

Unterschätzte Anforderungen der Datenschutz-Grundverordnung an den technischen Datenschutz

Merlin Backer LL.M. (Glasgow), davit AG IT-Recht im DAV | HK2 Rechtsanwälte
CeBIT, 20.03.2017



- 1 Datenschutz-Grundverordnung
- 2 **Schwerpunkte**
 - TOM + Stand der Technik
 - Rechenschaftspflicht
 - Auftragsverarbeitung von Daten
- 3 **Konkreter Umsetzungsbedarf**



Die Datenschutz-Grundverordnung

- Datenschutz-Grundverordnung (DSGVO) wurde im Mai 2016 verabschiedet
- Inkrafttreten der Regelungen nach zweijähriger Übergangsfrist am **25.05.2018**
- DSGVO schafft ein einheitliches Datenschutzrecht in ganz Europa
- Wirkt unmittelbar und löst nationales Datenschutzrecht in weiten Teilen ab
- BDSG wird angepasst und enthält Öffnungsregeln
- Verpflichtet Unternehmen und die öffentliche Verwaltung gleichermaßen

Datenschutzprinzipien, Art. 5 & 25 DSGVO



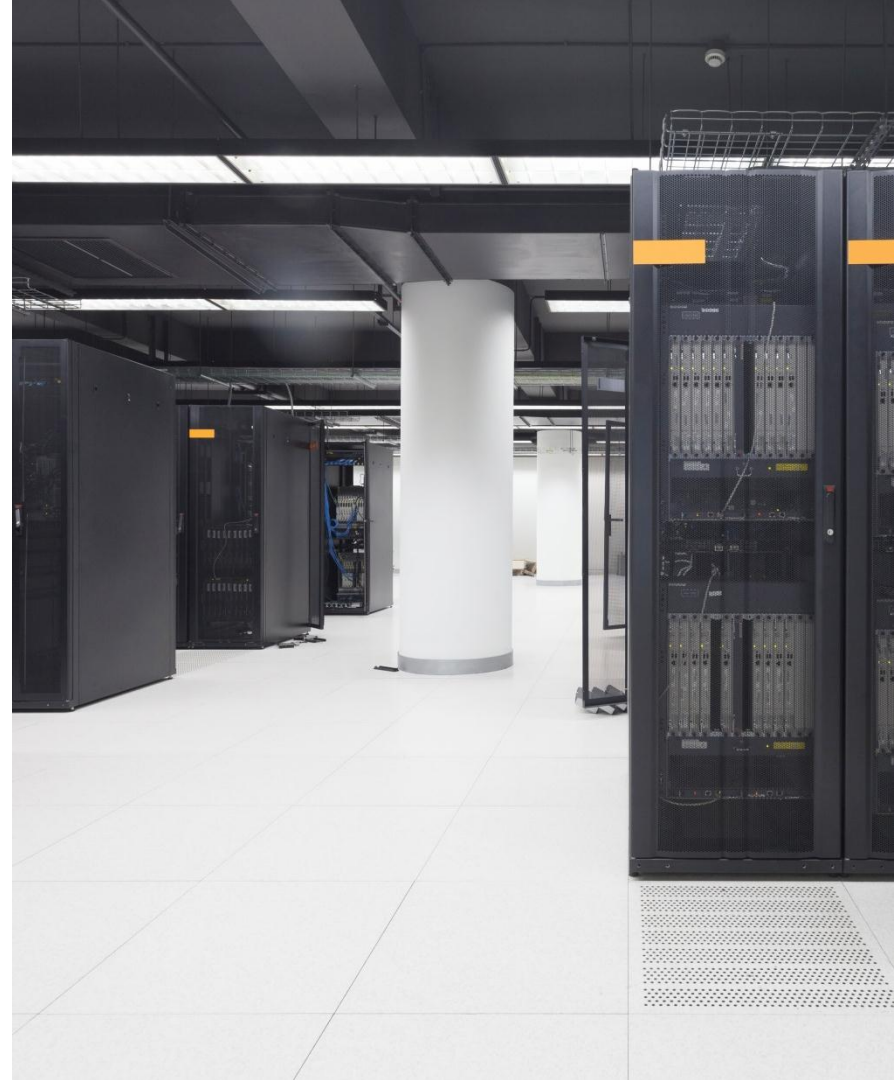
Folgen von Verstößen



- § 43 BDSG: Bußgelder bis max. EUR 300.000
- Art. 83 DSGVO: Bußgelder bis EUR 20.000.000 oder 4 % des weltweiten Vorjahresumsatzes

Technische und organisatorische Maßnahmen

- Keine Vorgabe von Maßnahmenkategorien wie in § 9 BDSG und Anlage zum BDSG
- Künftig müssen Vorgaben des Art. 32 DSGVO umgesetzt werden
- Abwägung der Maßnahmen nach Schutzbedarfsanalyse
- Anforderungen an Maßnahmen ähnlich den IT-Sicherheitsgesetzen, vgl. § 13 Abs. 7 TMG
- Rechenschaftspflicht über Maßnahmen nach Art. 5 Abs. 2 DSGVO



Art. 32 DSGVO: Sicherheit der Verarbeitung

Gewährleistung eines dem Risiko angemessenen Schutzniveaus



Geeignete technische und organisatorische Maßnahmen (TOM)



Berücksichtigen

Eintrittswahrscheinlichkeit und Schwere des Risikos
einer Rechtsverletzung (Schutzbedarfsanalyse)

Art, Umfang, Umstände, Zweck der Verarbeitung

Stand der Technik

Katalogmaßnahmen

Implementierungskosten



Stand von Wissenschaft
und Forschung



Stand der Technik



Anerkannte Regeln der
Technik



Ermittlung des Standes der Technik

- Innerhalb / außerhalb der Branche
- National / international
- Bewertung

- Beratung
- Arbeitshilfen (Handreichung zum Stand der Technik, TeleTrust)
- Dokumentation
- Nachweis

DSGVO: Umfangreiche TOM-Dokumentation

- Konsequenz: umfangreiche Abwägung aller Maßnahmen und Dokumentation des Auswahlprozesses
 - Durchführung einer Schutzbedarfsanalyse zur Bestimmung des erforderlichen Schutzniveaus und der dafür nötigen TOM
 - Abgleich sämtlicher TOM mit dem Stand der Technik: bei Nichteinhaltung Begründungspflicht
- Aus der jetzigen TOM-Liste muss künftig eine umfangreiche TOM-Dokumentation werden

Auftragsverarbeitungs- Vereinbarung, Art. 28 DSGVO

- Auftragsverarbeiter haftet direkt gegenüber Betroffenen
- Keine Beschränkung auf Datentransfer innerhalb EU/ EWR
- Neue Möglichkeit gemeinsamer Verantwortlichkeit für Datenverarbeitung
- Art. 28 Abs. 3 c): Stand der Technik muss im Rahmen der TOM berücksichtigt werden



Datenschutz-Folgenabschätzung, Art. 35 DSGVO

- Ähnlich wie § 4d Abs. 5 BDSG, aber größerer Anwendungsbereich
- Beurteilung im Vorfeld der Verarbeitung
 - Voranalyse: wenn „voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen“
 - Voranalyse identisch mit Abwägung nach Art. 32 DSGVO
- Pflicht zur Konsultation der Aufsichtsbehörde, wenn hohes Risiko festgestellt wird
- Pflicht des Auftragsverarbeiters zur Mitwirkung, Art. 28 Abs. 3 f)

Projektierung der Maßnahmen

- ✓ Differenzanalyse IST - SOLL
- ✓ Datenschutz- und IT-Sicherheitsprozesse prüfen und ggf. anpassen
- ✓ konsolidierte Umsetzung der Maßnahmen planen (ITSiG - DSGVO)

- ✓ Anpassung bestehender Verträge mit IT-Sicherheitsbezug
- ✓ Besonderheit: Vereinbarungen zur Auftrags(daten)verarbeitung an DSGVO anpassen

- ✓ Dokumentieren (neue Rechenschaftspflicht gem. Art. 5 Abs. 2 DSGVO)
- ✓ regelmäßig revidieren und Umsetzung prüfen

HK2
Rechtsanwälte

Rechtsanwalt, LL.M. (Glasgow)

Merlin Backer

Hausvogteiplatz 11 A
10117 Berlin

Telefon +49 (0)30 27 89 00-0

Telefax +49 (0)30 27 89 00-10

E-Mail backer@hk2.eu

www.hk2.eu