

# Das EU-Datenschutzrecht

Dr. Lukas Feiler, SSCP  
Baker & McKenzie

22.6. 2013



# TOPICS

- Einführung in das Thema Datenschutz aus rechtsvergleichender Sicht
- Rollen und Verantwortlichkeiten
- Anwendbares Recht
- Regulatorische Anforderungen
- Outsourcing

# Datenschutz als Grundrecht in der EU

- Europäische Menschenrechtskonvention
  - Schützt Privatsphäre (Artikel 8)
- EU Grundrechtscharte
  - Schützt das Grundrecht auf Datenschutz (Artikel 8)

# 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

# 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

# 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)

# Was sind “personenbezogene Daten”?

## Personenbezogene Daten

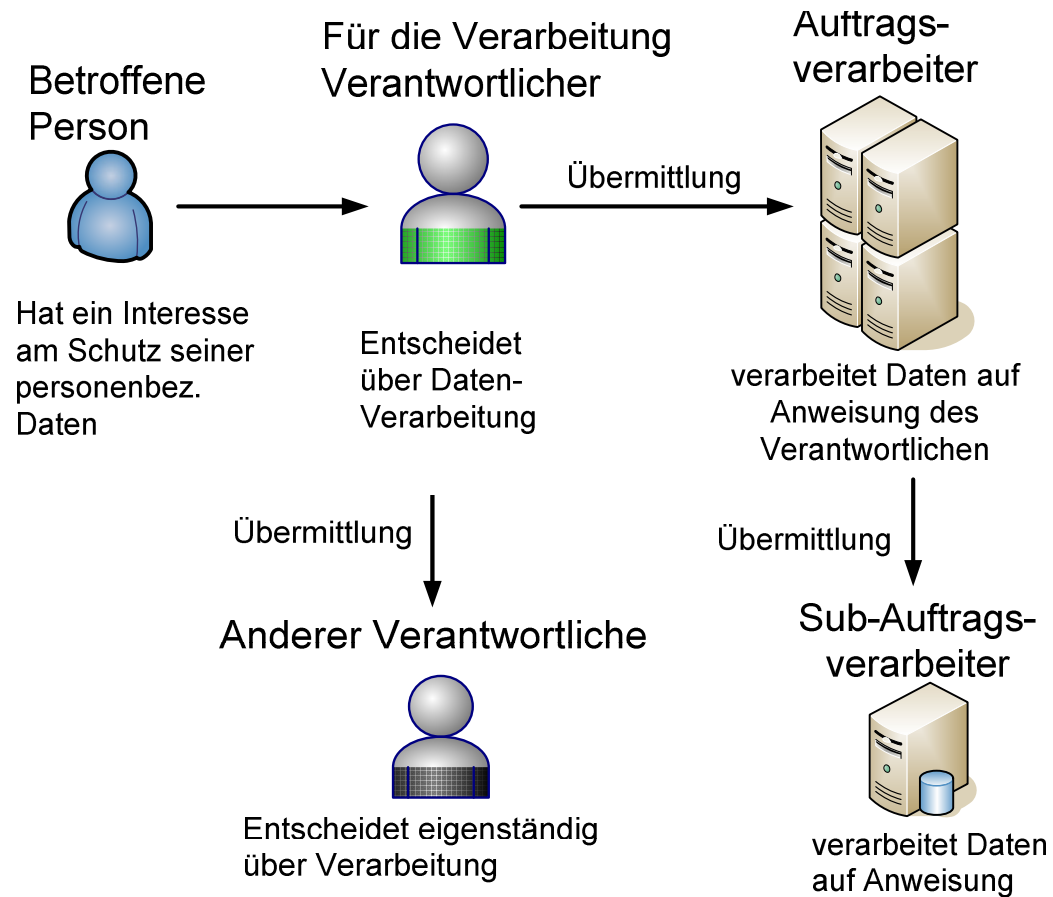
- Informationen über eine bestimmte oder bestimmbare Person
  - Es ist ausreichend, dass irgendjemand einen Personenbezug herstellen kann

# 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



# Akteure im Bereich des Datenschutzes



# 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

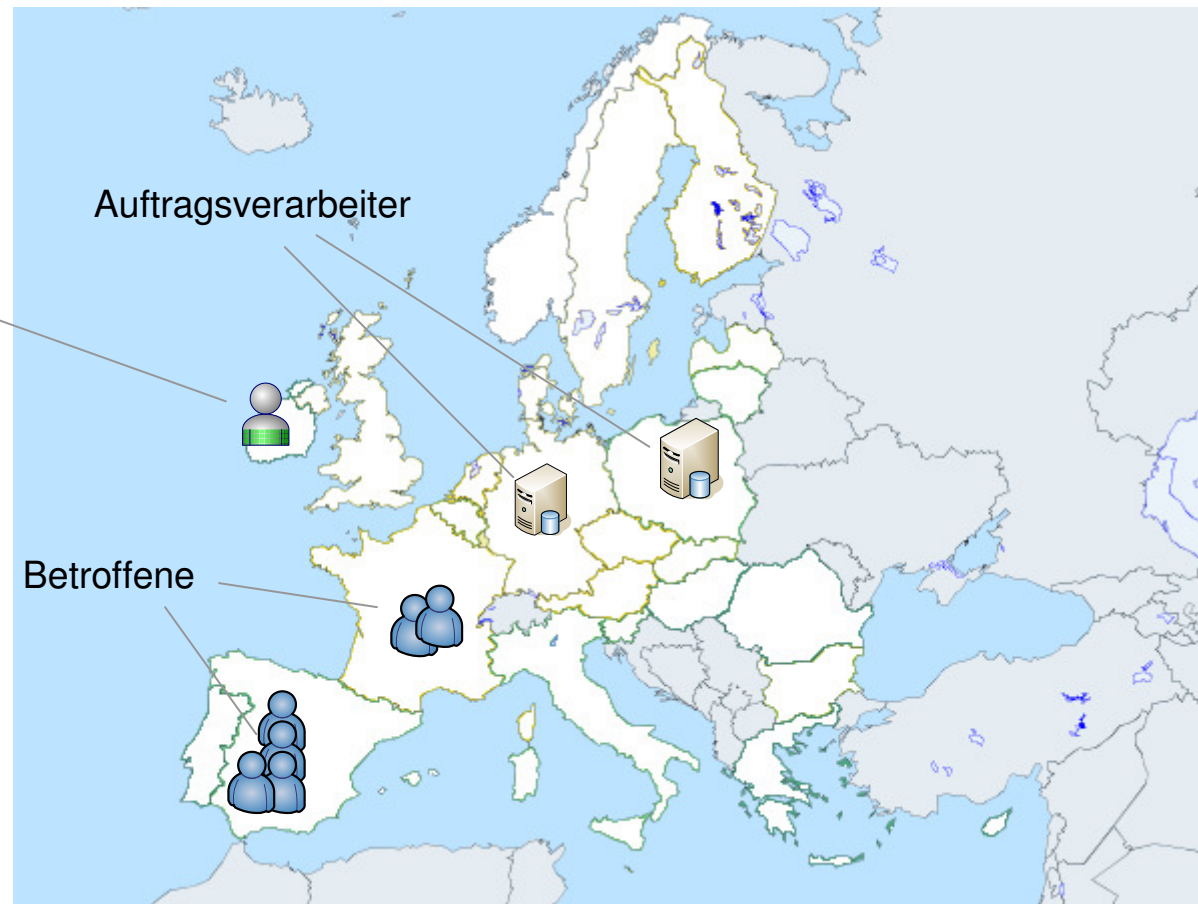
# Nationale Datenschutzrechte differieren – Welches Recht gilt? (Art 4)

- 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

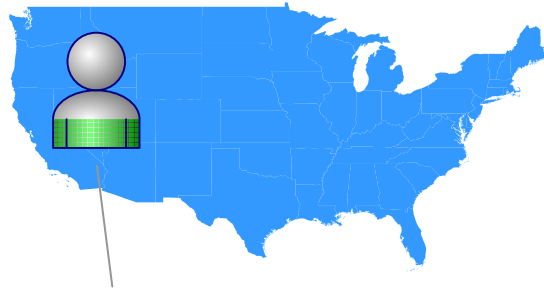
# Welches Recht gilt? Nur eine Niederlassung in der EU

Verantwortlicher  
ohne sonst.  
Niederlassungen

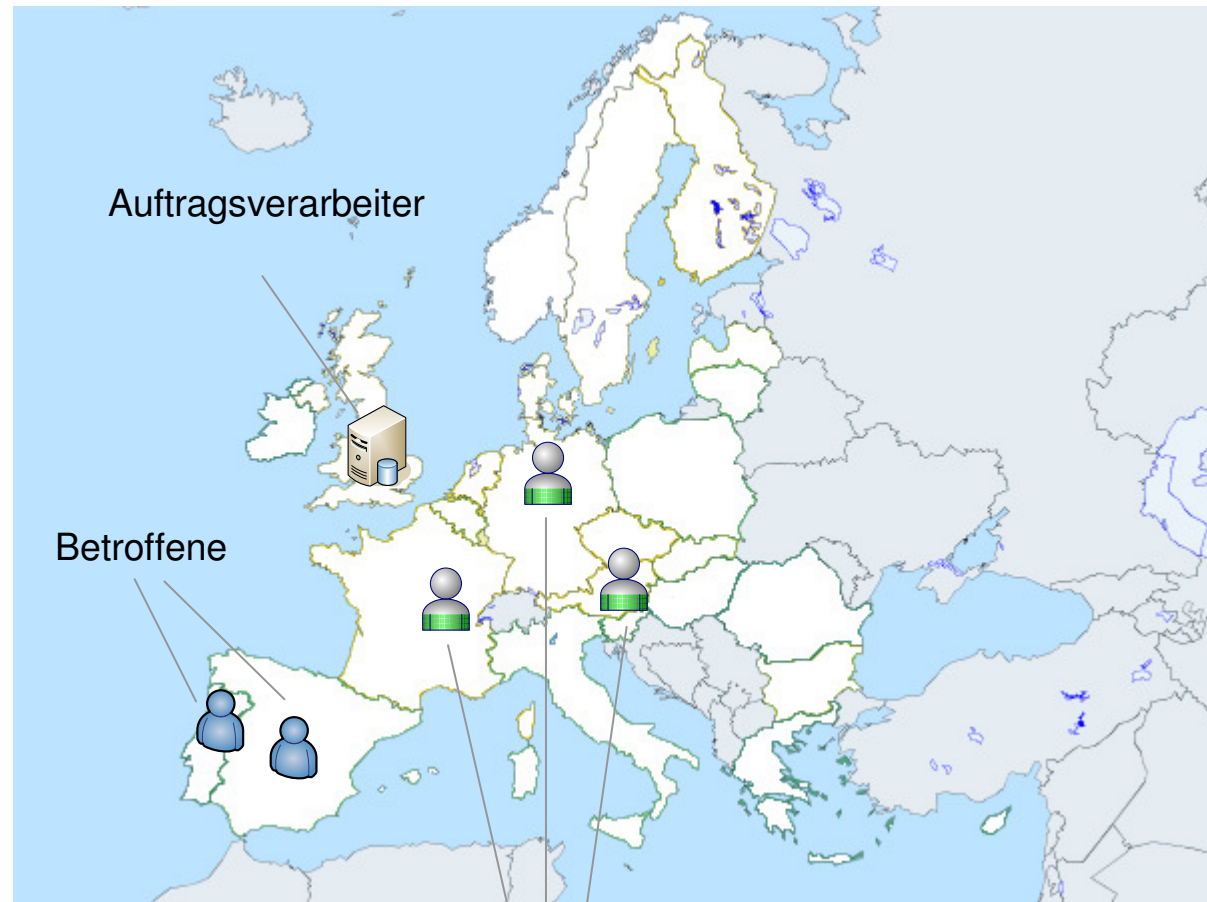
z.B.: Facebook  
Ireland Ltd.



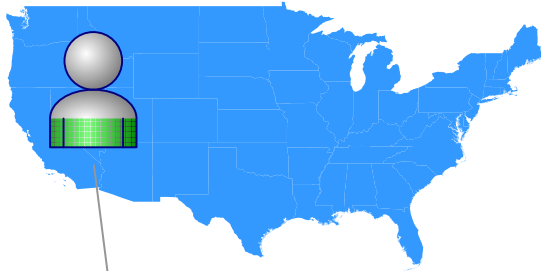
# Welches Recht gilt? Mehrere Niederlassungen in der EU



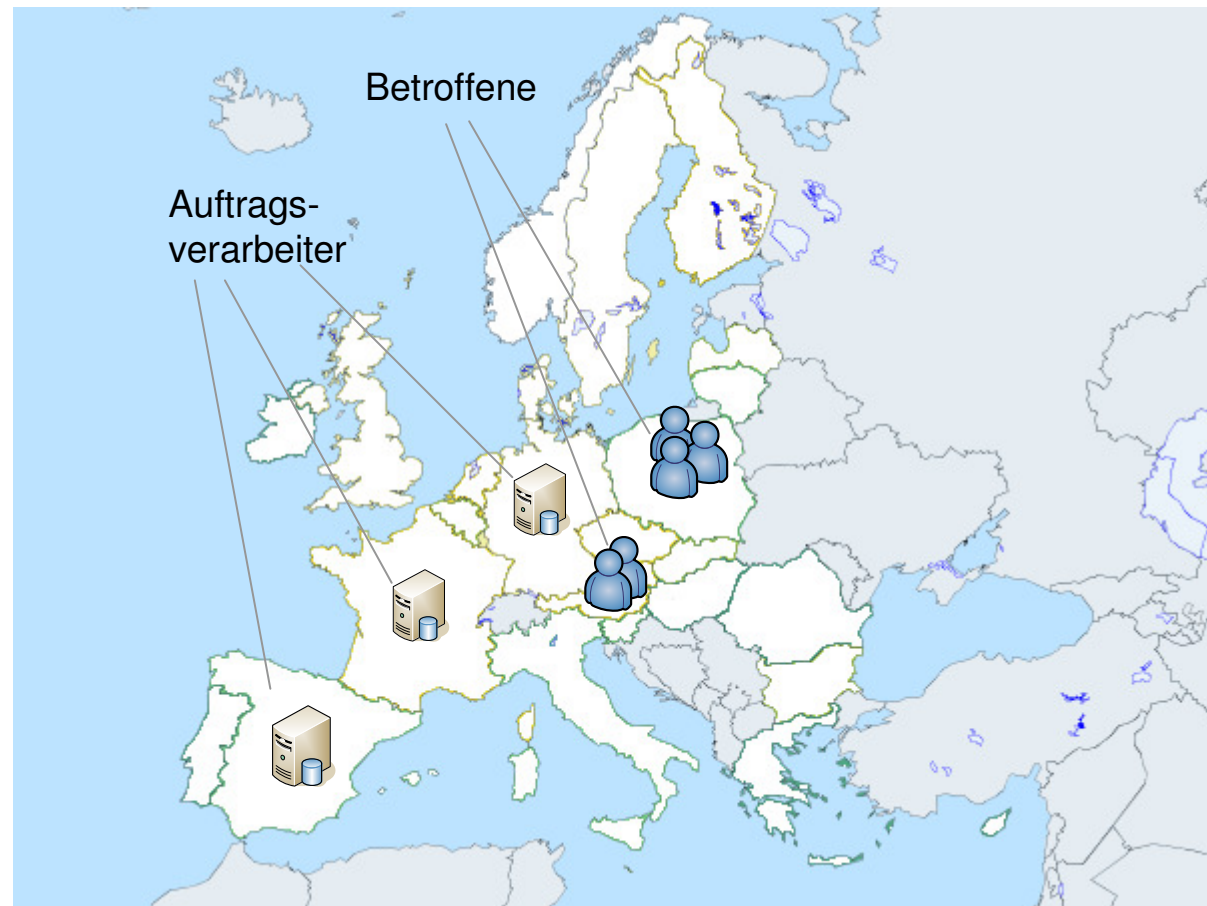
Verantwortlicher mit 3  
Niederlassungen in  
der EU



# Welches Recht gilt? Keine Niederlassung in der EU



Verantwortlicher  
ohne Niederlassung  
in der EU



# Zulässigkeit der Datenverarbeitung

Grundsätze:

- 1) Auf rechtmäßige Weise & nach Treu und Glauben
- 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

# 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 berechnigte Interessen des Verantwortlichen



# Zulässigkeit der Verarbeitung sensibler Daten

Besondere Kategorien personenbezogener Daten (sensible Daten)

- rassistische 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 ausdrücklich sein

# 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>

# 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

# 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

# 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

# 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)
  - Datenübermittlung muss durch Vertrag geregelt sein (Art 17 Abs 3), wonach
    - Daten nur im Rahmen der Aufträge des Verantwortlichen verarbeitet werden dürfen
    - angemessene Sicherheitsmaßnahmen zu implementieren sind
    - zu Beweis Zwecken schriftlich

# 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](http://safeharbor.export.gov/list.aspx)
        - Rechtsdurchsetzung: FTC Act § 5

# 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)



# 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:
    - Was sind personenbezogene Daten?
    - Zustimmung grds erforderlich?
    - Welche nationale Behörde soll zuständig sein?
    - Höhe der Strafen

# 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?

# 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)

# 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

# Is Privacy Dead?

- “You have zero privacy anyway, get over it”
- Milliarden von Usern haben Facebook-Profilen, 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 (oder Behörden)
    - 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”

## 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](mailto: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.