

Mag. Andreas Krisch
andreas.krisch@mksult.com

Die neue Datenschutz- Grundverordnung

Warum Datenschutz?

- Ein Mensch – Mehrere Rollen
 - Arbeitsleben
 - Familienleben
 - Freundeskreis
 - ...
 - Aktives Identitätsmanagement
 - Privatsphäre
 - Räumlich
 - Dezisional
 - Informationell
-

Warum Datenschutz?

- Datenschutz ist eine Maßnahme zum Schutz der Privatsphäre
- Datenschutz und Privatsphäre sind notwendige Voraussetzungen für eine funktionierende Demokratie

■ EU Datenschutzreform

- Verhandlungen
 - 01 / 2012: Entwurf der EU-Kommission
 - 03 / 2014: 1. Lesung im EU-Parlament
 - 06 / 2015: Einigung auf Position des Rates
 - 12 / 2015: Politische Einigung EP / Rat / COM
 - 05 / 2016: Beschlussfassung / Verlautbarung
 - 25.05.2018: Inkrafttreten

Vertrauen in Digitale Wirtschaft

- Eurobarometer 431 Datenschutz (06/2015)
 - 15 % glauben sie haben Daten online unter Kontrolle
 - 2/3 machen sich über diesen Kontrollverlust Sorgen
 - 62 % vertrauen Telefonieanbietern und ISPs nicht
 - 63 % vertrauen Online-Diensteanbietern nicht

■ Datenschutz Rechtsdurchsetzung

- Verordnung statt Richtlinie (Harmonisierung)
- Deutlich erhöhter Strafraumen
 - 10 Mio. EUR oder 2 % des Jahresumsatzes
 - 20 Mio. EUR oder 4 % des Jahresumsatzes
- Deutlich gestärkte Rechtsdurchsetzung
 - Mehr Befugnisse für Aufsichtsbehörden
 - Bessere Koordination / Kooperation von Aufsichtsbehörden
 - Mehr Nachkontrolle statt Vorabprüfung

■ Datenschutz Grundsätze

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
 - Zweckbindung
 - Datenminimierung
 - Richtigkeit
 - Speicherbegrenzung (= Löschpflicht)
 - Integrität und Vertraulichkeit (= Schutz vor unbefugter Verarbeitung, Zerstörung, ...)
 - Rechenschaftspflicht (Einhaltung nachweisen)
-

Entfallene Regelungen

- Datenschutz für juristische Personen
 - Ist in DSGVO nicht vorgesehen
 - Nationale Regelung evtl. noch möglich
- Indirekt personenbezogene Daten
 - Bisherige Erleichterungen entfallen (keine Auskunft- und Meldepflicht, ...)
 - Künftig genauso geschützt wie direkt personenbezogene Daten

■ Datenschutz-Grundverordnung

- Mehr Verantwortung für Auftraggeber
 - Dokumentationspflicht statt Meldepflicht
 - Privacy by Design / Default
 - Zertifizierungsmöglichkeiten
 - Durch Datenschutzbehörden
 - Betriebliche Datenschutzbeauftragte
 - Schwache Regelung aber in manchen Fällen zwingend
 - (Zu) Viele Öffnungsklauseln f. Nationalstaaten
 - Profiling / Big Data ungenügend geregelt
-

■ Pflichten der Verantwortlichen

- Ergreifen geeigneter technischer und organisatorischer Maßnahmen (TOM; Nachweispflicht)
- Datenschutz durch Technikgestaltung / Datenschutzfreundliche Voreinstellungen
- Verzeichnis der Verarbeitungstätigkeiten (ersetzt Meldungen an DVR)

■ Datensicherheit

- Gewährleisten eines angemessenen Schutzniveaus durch:
 - Pseudonymisierung / Verschlüsselung von Daten
 - die Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste sicherzustellen
 - die Fähigkeit, die Verfügbarkeit von Daten bei einem technischen Zwischenfall rasch wieder herzustellen
 - ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der TOM

■ Datenschutz-Folgenabschätzung

- Bei voraussichtlich hohem Risiko
 - für die Rechte und Freiheiten natürlicher Personen
 - aufgrund der Form der Verarbeitung, der Verwendung neuer Technologien, der Art, des Umfangs, der Umstände und Zwecke der Verarbeitung
- Insbesondere bei
 - systematischer, umfassender Bewertung persönlicher Aspekte (inkl. Profiling)
 - umfangreicher Verarbeitung „sensibler“ Daten
 - systematischer, umfangreicher Überwachung öffentlich zugänglicher Bereiche

■ Datenschutzbeauftragter

- Verpflichtend zu bestellen, wenn
 - Verarbeitung durch Behörde / öffentliche Stelle erfolgt
 - Kerntätigkeit des Verantwortlichen in Verarbeitungen besteht, die umfangreiche, regelmäßige und systematische Überwachung von Personen erforderlich machen
 - Kerntätigkeit des Verantwortlichen in der umfangreichen Verarbeitung „sensibler“ Daten besteht (inkl. strafrechtlich relevanten Daten)

■ Mitarbeiter-Datenschutz

- Regelung möglich durch
 - Nationales Recht
 - Kollektivvereinbarungen
- Inhalt
 - Wahrung der menschlichen Würde, der berechtigten Interessen und Grundrechte der Betroffenen
 - Insbesondere hinsichtlich Transparenz der Verarbeitung, Übermittlungen innerhalb von Konzernen, Überwachungssystemen am Arbeitsplatz

■ Umsetzung in AT-Recht

- Verordnung ist unmittelbar wirksam
 - Keine Umsetzung erforderlich
- Aber
 - Zahlreiche „Öffnungsklauseln“ für nationale Anpassungen
 - Änderung des DSG 2000 erforderlich
 - Mitarbeiter-Datenschutz-Gesetz?
 - ...

Safe Harbor / Privacy Shield

- EuGH hob im Fall Schrems Safe Harbor auf
 - Standardklauseln / BCR derzeit noch verwendbar
 - Nachfolge Abkommen „Privacy Shield“
 - Derzeit in Verhandlung
 - Ablehnung der Art. 29 Gruppe
 - Ablehnung des EP
 - Ablehnung des EDPS
 - Ausgang ungewiss
-

Mag. Andreas Krisch
andreas.krisch@mksult.com

Vielen Dank
für Ihre
Aufmerksamkeit!