

Grundlagen des Datenschutzrechts

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

KU Grundlagen des Technologierechts II
9.3.2016





Datenschutz - Inhalt

- Rechtsquellen und Grundbegriffe
- Anwendbares nationales Datenschutzrecht
- Zulässigkeitsprüfung
- Datensicherheit & Breach Notification
- Meldepflichten gegenüber der DSB
- Outsourcing innerhalb und außerhalb der EU
- Sanktionen
- Ausblick: Die Datenschutzgrundverordnung

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

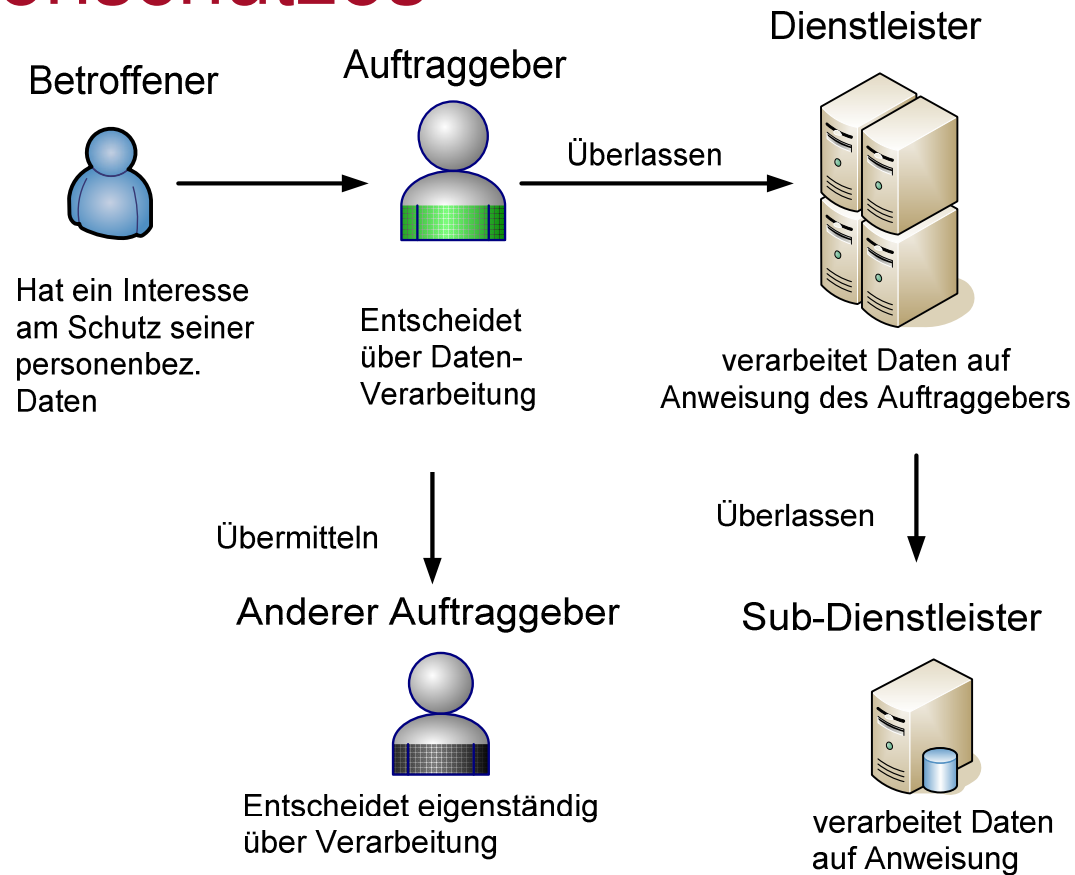
- wenn der Auftraggeber die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann
 - “personenbezogen” ist ein relativer Begriff
 - Daten können für ein Unternehmen direkt und für ein anderes nur indirekt personenbezogen sein



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
- 2) zulässigerweise veröffentlichte Daten
- 3) indirekt personenbezogenen Daten
- 4) gesetzliche Ermächtigung oder Verpflichtung
- 5) lebenswichtige Interessen des Betroffenen
- 6) überwiegende berechnete 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

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 DSGVO)
 - 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 DSGVO

- § 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: „unverzögerlich“
- Rechtsfolge der Verletzung:
 - Verwaltungsstrafe: bis zu EUR 10.000 (§ 52 Abs 2 DSGVO 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 DSGVO)

- 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 DSGVO)
 - Sensible Daten
 - Strafrechtlich relevante Daten
 - Videoüberwachung (§ 50c DSGVO)
 - 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 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 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
 - 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“

Outsourcing an ausländische Dienstleister II

- 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

Sanktionen nach DSGVO I

- § 51 DSGVO: 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
 - Strafraum bis zu einem Jahr Freiheitsstrafe

Sanktionen nach DSGVO II

- § 52 Abs 1 DSGVO: 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 DSGVO III

–§ 52 Abs 2 DSGVO: 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 – Die Datenschutz-Grundverordnung

- 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 anwendbaren Recht

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.