BAKER & MCKENZIE

Grundlagen des Datenschutzrechts

RA Dr. Lukas Feiler, SSCP, CIPP/E
Baker & McKenzie

KU Grundlagen des Technologierechts II
10.3.2015

Datenschutz - Inhalt

- Wozu Datenschutzrecht?
- Zulässigkeitsprüfung
- Datensicherheit & Breach Notification
- Meldepflichten gegenüber der DSB
- Outsourcing innerhalb und außerhalb der EU
- Whistleblowing, Compliance-Untersuchungen und Videoüberwachung
- Sanktionen

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

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 oder Big Brother Awards)
  - Datenverarbeitungsregister ist seit 1.9.2012 online für jedermann einsehbar

Der Rechtsrahmen in der EU

- Datenschutz-Richtlinie (RL 95/46/EG)
- ePrivacy Directive (2002/58/EG) – gilt grundsätzlich nur für Telekommunikationsunternehmen
- Am Horizont: neue Datenschutz-Grundverordnung der EU

Datenschutz als Grundrecht

- Europäische Menschenrechtskonvention
  - Schützt Privatsphäre (Artikel 8)
- EU Grundrechtscharta
  - Schützt das Grundrecht auf Datenschutz (Artikel 8)
- Österreich: § 1 Datenschutzgesetz 2000
- USA
  - 4. Verfassungszusatz: Schutz vor unreasonable searches & seizures; gilt aber nur wenn “reasonable expectation of privacy” (Katz v. United States, 389 U.S. 347 (1967))
    → secrecy paradigm

Was sind “personenbezogene Daten”?

Personenbezogene Daten

– Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist

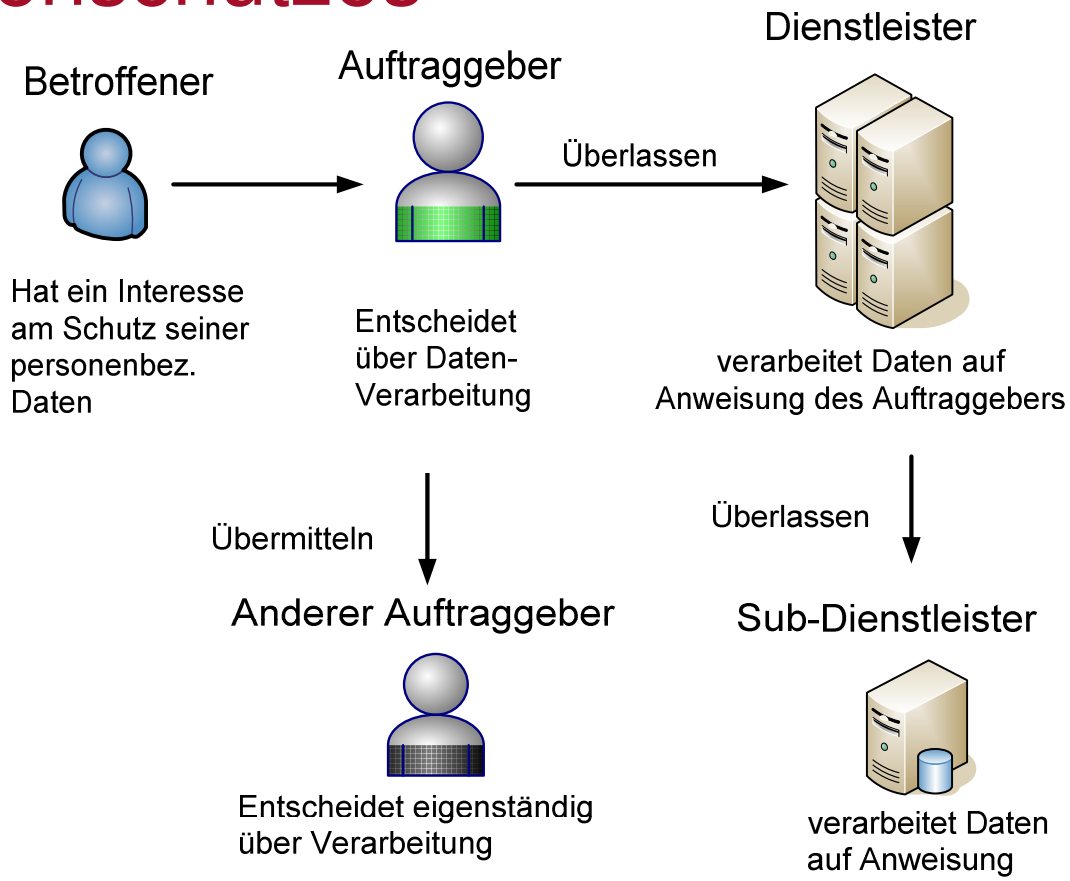
Indirekt personenbezogene Daten

– wenn der Auftraggeber die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann
  – “personenbezogen” ist ein relativer Begriff
  – Daten können für ein Unternehmen direkt und für ein anderes nur indirekt personenbezogen sein

Akteure im Bereich des Datenschutzrechts

- Betroffene
  - natürliche oder juristische Personen oder Personengemeinschaften, deren Daten verwendet werden
- Auftraggeber
  - Personen, die allein oder gemeinsam mit anderen die Entscheidung getroffen haben, Daten zu verwenden
  - unabhängig davon, ob sie die Daten selbst verwenden oder damit einen Dienstleister beauftragen
- Dienstleister
  - Personen, die Daten nur zur Herstellung eines ihnen aufgetragenen Werkes für einen anderen verwenden
- Datenschutzbehörde (DSB)

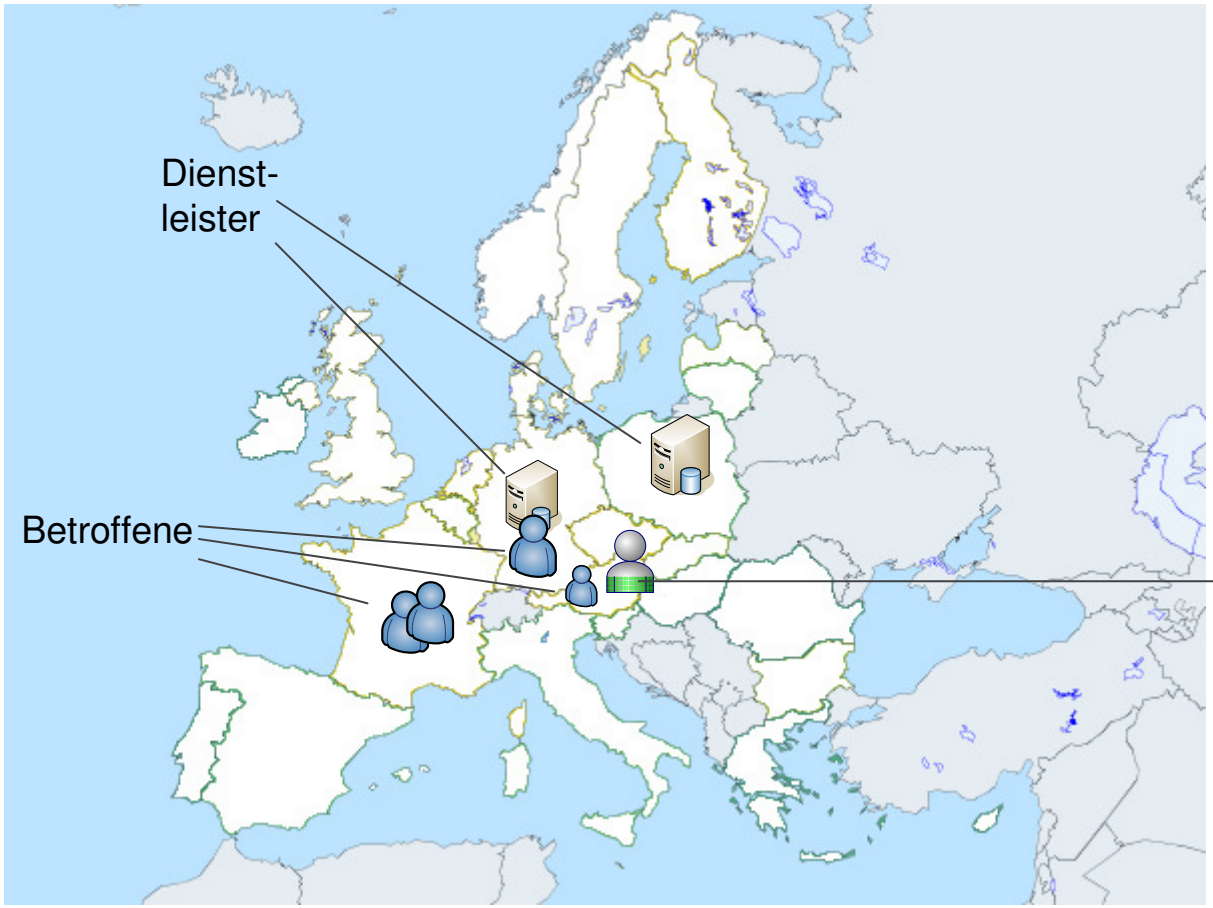
Akteure im Bereich des Datenschutzes



Nationale Datenschutz-gesetze differieren – Welches Recht gilt?

- Grundsatz: Ort der Niederlassung des Auftraggebers ist entscheidend
  - zB österr. Unternehmen bietet Online-Service in der ganzen EU an: es gilt österr. Recht
  - Ort der Niederlassung der Dienstleister ist unerheblich
- Wenn der Auftraggeber mehrere Niederlassungen in der EU hat:
  - Im Rahmen der Tätigkeiten welcher Niederlassung erfolgt die Datenverarbeitung?

Welches Recht gilt?



Zulässigkeit der Datenverarbeitung

1. Zulässiger Zweck der Datenverarbeitung?
   - festgelegt
   - eindeutig
   - rechtmäßig
2. Schutzwürdige Geheimhaltungsinteressen verletzt?
   - Rechtfertigungsgründe
   - Unterscheidung sensible / nicht-sensible Daten
   - Verhältnismäßigkeit (erforderliches Ausmaß / gelindestes Mittel)

Schutzwürdige Geheimhaltungsinteressen

Geheimhaltungsinteressen nur dann nicht verletzt, wenn:

1) der Betroffene zugestimmt hat (informierte und freie Zustimmung)
   - 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 AG oder eines Dritten;zB
   - zur Wahrung lebenswichtiger Interessen eines Dritten
   - zur Erfüllung einer vertragl. Verpflichtung zw. AG und Betroffenem
   - zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde

Geheimhaltungsinteressen bei sensiblen Daten

Sensible Daten: Daten natürlicher Personen über

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

Eingeschränkte Zulässigkeit der Verarbeitung; insb:

- „überwiegende berechtigte Interessen“ nicht ausreichend
- Zustimmung des Betroffenen muss ausdrücklich sein
- Jedoch Ausreichend: Arbeitsrechtliche Rechte/Pflichten + Betriebsvereinbarung

Datensicherheit I

- Daten sind zu schützen vor (§ 14 DSG)
  - Verlust
    - → Verfügbarkeit
  - zufälliger oder unrechtmäßiger Zerstörung
    - → Integrität
  - Zugang durch Unbefugte
    - → Vertraulichkeit
  - Nicht ordnungsgemäße Verwendung
    - → Rechtmäßigkeit

Datensicherheit II

- Angemessene Sicherheitsmaßnahmen: je nach
  - Art der verwendeten Daten
  - Umfang und Zweck der Verwendung
  - Stand der technischen Möglichkeiten
  - wirtschaftliche Vertretbarkeit
- Um Angemessenheit zu beurteilen:
  - Risiko-Analyse
  - Kosten-Nutzen-Analyse

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

Breach Notification nach DSG

- § 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

Datengeheimnis (§ 15 DSG)

- Gilt für Auftraggeber, Dienstleister und Mitarbeiter
- Gesetzliche Verpflichtung zur Geheimhaltung von Daten, die aufgrund berufsmäßiger Beschäftigung anvertraut oder zugänglich gemacht wurden
- Daten nur aufgrund Anordnung des Auftraggebers übermitteln
- Mitarbeiter sind über die Folgen der Verletzung des Datengeheimnisses belehren
- Rechtsfolge der Verletzung: bis zu EUR 25.000 Verwaltungsstrafe (§ 52 Abs 1 DSG)

Rechte des Betroffenen

- Recht auf Auskunft
  - Welche Daten verarbeitet?
  - Woher stammen die Daten?
  - Wozu verwendet?
  - An wen übermittelt?

  → auf schriftliches Verlangen des Betroffenen

  → binnen 8 Wochen nach Einlangen zu erfüllen
- Recht auf Richtigstellung der Daten
- Recht auf Löschung unzulässig verarbeiteter Daten

Meldepflicht gegenüber der DSB

- AG hat Datenanwendung vor Inbetriebnahme bei der DSB zu melden (§ 18 Abs 1 DSG)
- Meldung muss enthalten (§ 19 DSG)
  - Name und Anschrift des Auftraggebers
  - Zweck der Datenverarbeitung
  - Nachweis der rechtlichen Befugnis
  - Kreise der Betroffenen & verarbeiteten Datenarten
  - Kreise der Übermittlungsempfänger
  - Allgemeine Beschreibung der Datensicherheitsmaßnahmen
- Alle registrierten Meldungen sind öffentlich einsehbar: https://dvr.dsb.gv.at

Ausnahmen von der Meldepflicht

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
  - Bonus- und Beteiligungsprogramme im Konzern

Vereinfachte Meldepflicht für sog. Muster-Anwendungen

- zB Zutrittskontrollsysteme (für physischen Zugang zu Gebäuden)
- nur Name des Auftraggebers, Art der Muster-Anwendung & rechtliche Befugnis sind zu melden

Vorabkontrolle

- Datenanwendung darf erst nach erfolgter Genehmigung in Betrieb genommen werden, wenn (§ 18 Abs 2 DSG)
  - Sensible Daten
  - Strafrechtlich relevante Daten
  - Videoüberwachung (§ 50c DSG)
  - Auskunftserteilung über die Kreditwürdigkeit der Betroffenen
  - Informationsverbundsystems (gemeinsame Verarbeitung von Daten in einer Datenanwendung durch mehrere Auftraggeber; beide haben Zugriff auf alle Daten)

Outsourcing – Datenüberlassung an Dienstleister

- Auftraggeber kann sich zur Datenverarbeitung eines Dienstleisters bedienen (§ 10 DSG)
  - Dienstleister muss ausreichende Gewähr für rechtmäßige und sichere Datenverwendung bieten
  - 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

Outsourcing an ausländische Dienstleister I

- Dienstleister in der EU
  - Keine Meldung/Genehmigung erforderlich
- Dienstleister außerhalb der EU
  - Nur Genehmigungsfrei, wenn Drittstaat angemessenen Datenschutz bietet
    - Lt. Europ. Kommission zB Kanada, Schweiz und
    - die USA:
      - Safe Harbor Program
      - “angemessener” Datenschutz, wenn
        - Sich der Dienstleister nach Safe Harbor Rules selbst-zertifiziert hat → safeharbor.export.gov/list.aspx
        - Rechtsdurchsetzung: FTC Act § 5

Outsourcing an ausländische Dienstleister II

- Outsourcing an Dienstleister 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 ein Genehmigungsvorbehalt
    - Genehmigung ist zu erteilen, wenn Dienstleister-Vertrag Standardvertragsklauseln der Europ. Kommission enthält

Sanktionen nach DSG I

- § 51 DSG: Datenverwendung in Gewinn- oder Schädigungsabsicht
  - Berufsmäßig anvertraute oder zugänglich gemachte oder widerrechtlich verschaffte Daten – einem anderen zugänglich machen oder veröffentlichen, obwohl schutzwürdige Geheimhaltungsinteressen an Daten
  - Strafrahmen bis zu einem Jahr Freiheitsstrafe

Sanktionen nach DSG II

- § 52 Abs 1 DSG: Verwaltungsstrafbestimmung
  - Verwaltungsstrafe bis EUR 25.000,-:
    - widerrechtlicher Zugang zu Daten verschaffen
    - **Daten in Verletzung Datengeheimnis übermitteln**
    - entgegen rechtskräftigem Urteil nicht löschen/korrigieren
    - widerrechtlich löschen
    - sich Daten unter Vortäuschung falscher Tatsachen verschaffen

      ➢ Verletzung von Rechten bereits stattgefunden

Sanktionen nach DSG III

- § 52 Abs 2 DSG: Verwaltungsstrafbestimmung
  - Verwaltungsstrafe bis EUR 10.000,-:
    - ohne Meldung od. von Meldung abweichend Daten ermitteln, verarbeiten, übermitteln
    - ohne Genehmigung ins Ausland übermitteln / überlassen
    - gegen Zusagen / Auflagen der DSB verstoßen
    - Offenlegungs- und Informationspflichten verletzen
    - Sicherheitsmaßnahmen außer Acht lassen oder nicht innerhalb Löschungsfrist löschen

      ➢ noch keine Verletzung von Rechten, aber Unterlassungen, die Rechte des Betroffenen gefährden

Ausblick

- Datenschutz-Grundverordnung der EU
  - Einheitliches Datenschutzrecht in allen Mitgliedstaaten
  - Betrieblicher Datenschutzbeauftragter für größere Unternehmen
  - Weitgehender Entfall von Meldepflichten
  - Vereinfachte Konzern-interne Datenübermittlungen, sofern Binding Corporate Rules
  - Datenportabilität
  - Strafen von bis zu 5% des Jahresumsatzes

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?

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