BAKER & MCKENZIE

Die EU-Datenschutz-Grundverordnung

RA Dr. Lukas Feiler, SSCP, CIPP/E

q/Talk, 29. November 2016

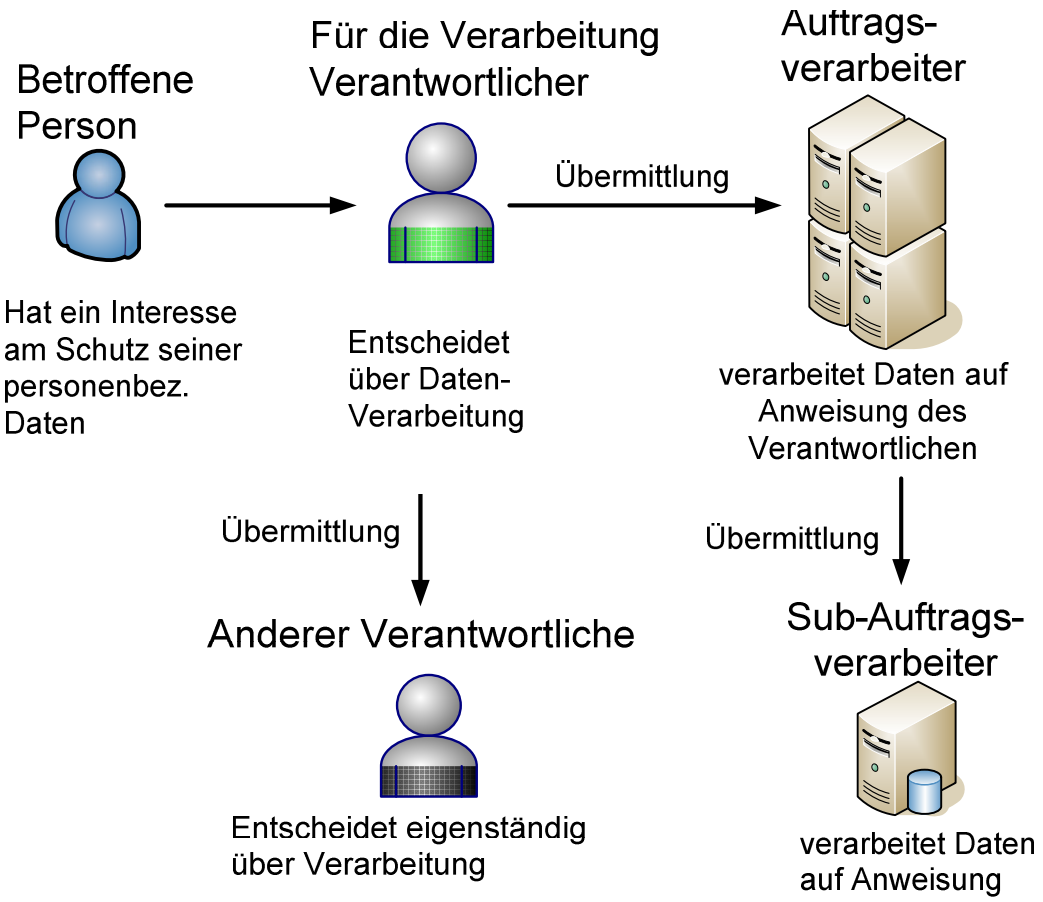
TOPICS

- Wozu Datenschutz-Compliance?
- Welche Datenverarbeitungen sind erfasst?
- Zulässigkeit der Datenverarbeitung
- Neue Betroffenenrechte
- Betrieblicher Datenschutzbeauftragter
- Datensicherheitspflichten
- Privacy by Design & by Default
- Meldepflichten
- Dokumentationspflichten
- Outsourcing
- Internationale Datenübermittlungen
- Geldstrafen & private Rechtsdurchsetzung

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

Akteure im Bereich des Datenschutzes



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

Geografischer Anwendungsbereich der DSGVO

- DSGVO gilt für Verantwortliche/Auftragsverarbeiter
  - mit Sitz in der EU
  - ohne Sitz in der EU aber mit einer Niederlassung in der EU, wenn Verarbeitung im Rahmen der Tätigkeiten der Niederlassung
  - ohne Sitz in der EU aber
    - Waren oder Dienstleistungen werden in der EU angeboten
    - Verhalten von Betroffenen in der EU wird beobachtet

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 von Kindern; 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 von 2

- 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
- Nationales Recht: Altersgrenze kann auf bis zu 13 Jahre herabgesetzt werden

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 Angebote 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

Neue Betroffenenrechte

- Recht auf Datenübertragbarkeit
  - Recht auf Übermittlung der Daten in einem wiederverwendbaren Format an den Betroffenen od Dritten
  - gilt nur gegenüber Verantwortlichen
  - gilt nur, wenn Daten vom Betroffenen bereitgestellt wurden
  - gilt nur, wenn Verarbeitung mit Einwilligung oder zur Vertragserfüllung
- Recht auf Vergessenwerden
  - = Recht auf Löschung

Bestellung eines betrieblichen Datenschutzbeauftragten – 1/2

- DSG 2000: Keine Regelungen
- Mit der DSGVO verpflichtend, wenn
  - Verarbeitung durch Behörde oder öffentliche Stelle
    oder
  - Daten-getriebenes Geschäftsmodell
    - Kerntätigkeit des Unternehmens ist umfangreiche regelmäßige und systematische Überwachung von Betroffenen
    - Kerntätigkeit des Unternehmens ist die umfangreichen Verarbeitung sensibler oder strafrechtlich relevanter Daten

    oder
  - nach nationalem Recht vorgeschrieben (voraussichtlich nicht in Österreich)

Bestellung eines betrieblichen Datenschutzbeauftragten – 2/2

- Persönliche Voraussetzungen
  - beruflichte Qualifikation und Fachwissen auf dem Gebiet des Datenschutzrechts
  - kann, muss aber nicht Arbeitnehmer des Verantwortlichen sein
  - es darf kein Interessenskonflikt vorliegen
- 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 – 1/2

BAKER & MCKENZIE

- 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 – 2/2

BAKER & MCKENZIE

- 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?

Privacy by Design & Privacy by Default

- Privacy by Design
  - Risiko- und Kosten-angemessene proaktive Maßnahmen
    → vgl auch allgemeine Rechenschaftspflicht
  - z.B. Möglichkeit für Betroffene die Verarbeitung ihrer Daten zu überwachen
  - Privacy by Default
  - insbesondere: Daten nicht per Default-Einstellungen öffentlich zu machen
  - Relevanz für Softwarehersteller?

Pflicht zur Durchführung von Privacy Impact Assessments

- DSGVO: PIA verpflichtend, wenn voraussichtlich hohes Risiko für Betroffene
  - insbesondere bei (i) Profiling, (ii) umfangreiche Verarbeitung sensibler oder strafrechtlich relevanter Daten oder (iii) systematische umfangreiche 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) unter Berücksichtigung der Abhilfemaßnahmen

Meldepflichten

BAKER & MCKENZIE

- In Österreich: Jede Datenanwendung ist vorab an Datenschutzbehörde zu melden
  - Ausnahme: sog. „Standard-Datenanwendung“ (zB Personalverwaltung für privatrechtliche Verhältnisse)
  - Wenn sensible Daten oder strafrechtlich relevante Daten betroffen (z.B. Videoüberwachung): Genehmigungsvorbehalt
- DSGVO: vorherige Konsultation der Behörde nur bei hohem Risiko (z.B. sensible Daten)

Dokumentationspflichten

BAKER & MCKENZIE

- Österreich: grds keine
- Deutschland: Führung eines Verfahrensverzeichnisses
- 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

Outsourcing – Datenüberlassungen 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
  - Ausnahme: Einwilligung der Betroffennen

Verhängung und Bemessung von Geldstrafen 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*)

Private Rechtsdurchsetzung

- Betroffene Person kann klagen
  - wo sie ihren Wohnsitz hat
  - wo der Verantwortliche/Auftragsverarbeiter eine Niederlassung hat
- Mögliche Ansprüche
  - Die Betroffenenrechte (Auskunft, Löschung, …)
  - Materieller und immaterieller Schadenersatz
- Rechtsdurchsetzung durch NGOs
  - NGOs können im Namen von Betroffenen klagen
  - Schadenersatzansprüche nur wenn nach nationalem Recht zugelassen (nach welchem?)
  - Betroffenenrechte unabhängig von Auftrag eines Betroffenen einklagen (je nach Gerichtsstand)

Kontakt

RA Dr. Lukas Feiler, SSCP CIPP/E
lukas.feiler@bakermckenzie.com

Baker & McKenzie
Schottenring 25
1010 Vienna
Tel.: +43 1 24 250
Fax: +43 1 24 250 600