

Datenschutz als Herausforderung für Unternehmen

WOLF THEISS

Dr. Lukas Feiler, SSCP

Associate, Wolf Theiss Rechtsanwälte

TOPICS

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

Datenschutz als Grundrecht in der EU

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

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

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”

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 öffentlich 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

Was sind “personenbezogene Daten”?

Personenbezogene Daten

- Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist

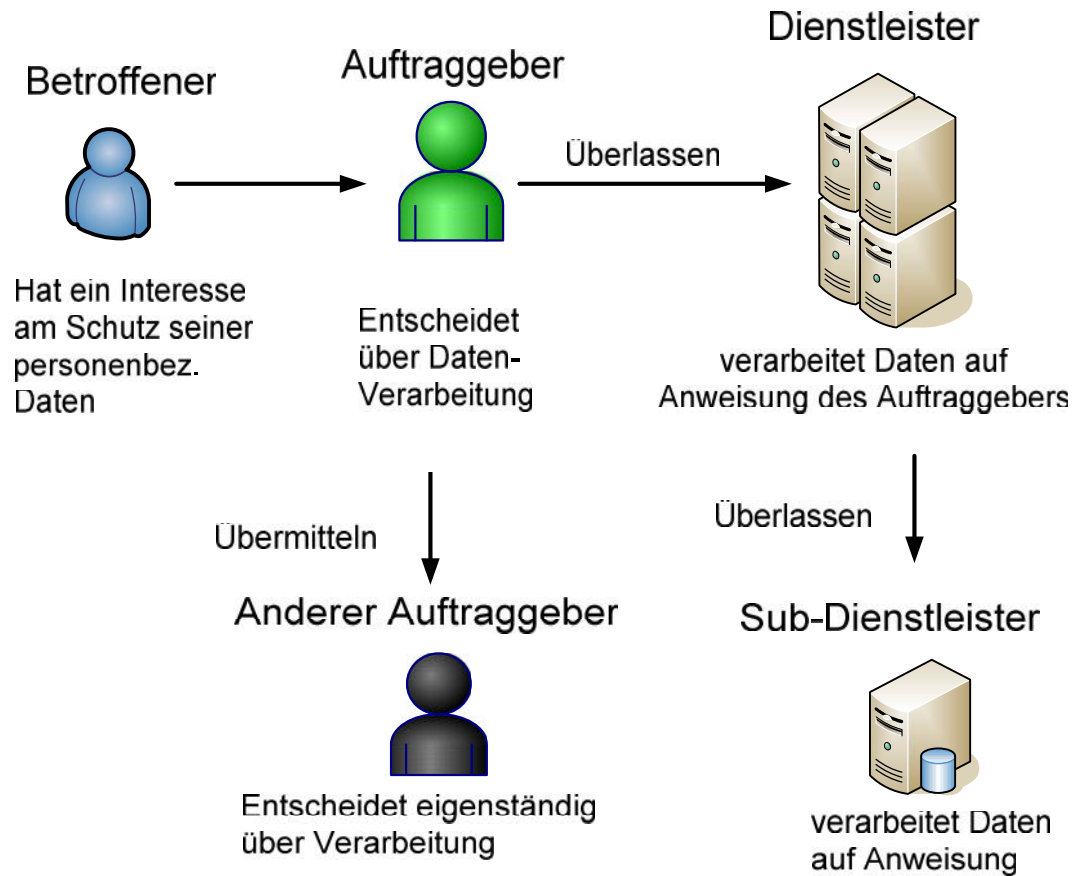
Indirekt personenbezogene Daten

- 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

Akteure im Bereich des Datenschutzes



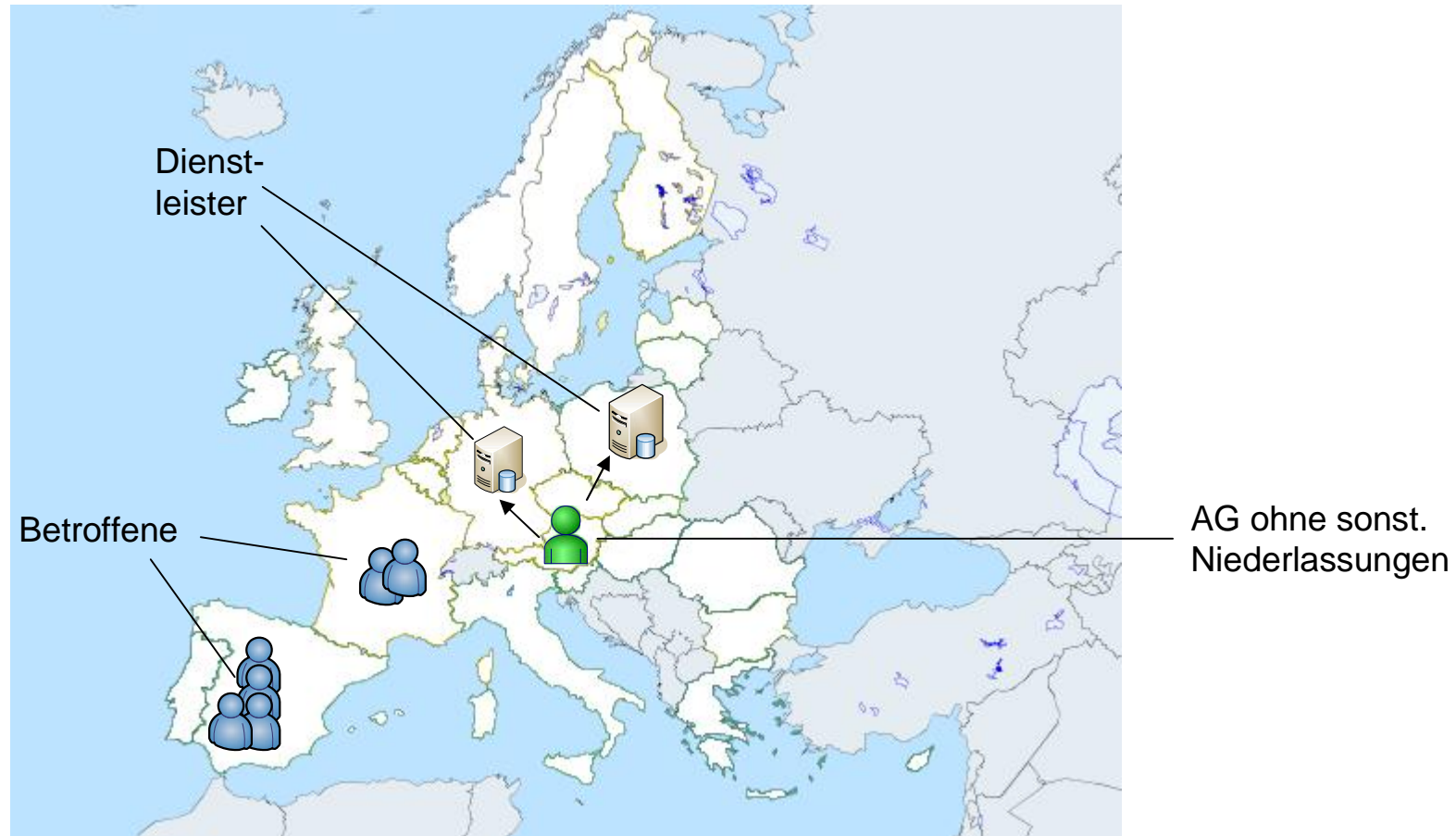
Regulierungsbehörden

- Nationale Aufsichtsbehörden – Datenschutzkommission in Österr.
 - EU Datenschutzrecht wird ausschließlich von nationalen Behörden vollzogen
- 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

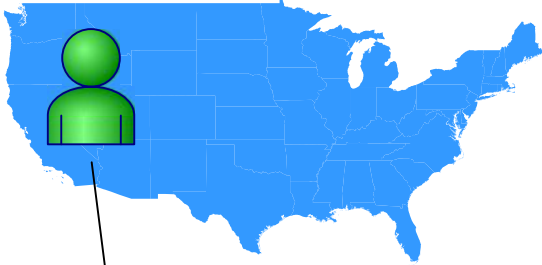
Nationale Datenschutzrechte differieren – Welches Recht gilt?

- Grundsatz: Ort der Niederlassung des Auftraggebers ist entscheidend
 - zB wenn XYZ GmbH Internet-Dienste in der ganzen EU anbietet aber nur in Österreich eine Niederlassung hat: Es gilt österr. Recht.
- Wenn der Auftraggeber 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 Auftraggeber keine Niederlassung in der EU hat:
 - Muss das Recht jener EU-Mitgliedstaaten befolgen, in denen Mittel zur Datenverarbeitung verwendet werden

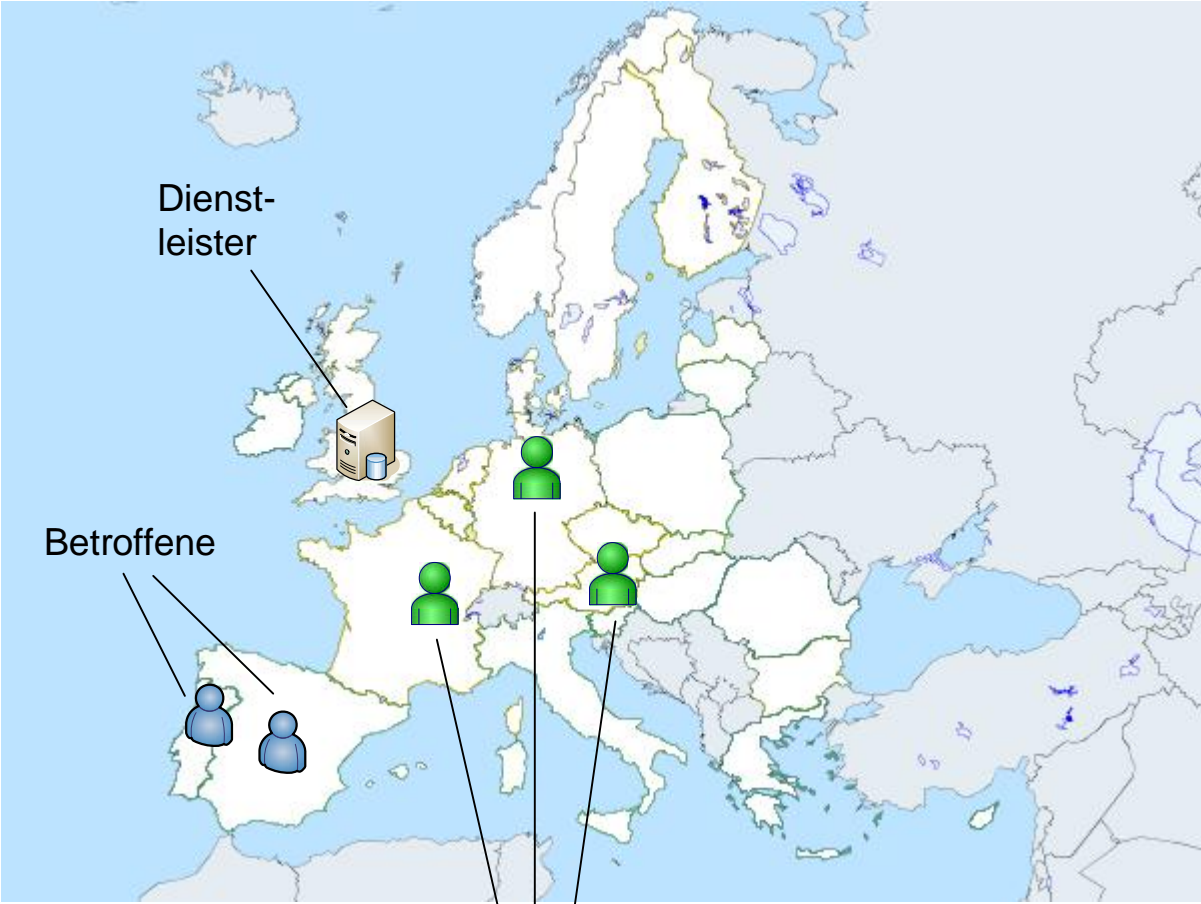
Welches Recht gilt?



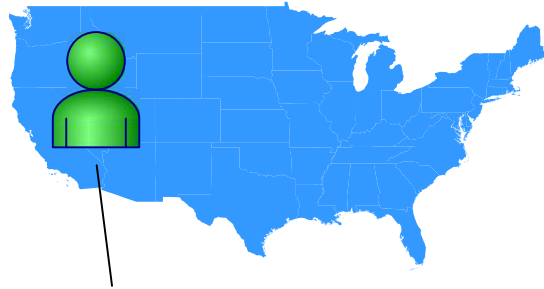
Welches Recht gilt?



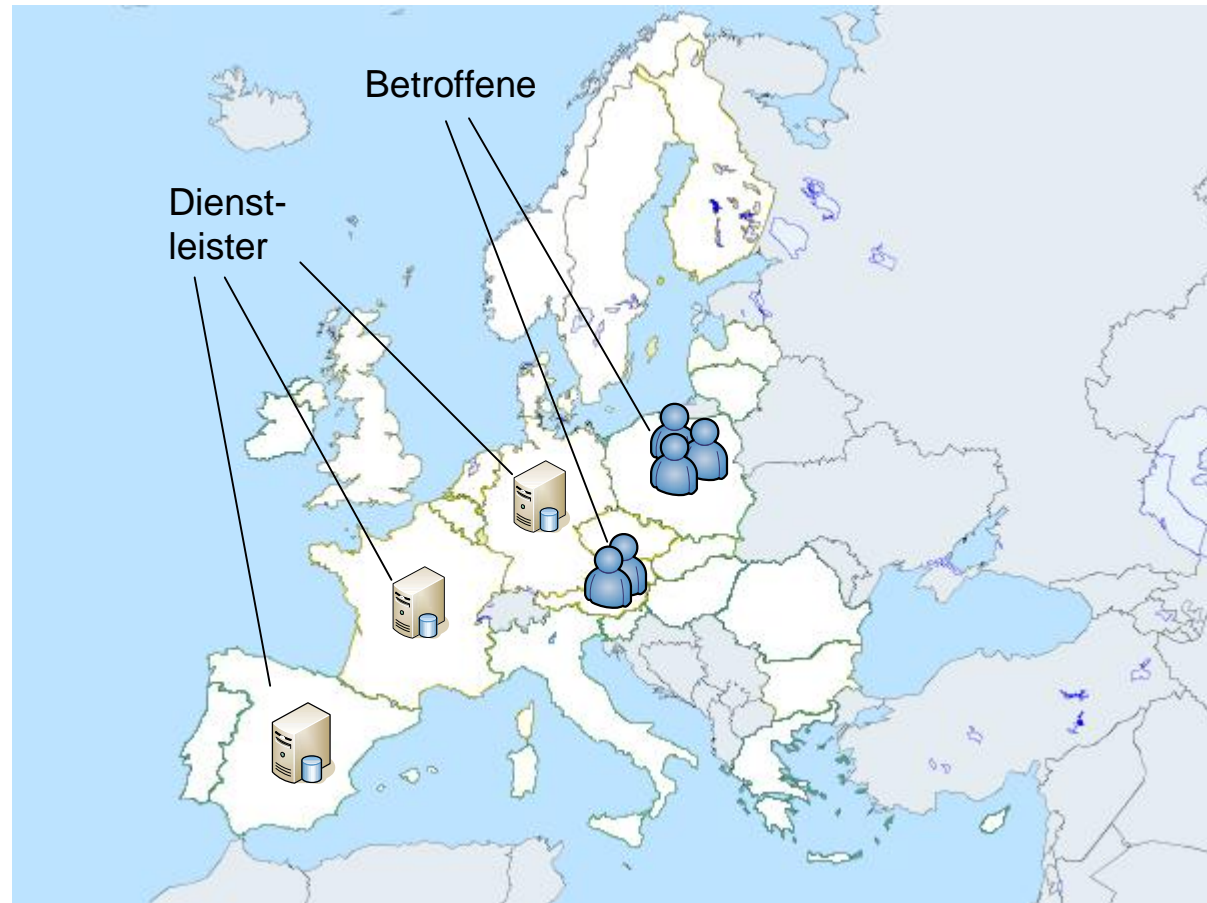
AG mit 3 Niederlassungen in der EU



Welches Recht gilt?



AG ohne
Niederlassung
in der EU



Zulässigkeit der Datenverarbeitung

Personenbez. Daten dürfen nur verarbeitet werden, wenn:

- 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 AG oder eines Dritten; zB
 - zur Wahrung lebenswichtiger Interessen eines Dritten
 - zur Erfüllung einer vertragl. Verpflichtung zw. AG und Betroffenenem
 - zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde

Zulässigkeit der Verarbeitung sensibler 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 des AG oder eines Dritten“ nicht ausreichend
- Zustimmung des Betroffenen muss ausdrücklich sein

Exkurs: Datenschutz im Arbeitsverhältnis

- Technische Kontrollmaßnahmen, die die Menschenwürde verletzen sind jedenfalls unzulässig; unabhängig von allfällige Zustimmung
 - zB WC-Videoüberwachung
- Kontrollmaßnahmen, die die Menschenwürde berühren
 - Zustimmung des Betriebsrats erforderlich, sofern vorhanden (§ 96 ArbVG)
 - Wenn es keinen Betriebsrat gibt: Individualvereinbarungen mit jedem Arbeitnehmer erforderlich (§ 10 AVRAG)
 - zB Überwachung der Facebook-Aktivitäten der Mitarbeiter
 - zB Videoüberwachung am Arbeitsplatz
- Sonstige elektronische Arbeitnehmer-Datenverarbeitungen
 - Zustimmung des Betriebsrats erforderlich (§ 96a ArbVG)

Exkurs: Whistleblowing Hotlines

- U.S. Sarbanes-Oxley Act verpflichtet Unternehmen, die in den USA öffentlich gehandelt werden, ein Whistleblowing-System einzuführen
- Datenschutzrechtliche Rechtfertigung?
 - Gesetzliche Verpflichtung des Auftraggebers?
 - Nein, da ausländisches Recht irrelevant
 - Überwiegende berechnigte Interessen des AG? (§ 8 Abs 4 DSGVO)
 - Gute Corporate Governance vs. Arbeitnehmer-Datenschutz
 - Möglich aber Verhältnismäßigkeit, Subsidiarität & Schwere der mutmaßlichen Verstöße, über die berichtet werden kann, ist zu berücksichtigen
 - Vgl. Stellungnahme 1/2006 der Article 29 Working Party

Meldepflichten gegenüber der DSK

- AG hat Datenanwendung vor Inbetriebnahme bei der DSK zu melden (§ 18 Abs 1 DSGVO)
- Meldung muss enthalten (§ 19 DSGVO)
 - 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 Meldungen sind öffentlich einsehbar:
<https://dvr.dsk.gv.at>

Ausnahmen von der Meldepflicht

- Meldepflicht entfällt, wenn (§ 17 Abs 2 DSGVO)
 - nur veröffentlichte oder nur indirekt personenbezogene Daten
 - Standard-Datenanwendung gemäß Standard- und Musterverordnung 2004; zB
 - Rechnungswesen und Logistik
 - Personalverwaltung für privatrechtliche Dienstverhältnisse
 - Videoüberwachung für Banken, Juweliere, Trafiken, Tankstellen und bebaute Privatgrundstücke
- 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 DSGVO)
 - Sensible Daten
 - Strafrechtlich relevante Daten
 - Auskunftserteilung über die Kreditwürdigkeit der Betroffenen
 - Informationsverbundsystems (gemeinsame Verarbeitung von Daten in einer Datenanwendung durch mehrere Auftraggeber; beide haben Zugriff auf alle Daten)
 - Videoüberwachung (§ 50c DSGVO)

Verpflichtende Datensicherheitsmaßnahmen

- Daten sind zu schützen vor
 - Verlust
 - Verfügbarkeit
 - zufälliger oder unrechtmäßiger Zerstörung
 - Integrität
 - Zugang durch Unbefugte
 - Vertraulichkeit
 - Nicht ordnungsgemäße Verwendung
 - Rechtmäßigkeit

Verpflichtende Datensicherheitsmaßnahmen #2

- 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

Verpflichtende Datensicherheitsmaßnahmen #3

Jedenfalls erforderlich sind (§ 14 Abs 2 DSGVO)

- 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)

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 DSGVO 2000; § 95a TKG 2003
 - Verträge

Breach Notification nach DSGVO 2000

- § 24 Abs 2a DSGVO 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 DSGVO 2000)
 - Haftung für Vermögensschäden nach allgem. Zivilrecht

Breach Notification 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

Breach Notification nach Vertrag

- Wenn Breach Notification in einem Vertrag nicht geregelt ist, gilt:
 - Notifikation einer Sicherheitsverletzung hat zu erfolgen, wenn dem Vertragspartner aus dieser ein Schaden droht (sog. nebenvertragliche Schutzpflicht)
 - Betroffene sind unverzüglich zu informieren
- Rechtsfolge der Verletzung:
 - Vertragliche Haftung für Vermögensschäden

Data Breach Notification: Auswirkungen auf den Markt

- Abbau der Informationsasymmetrie
 - Kunden haben – im Unterschied zu Anbietern – idR keine Information über die Sicherheit eines Dienstes
 - Breach Notifications bringen neue Transparenz & Konkurrenz in Bezug auf IT-Sicherheit
 - Chance für Unternehmen, die mehr Daten-Sicherheit bieten!
- Internalisierung des Risikos Data Breach
 - Bisher: Data Breach weitgehend eine Externality
 - Nunmehr: Betroffenes Unternehmen trägt größeren Teil der negativen Folgen

Outsourcing – Datenüberlassung an Dienstleister

- Auftraggeber kann sich zur Datenverarbeitung eines Dienstleisters bedienen (§ 10 DSGVO)
 - 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 DSGVO 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

- 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 #2

- Outsourcing an Dienstleister in Drittland ohne angemessenen Datenschutz
 - Genehmigungsfrei, wenn (u.a.; § 12 Abs 3 DSGVO)
 - 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

Rechte der Betroffenen

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

Ausblick

- **Datenschutz-Grundverordnung der EU**
 - einheitliches Datenschutzrecht in allen Mitgliedstaaten
 - Weitgehender Entfall von Meldepflichten
 - Vereinfachte Konzern-interne Datenübermittlungen, sofern Binding Corporate Rules
 - Strafen von bis zu 2% des Jahresumsatzes
- **Österreichische DSG-Novelle 2012**
 - Entfall der Meldepflicht, wenn betrieblicher Datenschutz-Beauftragter bestellt
 - Entfall der Vorabkontrolle für Videoüberwachung, Informationsverbundsysteme und Verwendung strafrechtlich relevanter Daten

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

Danke für Ihre Aufmerksamkeit



Contact Details

Dr. Lukas Feiler, SSCP

Wolf Theiss Rechtsanwälte
Schubertring 6, 1010 Wien

Tel: (+ 43 1) 515 10 5090
Fax: (+ 43 1) 515 10 665090

e-mail: lukas.feiler@wolftheiss.com

www.wolftheiss.com

