Datenschutz und IT-Sicherheit

Ein grundsätzlicher Gegensatz?

Wolfgang Schnabl
www.expertslive.at
@securityXtrem

Dr. Wolfgang Schnabl

CISSP, CISA, ISO27001 Lead Auditor

- seit 1998 IT- und IS-Sicherheit
- seit 2008 Fa. Business Protection
- Lektor FH Hagenberg
- Mitglied $(ISC)^2$, ISACA, IT-Law
- seit 2010 Studium Rechtswissenschaften

Agenda

- Rechtssystem EU
- EU-Datenschutz-Grundverordnung
  - Ö: DSG 2000
  - EU: DSGVO
  - Ö: DSG
- Security vs. Datenschutz
  - Logging, Kontrolle
- Blickwinkel Security

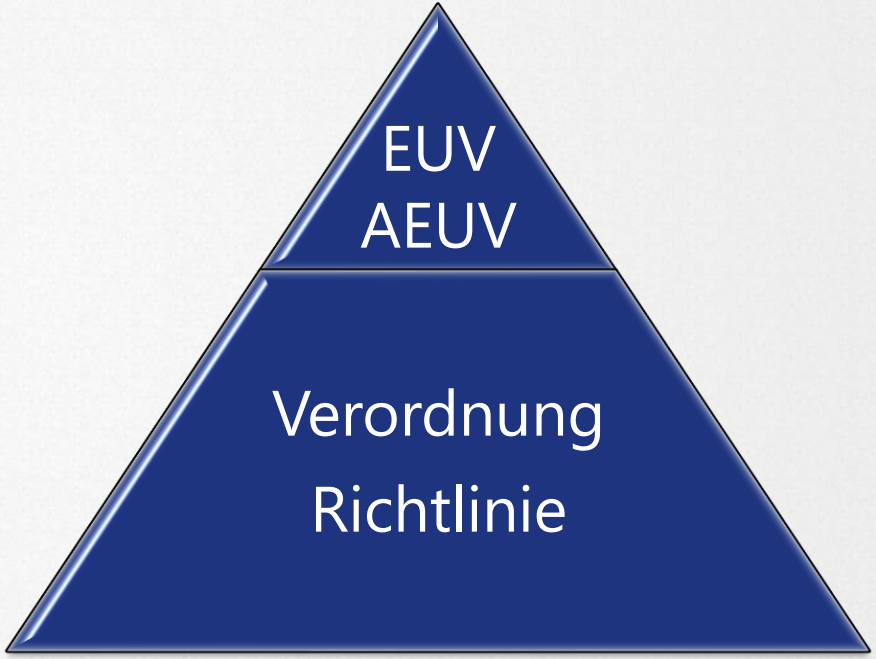
Gesetzliche Rahmenbedingungen

RECHTSSYSTEM DER EU

Recht – Österreich und EU

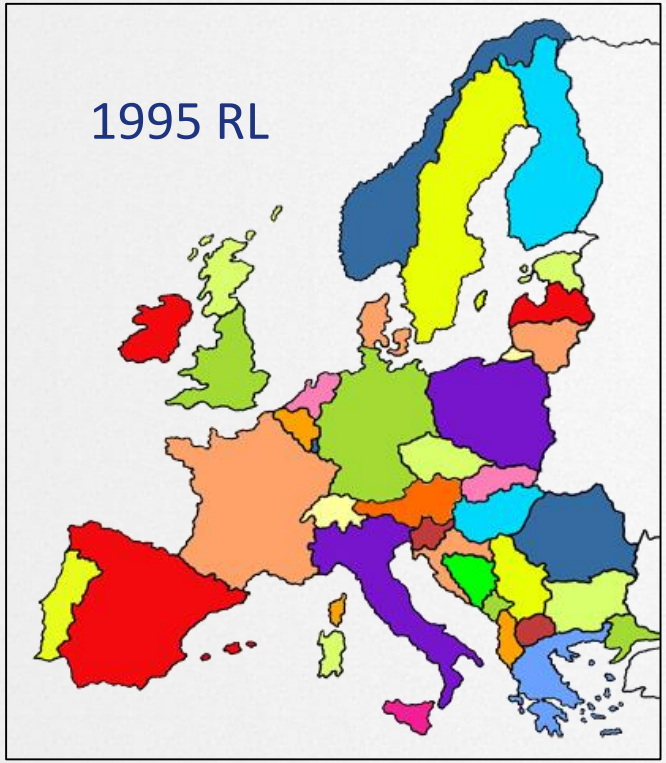
Stufenbau der Rechtsordnung

Recht – Österreich und EU



Stufenbau der Rechtsordnung

1995: 1 Richtlinie – 28 Datenschutzgesetze
2016: 1 Verordnung – 1 Datenschutzgesetz



DSGVO – Zeitachse

- 04.05.2016 Amtsblatt der EU veröffentlicht
- 25.05.2016 in Kraft getreten
- **25.05.2018 DSGVO anwendbar**

Gesetzliche Rahmenbedingungen

EU-DATENSCHUTZ-GRUNDVERORDNUNG

Personenbezogene Daten (Art. 4 Z 1)

- natürlicher Personen
  - identifiziert oder identifizierbar
  - indirekt personenbezogene Daten
    - Pseudonymisierung (Art. 4 Z 5)
- besondere Kategorien (Art. 9 Abs. 1)
    - Rassische/ethnische Herkunft
    - Politische Meinungen
    - Religiöse oder weltanschauliche Überzeugungen
    - Gewerkschaftszugehörigkeit
    - Genetischen Daten, biometrischen Daten
    - Gesundheitsdaten, Sexualleben

Personenbezug

- Name, Adresse, Mitglieds-, Personalnummer
- Bild- und Tondaten, biometrische Daten, technische Kennzahlen (z.B. Stromverbrauch), …
- E-Mail-Adresse **?**
  - **Ja** (OLG Bamberg/D 1U143/04)
- IP-Adresse **?**
  - **Ja** (DSK 213.005/0005-DSK/2006)
- **DSGVO**
  - IP-Adressen und Cookie-Kennungen **(#30)**

Grundsatz

Jede Verwendung personenbezogener Daten ist verboten*

* **Ausnahmen!**

Ausnahmen

- Ausdrückliche gesetzliche Ermächtigung
- Erfüllung von Vertrag
  - Nur erforderliche Daten für Vertragserfüllung
- Betroffene hat zugestimmt (Widerrufsrecht)
  - Nachweisbare Einwilligung
  - Freiwillig
- Berechtigte Interessen Dritter
- Lebenswichtige Interessen des Betroffenen
- Wichtiges öffentliches Interesses

Prinzipien (Art. 5)

- **Transparenz**
  - rechtmäßig
  - nach Treu und Glauben
  - nachvollziehbar
- **Zweckbindung**
  - festgelegt, eindeutig und rechtmäßig
  - Nicht auf Vorrat
    - Data-Warehousing, Data-Mining
- **Datenminimierung**
  - angemessenes und notwendiges Maß
    - Pseudonymisierung, Privacy-by-Default → vs. Big-Data

Bereits DSG 2000

- Datenschutzerklärung auf Webseite

> **Datenschutzerklärung**
>
> Wir erheben, verarbeiten und nutzen Ihre Daten nur im Rahmen der gesetzlichen Bestimmungen.

- Warum problematisch?
  - festgelegte, eindeutige und rechtmäßige Zwecke

Prinzipien (Art. 5)

Bereits DSG 2000

- **Richtigkeit**
  - richtig und aktuell
  - unverzügliche Löschung / Berichtigung
- **Speicherbegrenzung**
  - höchstens so lange, wie erforderlich
- **Integrität** und **Vertraulichkeit**
  - technische und organisatorische Maßnahmen
    - unbefugte Verarbeitung
    - zufälliger Verlust

Haftung

- Bisher – DSG 2000
  - Max. 25.000.- EUR
- Neu – DSGVO
  - Max. 20.000.000.- EUR (20 Mio)
  - oder 4 % Jahresumsatz weltweit

  (Je nachdem, was *höher* ist)

  Strafe: wirksam, verhältnismäßig und abschreckend
- Beweislastumkehr
  - Alt: Nachweispflicht durch Behörde
  - **Neu**: Unternehmen beweist Rechtskonformität

Selbstbeurteilung

- **Selbstbeurteilung** durch interne Dokumentation
  - **Entfall der Meldepflicht** bei DSB
    - DVR wird aufgelassen
  - **Verarbeitungsverzeichnis**
    - > 250 Mitarbeitern
    - Risiko für Betroffenen-Rechte
    - Nicht nur gelegentlich
    - Sensible oder strafrechtliche Daten

Datenschutz-Folgenabschätzung (Art. 35)

- systematische **Beschreibung** geplanter Verarbeitungsvorgänge
- **Bewertung** - Notwendigkeit und Verhältnismäßigkeit
- **Risikobewertung -** Betroffenenrechte
- geplante **Maßnahmen** gegen Risiken

- Datenschutzbehörde
  - Kann erstellen: Positiv / Negativliste
    (in Ö noch nicht erfolgt § 21 Abs. 2 DSG)

Rechte von Betroffenen

- **Informationspflicht** (Art. 13)
  - Zweck und Rechtsgrundlage
  - Dauer der Speicherung
  - Externe Empfänger
  - Auskunftsrecht, Beschwerderecht
  - Widerruf möglich
  - Welche Daten nötig und Folgen einer Nicht-Bereitstellung

Schutz der Privatsphäre

- **„Informationelle Selbstbestimmung“**
- Geschützte Rechte
  - Geheimhaltung
  - Auskunft (Art. 15)
  - Berichtigung (Art. 16)
  - Löschung: „Recht auf Vergessenwerden“ (Art. 17)
    - Informationspflicht an Dritte
  - Einschränkung der Verarbeitung (Art. 18)
    - Nur Speicherung erlaubt

Meldepflicht

- Meldepflicht bei Verletzung (Art. 33, 34)
  - An Betroffene **unverzüglich**
  - An Aufsichtsbehörde innerhalb **72 Stunden**
  - Definierte Information
  - Dokumentationspflicht

Österreich – Anpassungsgesetz

- Name: Datenschutzgesetz – DSG
- Anwendbarkeit
  - Elektronisch und Papier
- Backup: „herauswachsen“
- Mitarbeiter: Datengeheimnis
- DS-Behörde: „weiße“ und „schwarze“ Listen
- Zustimmung Kinder: 14 Jahre
- Beschwerde bei DS-Behörde und BVwG
- Akkreditierung von Zertifizierungsstellen
- Befugnisse im ArbVG bleiben

Logging und Kontrolle

SECURITY VS. DATENSCHUTZ

Typisches

Datenlieferanten

- Anwendungen
  - Internet-Browser
- Services
  - Datenbank-Server
  - Proxy-Server
  - Web-Server
  - E-Mail-Server
- Netzwerkkommunikation
  - Überwachungstools (FW, AV)
  - Netzwerkkomponenten

Logfile-Daten

- Weblog
  - IP-Adresse
  - HTTP-Benutzername
  - Datum und Uhrzeit
  - Aufgerufene Seite
  - Referer
  - Statuscode, UserAgent
- E-Mail-Log
  - Quell- und Ziel-IP-Adresse
  - Absender und Empfänger
  - Statusmeldungen

Warum Logging

- **Vorgaben aus Gesetz**
  - Datenschutzgesetz
- **Vertragliche Verpflichtungen**
  - Schutz von Geschäftsgeheimnissen
- **Unternehmensseitige Regelungen**
  - Informationssicherheit
  - Statistiken

Warum Logging

- Governance
  - AktG § 82, GmbHG § 22

    „Der **Vorstand/GF** hat dafür zu sorgen [...] dass ein **internes Kontrollsystem** geführt wird, [...]“.
  - Dies gilt auch für Bereich IT-Sicherheit
    - da Verfügbarkeit, Integrität, Vertraulichkeit der IT-Infrastruktur **Grundlage** des **Geschäftsbetriebs**
  - Vorstand **proaktiv** für IT-Sicherheit verantwortlich

Compliance

- **Compliance Gedanke**
  - Haftungsentlastung bei Konvergenz zwischen Technik und Recht

- **Compliance**
  - **Einhaltung** – Gesetze & Richtlinien
  - **Einrichtung** – Kontrolle und Steuerung
  - **Dokumentation** – Prozesse

Kontrolle

LOGGING UND MITARBEITER

Mitarbeiterkontrolle

- Web-Surfen
- E-Mail, IM/Chat/Blogs etc.
- Keylogger, Screenshots etc.

- Durch **direkte** Beobachtung von Vorgesetzten
  - Rechtlich **kein** Problem
  - Mitarbeiter zur Arbeit verpflichtet, diese darf auch von anderen **Menschen** überwacht werden
  - Datenschutz erst bei Aufzeichnung relevant

Logging erlaubt

- Berechtigte Interessen Dritter
  - DSGVO #49
- Betroffene hat zugestimmt (Widerrufsrecht)
  - Betriebsvereinbarung § 96 (1) Z 3 ArbVG
  - Einzelverträge § 10 AVRAG

Erwägungsgrund #49

Die **Verarbeitung** von personenbezogenen Daten **durch** Behörden, Computer-Notdienste (CERT, CSIRT), Betreiber von elektronischen Kommunikationsnetzen und -diensten sowie durch Anbieter von Sicherheitstechnologien und -diensten **stellt** in dem Maße ein **berechtigtes Interesse** des jeweiligen Verantwortlichen dar, wie dies **für** die Gewährleistung der Netz- und **Informations-sicherheit** unbedingt **notwendig und verhältnismäßig** ist, […].

Ein solches berechtigtes Interesse könnte **beispielsweise** darin bestehen, den **Zugang Unbefugter** zu elektronischen Kommunikationsnetzen und die **Verbreitung schädlicher Programmcodes** zu verhindern sowie Angriffe in Form der **gezielten Überlastung** von Servern („Denial of service"-Angriffe) und Schädigungen von Computer- und elektronischen Kommunikationssystemen **abzuwehren**.

Betriebsvereinbarung

- **Zustimmungspflichtige Maßnahmen**
  § 96 (1) Z 3 ArbVG (bzw. § 10 AVRAG)
  - Einführung von […] technischen Systemen zur Kontrolle der Arbeitnehmer, sofern diese die **Menschenwürde berühren**
    - **Nicht berühren** – unproblematisch
      zB kein Personenbezug
    - **Berühren** – Betriebsvereinbarung
      zB Fingerabdruck-Scanner
      (OGH, 9 ObA 109/06d)
    - **Verletzen** – nicht möglich
      zB geheime Überwachungsprogramme

Beispiel Internet

- **Kontrolle**
  - Verhalten oder Leistung
    - zB Internet, E-Mails
  - Aufzeichnung (ohne Auswertung) reicht

- **Logfiles**
  - keine Betriebsvereinbarung nötig
    - Anonymisierte Zugriffsstatistiken
    - Proxy-Server (bzw. Cache) ohne Kontrolle und in kurzen Abständen wieder gelöscht (Anm.: **entgegen OGH**)
  - Betriebsvereinbarung nötig
    - Sofortige Kontrollen
    - Speicherung ohne (sofortige) Kontrollen

Privatnutzung

- **Nur dienstliche Nutzung**
  - Menschenwürde **kann nicht (?)** betroffen sein
  - Jedoch
    - **Pop-Ups** mit „privaten“ Inhalt
    - Mitarbeiter **erhält** private E-Mails
    - Guter Verkäufer **sendet** „gemischte“ E-Mails
    - „Notfall“
- **Privatnutzung nicht verboten**
  - Menschenwürde **ist** betroffen

Speicherdauer

- Grundsätzlich
  - Löschen, sobald nicht mehr benötigt (Zweckerfüllung)

- Beispiele – Web-Logs
  - **14 Tage**
    - K121.259/0013-DSK/2007 (MA vs. BMF)
  - 3 Wochen - nicht unverhältnismäßig
    - K121.358/0009-DSK/2008 (MA vs. BMF)

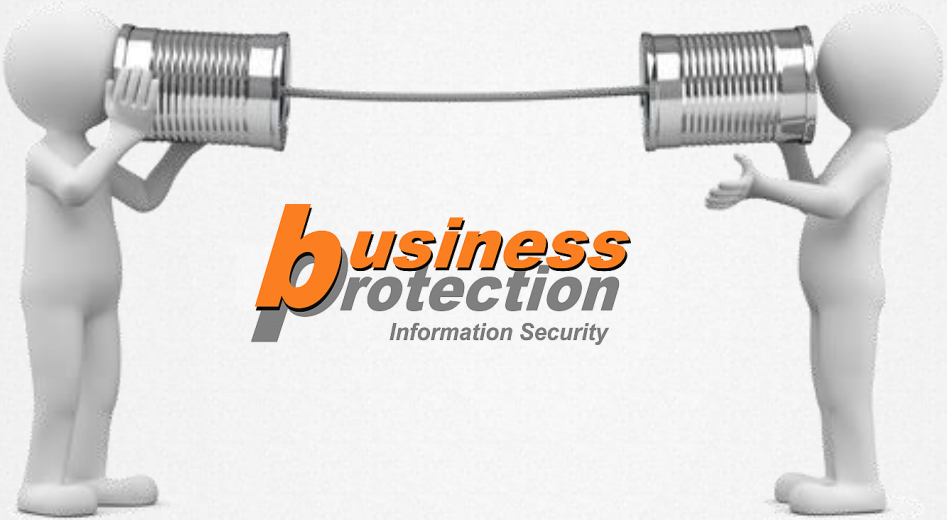
Klare Richtlinien

- Logging-Policy
  - Zweck – Dauer – Auswertung – Tools
  - Speicherung lokal/zentral
  - Wer Zugriff lesenden/schreibenden
- Informationspflicht (Mitarbeiter + Web)
  - Was – Warum – Wie lange
- Acceptable Use Policy
  - Privatnutzung J/N

Klare Richtlinien

- Sicherheitsrichtlinie
  - Verschlüsselung, Antivirussoftware, Passwort
- Betriebsrat nötig
  - Praktisch immer!
- Kontrollrechte des Arbeitgebers
  - regelmäßig, nur im Verdachtsfall, in welcher Form
- Beendigung des Arbeitsverhältnisses
  - Herausgabe, Löschung von Unternehmensdaten
- Administrator
  - NDA, Datenschutz-Schulung

Kontakt



Dr. Wolfgang Schnabl, CISSP, CISA
ISO 27001 Lead Auditor

schnabl@business-protection.at

www.business-protection.at
www.security-awareness.at
www.dataprotection-officers.eu

Thanks to our Sponsors!