Baker McKenzie.

Grundlagen des Datenschutzrechts

VO Grundlagen des Technologierechts II

14. März 2017 / RA Dr. Lukas Feiler, SSCP, CIPP/E

Agenda

1. Wozu Datenschutz-Compliance?
2. Welche Datenverarbeitungen sind erfasst?
3. Zulässigkeit der Datenverarbeitung
4. Betrieblicher Datenschutzbeauftragter
5. Datensicherheitspflichten
6. Pflichten zur Datenaufbewahrung und -löschung
7. Meldepflichten
8. Section titleDokumentationspflichten
9. Outsourcing
10. Internationale Datenübermittlungen
11. Geldstrafen

Wozu Datenschutz-Compliance?

- Rechtsrahmen
  - In Österreich: Datenschutzgesetz 2000 (DSG 2000)
- ab 25. Mai 2018: Datenschutz-Grundverordnung der EU (DSGVO)
  - Geldstrafen von bis zu 20 Millionen Euro oder 4 % des gesamten weltweit erzielten Jahresumsatzes
- Haftung der Geschäftsleitung
  - Für Verwaaltungnsstrafen haften Mitgleider der Geschäftsleitung grds solidarisch mit der Gesellschaft (für DSGVO noch offen)
  - Haftung gegenüber der Gesellschaft aus Dienstvertrag

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

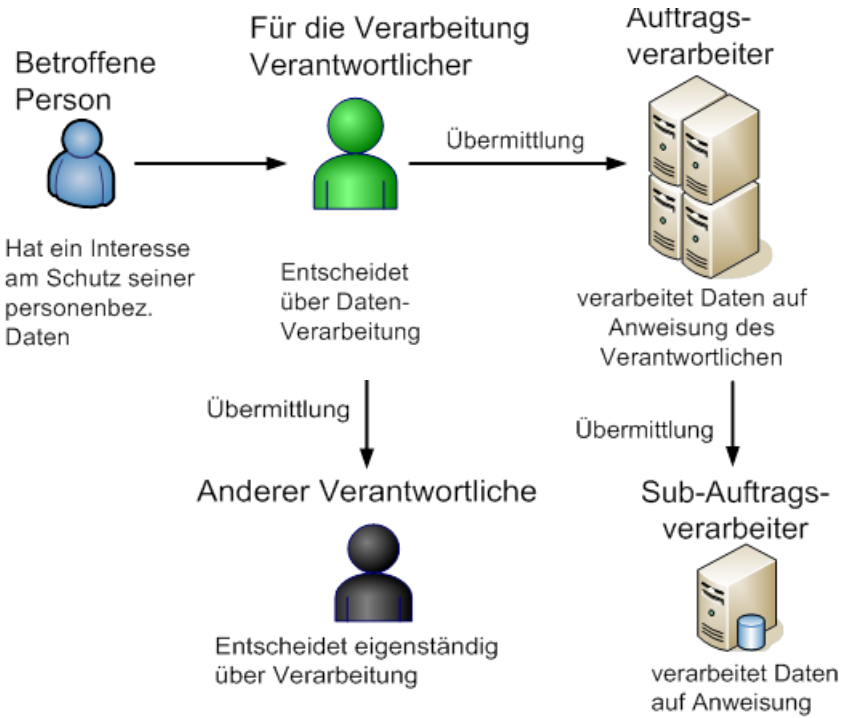
Welche Datenverarbeitungen sind erfasst?

- Jede Verarbeitung personenbezogener Daten ist erfasst
- Verarbeiten: jede Handhabung von Daten (auch gespeichert halten)
- personenbezogene Daten: Daten, die sich auf eine bestimmte oder bestimmbare Person beziehen
  - DSG 2000: natürlich und juristische Personen
  - DSGVO: nur natürliche Personen

Akteure im Bereich des Datenschutzrechts

- betroffene Person
  - natürliche Personen
- Verantwortlicher
  - natürliche oder juristische Person
  - entscheidet allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet
- Auftragsverarbeiter
  - natürliche oder juristische Person, die im Auftrag eines Verantwortlichen personenbezogene Daten verarbeitet
- Aufsichtsbehörde

Akteure im Bereich des Datenschutzes



Räumlicher Anwendungsbereich – Wo gilt die DSGVO?

- Verantwortlicher/Auftragsverarbeiter haben ihren Sitz in der EU
  - die Verarbeitung findet im Rahmen der Tätigkeiten einer Niederlassung in der EU statt
- Verantwortlicher/Auftragsverarbeiter haben keinen Sitz in der EU
  - Verarbeitung von Daten von Personen mit Wohnsitz in der EU steht im Zusammenhang mit
    - dem Anbieten von Waren oder Dienstleistungen an EU Bürger unabhängig von einer Zahlung durch die betroffene Person
    - der Beobachtung des Verhaltens von betroffenen Personen innerhalb der EU

Verhältnis der DSGVO zu nationalen Datenschutzgesetzen

- Unmittelbare Anwendbarkeit der DSGVO
  - kein Fortbestehen der nationalen Datenschutzgesetze nach dem 25. Mai 2018
- Außerhalb des Anwendungsbereichs der DSGVO
  - Spielraum des nationalen Gesetzgebers
  - 69 Öffnungsklauseln
    - zB Einwilligung, Daten über strafrechtliche Verurteilungen

Zulässigkeit der Datenverarbeitung

Grundsätze der Datenverarbeitung

- Rechtmäßigkeit – datenschutzrechtliche Rechtsgrundlage erforderlich
- Treu und Glauben
- Transparenz
- Zweckbindung
- Datenminimierung und Speicherbegrenzung
- Richtigkeit
- Sicherheit

Datenschutzrechtliche Rechtsgrundlage

1. Einwilligung gegeben (informierte und freie Zustimmung)
2. Verarbeitung ist für die Erfüllung eines Vertrags erforderlich
3. gesetzliche Verpflichtung des Verantwortlichen
4. lebenswichtige Interessen der betroffenen Person
5. öffentliches Interesse oder in Ausübung öffnetlicher Gewalt, die dem Verantwortlichen übertragen wurde
6. überwiegende berechtigte Interessen des Verantwortlichen oder eines Dritten

Neue Grenzen für die elektronische Einwilligung nach der DSGV

- Schlüssige oder ausdrückliche Zustimmung
- Checkbox darf nicht per default angehakt sein
- Zustimmung durch AGB?
  - in verständlicher und leicht zugänglicher Form
  - in klarer und einfacher Sprache
  - von anderen Regelungsgegenständen der AGB klar zu unterscheiden

Herausforderungen bei der Einwilligung von Personen unter 16 Jahren (1)

- Zustimmung von Minderjährigen grds erst gültig ab 16 Jahren (Art 8 DSGV)
- < 16 Jahre: Zustimmung der Erziehungsberechtigten erforderlich
  - Verantwortlicher muss „angemessene Anstrengungen unter Berücksichtigung der vorhandenen Technologie“ unternehmen
- Praktische Umsetzung
  - Angebot nicht auf Unter-16-Jährige ausrichten
  - Registrierung nur zulassen, wenn Geburtsdatum angegeben

Herausforderungen bei der Einwilligung von Personen unter 16 Jahren (2)

- Überwiegendes berechtigtes Interesse als alternative Rechtsgrundlage?
  - z.B. wenn pseudonymisiert
- DSGV ermächtigt nationalen Gesetzgeber zur Herabsetzung der Altersgrenze

Daten als Ware & neue Grenzen der Einwilligung

- Viele „Gratis“ – Dienste im Internet setzen Zustimmung zur Datenerhebung voraus
- Zustimmung nur gültig, wenn sie „frei“ ist
- Grds nicht „frei“, wenn (Art 7 Abs 4 DSGV):
  - Durchführung eines Vertrages wird von Zustimmung zur Datenverarbeitung abhängig gemacht und
  - Datenverarbeitung für Vertragserfüllung nicht erforderlich

→ Daten-getriebene Geschäftsmodelle prüfen und absichern

Sensible Daten

- rassische und ethnische Herkunft,
- politische Meinung,
- Gewerkschaftszugehörigkeit, und
- religiöse oder weltanschauliche Überzeugung hervorgeht.
- genetischen und biometrischen Daten zur Identifizierung einer natürlichen Person,
- Gesundheitsdaten und Daten zum Sexualleben

→ überwiegendes berechtigtes Interesse ist nicht ausreichend

→ Einwilligung muss ausdrücklich erfolgen

Bestellung eines betrieblichen Datenschutzbeauftragten (1)

- DSG 2000: Keine Regelungen
- Mit der DSGVO verpflichtend, wenn
  - Behörde oder öffentliche Stelle aus Verantwortlicher fungiert
  - Daten-getriebenes Geschäftsmodell
  - nach nationalem Recht vorgeschrieben (voraussichtlich in Deutschland, nicht in Österreich)

Bestellung eines betrieblichen Datenschutzbeauftragten (2)

- Persönliche Voraussetzungen
  - beruflichte Qualifikation und Fachwissen auf dem Gebiet des Datenschutzrechts
  - kann, muss aber nicht Arbeitnehmer des Verantwortlichen sein
- Bestellung eines externen Datenschutzbeauftragten ist möglich

Stellung des betrieblichen Datenschutzbeauftragten nach der DSGVO

- Unmittelbare Berichterstattung an die höchste Managementebene
- Einbindung in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen
- muss über alle notwendigen Ressourcen verfügen
- hat Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen
- Anlaufstelle für betroffene Personen
- Verschwiegenheitsverpflichtung
- Grds keine Haftung nach der DSGVO

Datensicherheitspflichten nach der DSGVO (1)

- Daten sind zu schützen vor
  - Verlust der Vetraulichkeit
  - Verlust der Verfügbarkeit
  - Verlust der Integrität
- Risikoangemessene Sicherheitsmaßnahme unter Berücksichtigung
  - des Stands der Technik,
  - der Implementierungskosten,
  - der Art, Umfangs & Zwecke der Verarbeitung und
  - der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen

Datensicherheitspflichten nach der DSGVO (2)

- Angemessene Maßnahmen umfassen laut DSGV insb.:
  - Pseudonymisierung und Verschlüsselung
  - die Fähigkeit, die Sicherheit der Systeme sicherzustellen
  - die Fähigkeit, Verfügbarkeit nach einem Zwischenfall rasch wiederherzustellen → Incident Response Capabilities
  - Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Sicherheitsmaßnahmen → Audits
- Technische Standards ausreichend?
  - z.B. Center for Internet Security Critical Security Controls oder ISO/IEC 27001?

Dokumentationspflichten

- Österreich: grds keine
- DSGVO: Führung eines „Verzeichnisses der Verarbeitungstätigkeiten“
  - auf Anfrage der Aufsichtisbehörde bereitzustellen
  - betroffene Personen haben kein Recht auf Einsicht
- Mindesinhalt des Verzeichnisses nach DSGVO:
  - Name und Kontaktdaten des Verantwortlichen und eines etwaigen Datenschutzbeauftragten
  - Verarbeitungszwecke, Kategorien betroffener Personen, personenbezogener Daten und Empfänger
  - Informationen zu Datenübermittlungen in Drittländer
  - Speicherdauer
  - Datensicherheitsmaßnahmen

Privacy Impact Assessments & vorherige Konsultation

- verpflichtend, wenn voraussichtlich hohes Risiko für, insb. bei
  - Profiling
  - umfangreicher Verarbeitung sensibler oder strafrechtlich relevanter Daten
  - systematischer, umfangreicher Überwachung öffentlicher Bereiche
- Inhalt des Privacy Impact Assessments
  - Beschreibung der Verarbeitungsvorgänge und Zwecke
  - Bewertung der Notwendigkeit und Verhältnismäßigkeit
  - Beschreibung allfälliger Abhilfemaßnahmen
  - Risikobewertung (niedrig/mittel/hoch)
- Wenn hohes Risiko: vorherige Konsultation mit Datenschutzbehörde

Outsourcing – Datenübermittlung an Dienstleister

- Verantwortliche kann sich zur Datenverarbeitung eines Auftragsverarbeiters bedienen
  - Auftragsverarbeiter muss ausreichende Gewähr für rechtmäßige und sichere Datenverwendung bieten
- Auftragsverarbeitervereinbarung muss nach DSGVO Pflichten des Auftragsverarbeiters festlegen
  - Weisungsgebundenheit
  - Verpflichtung zur Vertraulichkeit aller Gehilfen
  - Sicherheitsmaßnahmen
  - Sub-Auftragsverarbeiter nur mit Zustimmung
  - Duldung und Unterstützung von Audits
  - Datenrückgabe (in welchem Format?)

Internationale Datenübermittlungen

- Wenn Empfänger in der EU/EWR: ok
- Wenn in Drittland mit adäquatem Datenschutzniveau: ok
  - zB Kanada, Schweiz
  - U.S. Privacy Shield: angemessener Datenschutz, wenn sich der Empfänger nach Privacy Shield selbst-zertifiziert hat
- Wenn in Drittland kein adäquates Datenschutzniveau
  - Grds: sog. Standardvertragsklauseln erforderlich
    - DSG 2000: genehmigungspflichtig
    - DSGVO: keine Genehmigung erforderlich
  - Wichtigste Ausnahme: ausdrückliche Einwilligung der Betroffennen

Verhängung und Bemessung von Geldbußen im Konzern

- Strafrahmen nach DSGVO: bis zu 20 Millionen Euro oder 4 % des weltweiten jährlichen Umsatzes des Unternehmens
- Unionskartellrechtlicher Unternehmensbegriff
  - Bemessung der Strafe: weltweiter Umsatz des gesamten Konzerns maßgeblich (Art 83 iVm Erwägungsgrund 150 Satz 3 DSGVO)
  - Strafe kann auch über Konzernmutter verhängt werden
    - Mitverantwortung der Konzernobergesellschaft, wenn Tochtergesellschaft Verhalten nicht autonom bestimmt
    - widerlegliche Vermutung bei 100%-igen Tochtergesellschaften (EuGH C-107/82 – *AEG*)

RA Dr. Lukas Feiler, SSCP CIPP/E
Senior Associate

Baker & McKenzie
Schottenring 25
1010 Wien

T: +43 1 2 42 50
F: +43 1 2 42 50 600
lukas.feiler@bakermckenzie.com

www.bakermckenzie.com