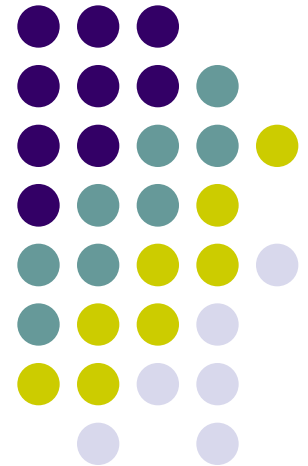


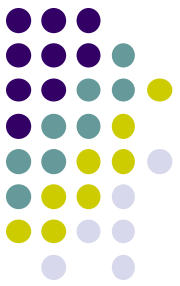
Datenschutz- Grundverordnung

Dr. Gregor König, LL.M.

Club-IT, 21. Februar 2017



Heute: Datenschutz-Richtlinie

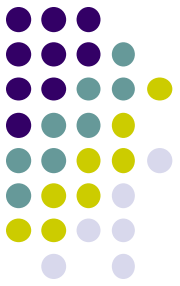


- „Datenschutz-Richtlinie“ 95/46/EG
 - ... des europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr
- Adressat: EU-Mitgliedstaat
- Ziel:
 - Schaffung eines gemeinsamen, **gemeinschaftlichen Datenschutzstandard**
 - Datenschutz innerhalb der EU zu gewährleisten
 - gleichzeitig möglichst freien Datenfluss sicherzustellen
 - → Bandbreiten-RL
- Anwendungsbereich: alle **personenbezogenen Daten natürlicher Personen, unabhängig von der Art der Verarbeitung**
 - also sowohl die vollständig, teilweise oder auch gar nicht automatisierte Verarbeitung persönlicher Daten
- Umsetzung: in AT das DSG 2000

Morgen: Datenschutz- Grundverordnung



- Datenschutz neu
 - **VERORDNUNG** 2016/679 des EP und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Warenverkehr (Datenschutz-Grundverordnung - DSGVO)
 - ersetzt RL 95/46/EG
 - (**RICHTLINIE** für den Bereich der Strafverfolgung)
- Werdegang
 - Vorschlag im Jänner 2012
 - Seit 27. April 2016 nach mehr als 4jährigen Verfahren im Abl der EU
 - Ab **25. Mai 2018 in Geltung und damit verbindlich**
- Adressat: **unmittelbar** alle Rechtsunterworfenen
- ein **einheitlicher Rechtsakt** für alle Mitgliedstaaten
 - aber: „hinkende VO“: viele Öffnungsklauseln, „delegierte Rechtsakte“, „Standardformate“, etc.



Eckpunkte

- personenbezogene Daten
 - Definition: „Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist“
 - Sensible Daten = besondere Kategorien von personenbezogenen Daten
 - rassistische und ethnische Herkunft
 - politische Meinung, Gewerkschaftszugehörigkeit
 - religiöse oder weltanschauliche Überzeugung
 - Gesundheitsdaten, Sexualleben
 - genetische/biometrische Daten zur eindeutigen Identifizierung einer Person
- Räumlicher Anwendungsbereich erweitert
 - Niederlassung in EU
 - Niederlassung nicht in der EU, aber
 - Waren- oder Dienstleistungsangebot an Unionskunden oder
 - Beobachtung des Verhaltens von Kunden, soweit dieses in der EU erfolgt
- Begriffe
 - Auftraggeber → Verantwortlicher
 - Dienstleister → Auftragsverarbeiter (NEU: mit eigenen Pflichten)

Zulässigkeit der Datenverarbeitung 1/3



- Grundsätze für die Verarbeitung (kumulativ)
 - Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
 - Zweckbindung: festgelegt, eindeutig und rechtmäßig; bei Ermittlung und Weiterverwendung
 - angemessen und erheblich („Datenminimierung“)
 - sachlich richtig („Richtigkeit“)
 - nur solange, wie für Zweckerreichung notwendig („Speicherbegrenzung“)
 - „Integrität und Vertraulichkeit“

Zulässigkeit der Datenverarbeitung 2/3



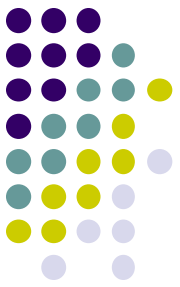
- Rechtmäßigkeit der Verarbeitung (alternativ)
 - Einwilligung
 - Erfüllung eines Vertrages
 - Erfüllung eines EU- oder nationalen Gesetzes
 - lebenswichtiges Interesse eines Beteiligten
 - Wahrnehmung einer Aufgabe im öffentlichen Interesse
 - Wahrung von berechtigten Interessen des Verantwortlichen oder eines Dritten
- Engere Voraussetzungen für „sensible Daten“

Zulässigkeit der Datenverarbeitung 3/3



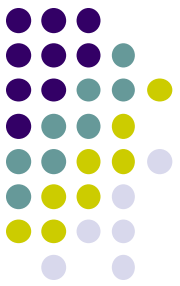
- Zusätzliche Voraussetzungen für internationalen Datenverkehr
 - Ziel: gleicher Rechtsschutz wie durch DSGVO in EU
 - Wie?
 - Angemessene Drittstaaten
 - Standardvertragsklauseln
 - Binding Corporate Rules
 - Genehmigte Verhaltensregeln
 - Sonderfälle wie EU-US-Privacy-Shield
 - in manchen Fällen Genehmigung der DSB erforderlich

Pflichten der Verantwortlichen



- Verantwortlichkeit der „Verarbeiter“ verschärft
 - Abschaffung des allgemeinen Meldeverfahrens zum DVR
 - Einführung von **Datenschutzbeauftragten** im Unternehmen
 - **Datenschutzfolgeabschätzung**/vorherige Konsultation
 - Risikofolgenabschätzung
 - verpflichtend bei
 - Bewertung persönlicher Aspekte (insb Profiling)
 - „umfangreiche“ Verarbeitung besonderer Kategorien pers.bez Daten
 - systematische „umfangreiche“ Überwachung öffentlich zugänglicher Bereiche
 - **Verzeichnis von Verarbeitungstätigkeiten**
 - Dokumentation, auch für Aufsichtsbehörde
 - verpflichtet auch den Auftragsverarbeiter

Der Datenschutzbeauftragte 1/3



- Verpflichtung ...
 - Behörden/öffentliche Einrichtungen
 - Kerntätigkeit: Durchführung von Verarbeitungsvorgängen, die eine regelmäßige und systematische Beobachtung von betroffenen Personen erforderlich machen
 - Kerntätigkeit: Verarbeitung von sensiblen/strafrechtlich relevanten Daten
 - Gruppe von Unternehmen darf gemeinsamen Datenschutzbeauftragten bestellen
 - Sonst: Berechtigung (mit Rechtsfolgen)
- Voraussetzungen
 - Berufliche Qualifikation, Fachwissen
 - Keine Interessenkonflikte mit anderen beruflichen Pflichten (Unvereinbarkeiten)
 - Ernennungsdauer nicht festgelegt
 - Extern/intern möglich
 - Veröffentlichung und Mitteilung an Datenschutzbehörde

Der Datenschutzbeauftragte 2/3



- Stellung
 - Beratungsorgan für Betroffene (Kunden)
 - „ordnungsgemäße und frühzeitige“ Einbindung in alle datenschutzrechtlich relevanten Fragestellungen
 - Unabhängigkeit (AG muss dafür sorgen)
 - Bericht an Unternehmensleitung
 - AG muss unterstützen
 - Personal
 - Räumlichkeiten
 - Ressourcen

Der Datenschutzbeauftragte 3/3



- Aufgaben („Mindeststandards“)
 - Unterrichtung/Beratung des AG über Pflichten aus DSGVO + Dokumentation
 - Überwachung der Umsetzung/Anwendung der Strategien des AG für Datenschutz
 - inkl Zuständigkeiten/Schulungen/Überprüfungen
 - Überwachung der Datenschutz-Folgeabschätzung bzw – auf Anfrage – Unterstützung
 - Zusammenarbeit mit der Datenschutzbehörde
 - bei Anfragen
 - bei Implementierung von ergriffenen Maßnahmen
 - dabei: Einbeziehung der Risiken, die mit Datenverwendung verbunden sind



Betroffenenrechte

- Recht auf **Information**
- Recht auf **Auskunft**
- Recht auf **Richtigstellung**
- Recht auf **Löschung/Widerspruch/Vergessenwerden/Einschränkung der Verarbeitung**
- Recht auf **Datenübertragbarkeit (Art 20)**



Weitere Inhalte ...

- Data Breach Notification Duty
 - ... in 2 Stufen
- Privacy by design, privacy by default
 - Zertifizierungen
 - „Datenschutz-Gütesiegel“
- Verhaltensregeln
- „Verbandsklagen“
- Behörden
 - nationale Aufsichtsbehörden
 - Europäischen Datenschutzausschuss

Strafbestimmungen



- derzeit: Verwaltungsstrafen bis max. € 25.000,--
- DSGVO: empfindliche Erhöhung
 - Strafraumen bis 20 Mio Euro bzw 4 % vom weltweiten (Konzern)Jahresumsatz, je nachdem, was höher ist
 - aber: konkrete Strafe muss wirksam, verhältnismäßig und abschreckend sein
 - Unternehmensstrafen, angelehnt an Wettbewerbsrecht
 - Strafbefugnis bei der DSB
 - pönalisiert werden
 - unrechtmäßige Datenverwendung
 - Nichteinhaltung der Pflichten des Verantwortlichen
 - unzureichende Erfüllung der Betroffenenrechte



Danke für Ihre Aufmerksamkeit !