Baker McKenzie.

Das neue Datenschutzrecht

Erforderliche Maßnahmen für Kanzleien und Unternehmen

18. SWK Steuerrechtstag, 16. November 2017

RA Dr. Lukas Feiler, SSCP CIPP/E

Themen

1 Einleitung in die Datenschutz-Grundverordnung

Wozu Datenschutz-Compliance?

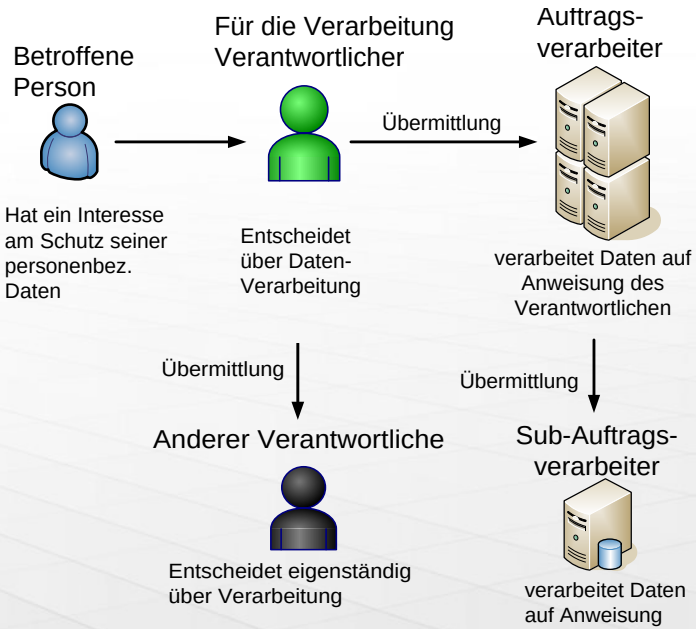
- Bisher:
  - In Österreich: Datenschutzgesetz 2000 (DSG 2000)
- Ab 25. Mai 2018: Datenschutz-Grundverordnung der EU (DSGVO)
  - Geldstrafen von bis zu 20 Millionen Euro oder vier Prozent des gesamten, weltweit erzielten Jahresumsatzes
- Haftung der Geschäftsleitung
  - Für Verwaltungsstrafen haften Mitglieder der Geschäftsleitung grds solidarisch mit der Gesellschaft
  - Haftung gegenüber der Gesellschaft aus Dienstvertrag
- Private Rechtsdurchsetzung & Sammelklagen
  - Betroffene haben auch Recht auf Ersatz des immateriellen Schadens
  - NGOs können im Namen von Betroffenen klagen

Anwendungsbereich

Welche Datenverarbeitungen sind erfasst?

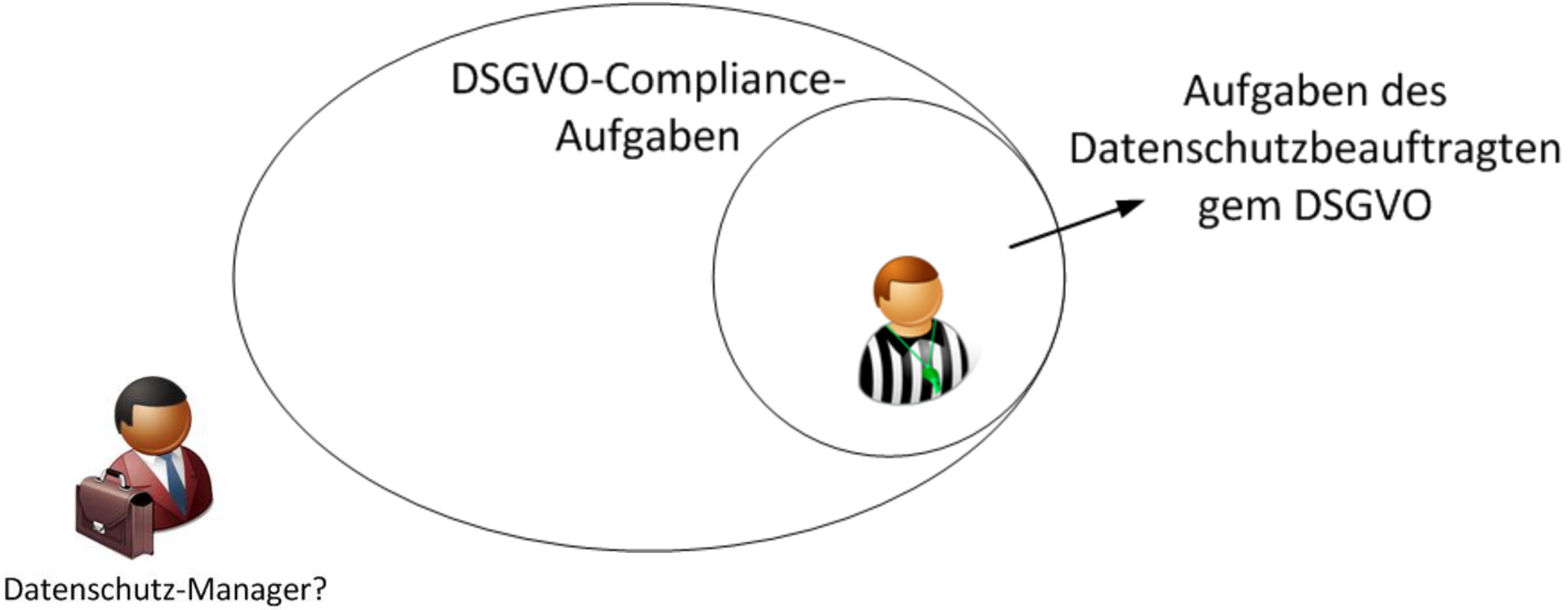
- Jede Verarbeitung personenbezogener Daten ist erfasst
- Verarbeiten: jede Handhabung personenbezogener Daten (auch das Gespeichert-Halten)
- Personenbezogene Daten: Daten, die sich auf eine bestimmte oder bestimmbare Person beziehen
  - DSG 2000: natürliche und juristische Personen
  - DSGVO: nur natürliche Personen

Die Rollenverteilung der DSGVO



2 Die wichtigsten TODOs für Wirtschaftstreuhänder

Datenschutzbeauftragten/Manager ernennen



Ziele des Datenschutzmanagements definieren

Aus personenbezogenen Daten einen wirtschaftlicher Wert gewinnen?

- Defensive vs. offensive Datenschutzstrategie

100% Compliance oder pragmatischer Compliance-Ansatz?

- Betriebswirtschaftliche vs. politische Risiken

Wer ist wofür zuständig?

- Rollen und Verantwortlichkeiten definieren

Infos über Datenverarbeitungsprozesse erheben

Für jede Verarbeitungstätigkeit zu klären:

- Wer ist der Verantwortliche?
- Welche Datenkategorien werden verarbeitet? Wie lange werden sie aufbewahrt?
- Zu welchen Zwecken erfolgt die Verarbeitung?
- Werden Auftragsverarbeiter eingesetzt? (Welche? Wo? Vertragsgrundlage?)
- Werden Daten an andere Verantwortliche übermittelt? (Welche? An wen? Zu welchen Zwecken? Wohin? Vertragsgrundlage?)
- Verarbeitung auf Grundlage einer Einwilligung? (Kopie der Einwilligungserklärung?)
- Kopie der Datenschutzmitteilung (sofern vorhanden)
- Datensicherheitsmaßnahmen

→ Vorbedingung für VZ der Verarbeitungstätigkeiten (Schritt 7) und Prüfung der Rechtsmäßigkeit (Schritt 8)

Verzeichnis der Verarbeitungstätigkeiten erstellen

Ausnahme von der Pflicht zur Führung eines Verzeichnisses

- weniger als 250 Mitarbeiter *und*
- Verarbeitung birgt keine Risiken für Betroffene *und*
- Verarbeitung erfolgt nur gelegentlich *und*
- Verarbeitung umfasst keine sensiblen oder strafrechtlich relevanten Daten.

Rechtmäßigkeit der Datenverarbeitung absichern

Für jede Verarbeitungstätigkeit

1) Rechtsgrundlage für Datenverarbeitung identifizieren
2) Datenschutzmitteilungen korrekt gestalten – Ausnahme für Wirtschaftstreuhänder
3) Auftragsdatenverarbeitungsvereinbarungen mit Dienstleistern abschließen
4) Wo erforderlich Standardvertragsklauseln für internationale Datenübermittlungen vereinbaren
5) Betriebsvereinbarungen abschließen
6) Datensicherheit gewährleisten

Privacy Impact Assessments durchführen

Für jede Verarbeitungstätigkeit

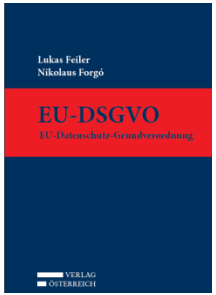
- Prüfen, ob prima facie ein hohes Risiko für Betroffene gegeben ist (z.B. sensible Daten, Profiling oder „schwarze Liste“ der Datenschutzbehörde)
  - Grds kein hohes Risiko, „wenn die Verarbeitung personenbezogene Daten von Patienten oder von Mandanten betrifft und durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufes oder Rechtsanwalt erfolgt“ (Erwägungsgrund 91 DSGVO)
- Nur wenn prima facie hohes Risiko gegeben ist: Privacy Impact Assessment durchführen
- Wenn PIA ein hohes Risiko ergibt: Konsultation mit der Datenschutzbehörde

Datenschutzrelevante Unternehmensrichtlinien

Datenschutzrelevante Unternehmensrichtlinien erstellen

- Richtlinie zum Umgang mit personenbezogenen Daten
- Richtlinie zur Informationssicherheit
- Richtlinie zur Reaktion auf Zwischenfälle
- Richtlinie zur Nutzung der Unternehmens-IT
- …

Baker McKenzie.



Dr. Lukas Feiler, SSCP CIPP/E
Senior Associate
Leiter des Teams für IT-Recht in Wien

Schottenring 25
1010 Vienna

T: +43 1 24 250
lukas.feiler@bakermckenzie.com

Lukas Feiler ist Co-Autor des ersten österreichischen Kommentars zur Datenschutz-Grundverordnung und begleitet Unternehmen auf www.digitalwave.at bei der digitalen Transformation

www.bakermckenzie.com