datenübermittlung muss durch Vertrag geregelt sein (Art 17 Abs 3), wonach
    - Daten nur im Rahmen der Aufträge des Verantwortlichen verarbeitet werden dürfen
      - in manchen MS: Vetorecht bei Sub-Auftragsverarbeitern
    - angem. Sicherheitsmaßnahmen zu implementieren sind
    - zu Beweiszwecken schriftlich


©2013 Baker & McKenzie

# Outsourcing an ausländische Auftragsverarbeiter

- Auftragsverarbeiter in der EU
  - Grds keine Meldung/Genehmigung erforderlich
- Auftragsverarbeiter außerhalb der EU
  - Nur Genehmigungsfrei, wenn Drittstaat angemessenen Datenschutz bietet (Art 25)
    - Lt. Europ. Kommission zB Kanada, Schweiz, Israel
    - und die USA:
      - Safe Harbor Program
      - "angemessener" Datenschutz, wenn
        - Sich der Auftragsverarbeiter nach Safe Harbor selbst-zertifiziert hat → safeharbor.export.gov/list.aspx
        - Rechtsdurchsetzung: FTC Act § 5


©2013 Baker & McKenzie

# Outsourcing an ausländische Auftragsverarbeiter #2

- Outsourcing an Auftragsverarbeiter in Drittland ohne angemessenen Datenschutz
  - Genehmigungsfrei, wenn (u.a.; Art 26 Abs 2)
    - Zustimmung der Betroffenen
    - Zur Erfüllung eines Vertrages mit dem Betroffenen
    - im Inland zulässigerweise veröffentlichte Daten
  - Ansonsten besteht grds ein Genehmigungsvorbehalt
    - Genehmigung ist zu erteilen, wenn Dienstleister-Vertrag Standardvertragsklauseln der Europ. Kommission enthält (Art 26 Abs 2 iVm Abs 4)
    - In vielen Mitgliedstaaten: genehmigungsfrei, wenn Standardvertragsklauseln verwendet (nicht in Österreich)


©2013 Baker & McKenzie

# Herausforderungen durch aktuelle IT-Trends

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


©2013 Baker & McKenzie

# Bring Your Own Device

- BYOD verringert Sicherheitsniveau erheblich:
  - Authentifizierung der Nutzer am Endgerät?
  - Patch Management?
  - Datenverschlüsselung?
- Sicherheitsniveau häufig nicht angemessen (Art 17)
  - Kompensatorische Maßnahmen nötig
  - z.B. Remote Wiping und/oder Usage Monitoring


©2013 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 in allen Mitgliedstaaten strafbar (2005/222/JI bzw RL 2013/40/EU)
  - zB § 126a öStGB:

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


©2013 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


©2013 Baker & McKenzie

# Bring Your Own Device – Usage Monitoring

- Frühzeitige Missbrauchserkennung durch Usage Monitoring, z.B.:
- Inhalt der Vereinbarung
  - GPS Tracking
  - Traffic Monitoring
  - Überwachung der Verwendung lokaler Apps
- Datenschutz im Arbeitsverhältnis
  - zB in Österreich: da Menschenwürde „berührt“ ist:
    - Zustimmung des Betriebsrats erforderlich, sofern einer vorhanden (§ 96 ArbVG)
    - Wenn kein Betriebsrat: Individualvereinbarungen mit jedem Arbeitnehmer (§ 10 AVRAG)


©2013 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

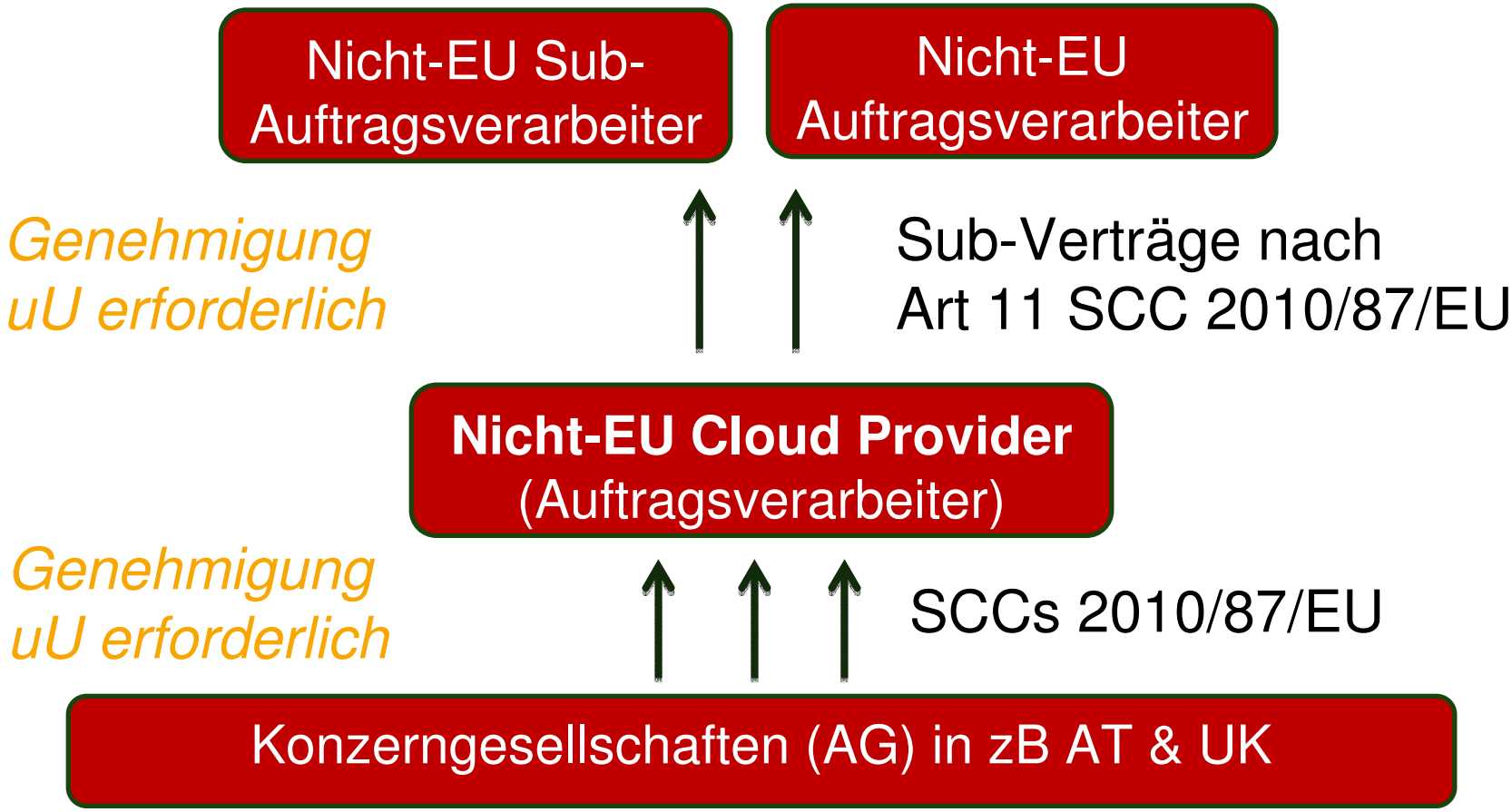

©2013 Baker & McKenzie

# 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


©2013 Baker & McKenzie

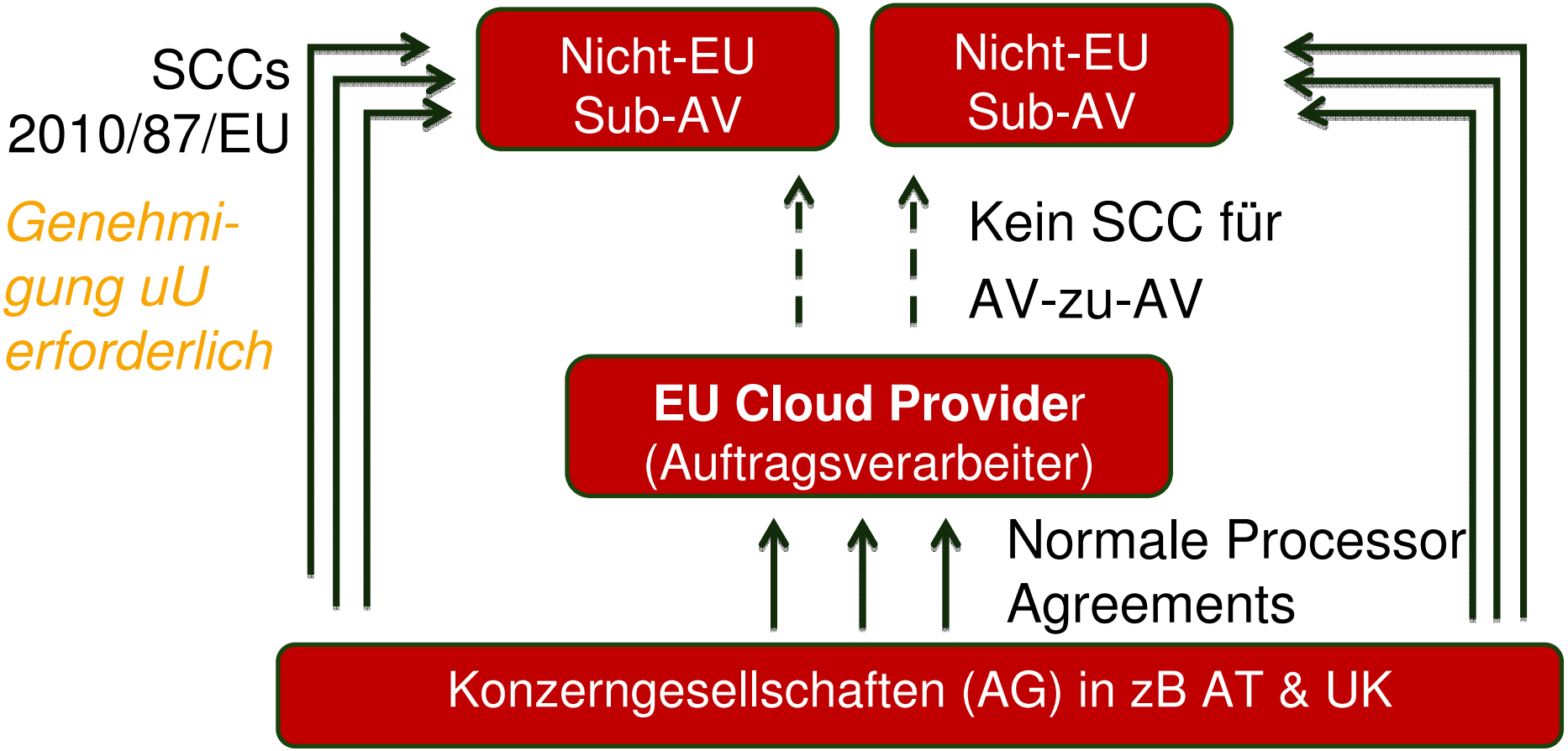
# Compliance-Lösung for Nicht-EU Cloud Provider & Sub-Auftragsv.





©2013 Baker & McKenzie

# Compliance-Lösung für EU Cloud Provider & Sub-Auftragsverarb.





©2013 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


©2013 Baker & McKenzie

# Big Data – Zentrale Herausforderungen

- 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 (Art 15): grds unzulässig, wenn
  - rechtliche Folgen oder erhebliche Beeinträchtigung des Betroffenen und
  - Bewertung einzelner Aspekte der Person (zB Leistungsfähigkeit, Kreditwürdigkeit, Zuverlässigkeit)


©2013 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?


©2013 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)


©2013 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


©2013 Baker & McKenzie

# Ausblick

- Datenschutz-Grundverordnung der EU
  - einheitliches Datenschutzrecht in allen Mitgliedstaaten
  - Weitgehender Entfall von Meldepflichten (betrieblicher Datenschutzbeauftragte)
  - Vereinfachte Konzern-interne Datenübermittlungen, sofern Binding Corporate Rules
  - Strafen von bis zu 2% des Jahresumsatzes
  - Streitpunkte:
    - Zustimmung grds erforderlich?
    - Welche nationale Behörde soll zuständig sein?
    - Höhe der Strafen
    - Anti-NSA-Bestimmung


©2013 Baker & McKenzie

# Kontakt

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

**Dr. Lukas Feiler, SSCP**
**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