Skriptum: Datenschutzrecht und Technik im Kontext der DSGVO

Thema: Recht und Technik – DSGVO, österreichische Besonderheiten, technische Umsetzung und praktische Herausforderungen

---

1. Einführung & Überblick

- **Thema:** Kombination aus **Recht** und **Technik** im Datenschutz
- **Kontext:** DSGVO (Datenschutz-Grundverordnung) seit 25. Mai 2018 in Kraft
- **Österreichische Besonderheit:** Vor 2018 eigenes **Datenschutzgesetz (2000)** und **Datensicherheitsgesetz** – Österreich war **2001 erste Nation in Europa** mit dediziertem Datenschutzgesetz
- **Aktuelle Rechtsgrundlage:** DSGVO + **Datenschutz-Anpassungsgesetz (Österreich)**

---

2. Grundbegriffe der DSGVO

Begriff	Definition	Beispiele
Personenbezogene Daten	Alle Informationen, die eine natürliche Person **identifizieren** oder **identifizierbar** machen	Name, Adresse, Religion, Hausfarbe, Gesundheitsdaten
Besondere Kategorien (sensible Daten)	Daten mit **besonders schützenswertem Charakter**	Rasse, ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, Gesundheit, Sexualleben, biometrische Daten
Datenverarbeitung	Jeder Vorgang mit personenbezogenen Daten (Erhebung, Speicherung, Nutzung, Löschung)	**Altes österr. Gesetz:** Speicherung > **0,5 Millisekunden** = Verarbeitung

---

3. Rechte der betroffenen Personen („Extended Version“)

- **Recht auf Löschung** („Recht auf Vergessenwerden“)

- **Recht auf Berichtigung**
- **Recht auf Einschränkung der Verarbeitung**
- **Recht auf Datenübertragbarkeit**
- **Widerspruchsrecht**
- **Recht auf Auskunft**

Realität: Formal vorhanden, aber **Durchsetzung oft schwierig**
→ „In der Realität können wir uns ab rausgehen gehen“

---

4. Historisches österreichisches Datenschutzrecht (vor 2018)

Merkmal	Details
Datenschutzgesetz 2000	Technisch **sehr präzise**, aber **kein rechtlicher Hebel** zur Durchsetzung
Datenverarbeitungsregister (DVR)	Zentrales Register bei der **Datenschutzbehörde**
DVR-Nummer	Pflicht bei Massenversand (z. B. Rechnungen, Werbung) → **heute noch auf Postzusendungen sichtbar**
Auskunftsrecht	Gegen Gebühr („Einwurf von Münzlern“) → Liste aller Firmen, die Daten verarbeiten (Antwortfrist: **3 Monate**)

Nachteil: Kein **gesetzlich garantiertes Durchsetzungsrecht auf Löschung**

---

5. DSGVO vs. altes österreichisches Recht

Aspekt	Altes Recht (AT)	DSGVO
Präzision	Sehr hoch (technisch)	Weniger präzise, aber einheitlich EU-weit
Durchsetzbarkeit	Schwach	Stark (Geldbußen, Klagsrecht)

Aspekt	Altes Recht (AT)	DSGVO
Register	Zentral (DVR)	**Dezentral** – **jeder Verantwortliche führt eigenes Verzeichnis**
Meldepflicht bei Datenpannen	Keine	**72-Stunden-Frist** (in AT: Wochenende dazwischen erlaubt → Montag 9 Uhr möglich)

Österreichische Ausnahme: Dank Intervention → **keine 7×24-Besetzung** der Meldestelle

---

6. Datenschutzbehörde & Datenschutzkommission (AT)

Datenschutzkommission

- Zusammensetzung:
  - Vertreter der **Bundesländer**
  - **Sozialpartner**
  - **Ministerien**
  - **Bundeskanzleramt**
  - **Bundeskanzler kann 2. Person entsenden → politische Mehrheit**

Datenschutzbehörde

- **Exekutivorgan** → zuständig für **Durchsetzung**
- **Meldepflicht bei Datenpannen:**
  - Kein **standardisiertes Formular** (Stand 2025!)
  - Abhängig vom **Beamten** vor Ort
  - **Polizeikommissariate:** Nur **eingeschulte Beamte** (Doppelstunde!)
  - Formular → Innenministerium → Journaldienst → **innerhalb 8 Stunden** Entscheidung: Weiterleitung oder „Waste-Time“

---

7. Technische & Organisatorische Maßnahmen (TOMs)

Prinzip	Inhalt
Privacy by Design	Datenschutz **von Anfang an** einplanen
Privacy by Default	Standardeinstellungen = **maximale Sicherheit**
Zumutbarkeit	Maßnahmen müssen **wirtschaftlich vertretbar** sein → **Streitpunkt!**

Beispiel: E-Mail-Verschlüsselung & Signatur

- **Sachverständige** entscheiden, ob Maßnahme **zumutbar**
- **Richter** hat letztes Wort (Zivilprozess)
- **Schöffen** entscheiden bei Strafprozessen

  Kosten: - Verurteilung: oft nur **einige hundert Euro** - **Anwalts- & Sachverständigenkosten:** bis zu **Millionen** (z. B. ÖBB: 400.000 € Strafe, aber 4,5 Mio. € Verfahrenskosten)

---

8. Verantwortlicher vs. Auftragsverarbeiter

Rolle	Definition	Haftung
Verantwortlicher	Entscheidet über **Zweck und Mittel** der Verarbeitung	**Vollhaftbar** (z. B. IKEA)
Auftragsverarbeiter	Führt Verarbeitung **im Auftrag** durch	Nur bei **Vertragsverletzung**

Pflicht: Verarbeitungsverzeichnis (AVV)

- **Vertraglich** geregelt
- **Keine E-Mail** ausreichend
- Muss enthalten:
  - Anwendung der DSGVO
  - **Konkrete Schutzmaßnahmen**

  Beispiel IKEA-Druckerei: - Druckerei gehackt → **Konkurs** wegen Kosten - **IKEA bleibt verantwortlich → beide verurteilt**

---

9. Datenschutzbeauftragter (DSB)

Kriterium	Regelung
Pflicht	Nur bei:

- 250 Mitarbeiter **oder**
- Regelmäßige, systematische Verarbeitung sensibler Daten
- Öffentliche Stellen | | **Aufgaben** | **Beratung**, **Überwachung**, **Sensibilisierung** | | **Haftung** | **Keine – nur Geschäftsführer haftbar** | | **Kündigungsschutz** | **Darf nicht wegen DSB-Tätigkeit gekündigt werden** |

Realität: Oft „Schweizersessel“ – **viele Pflichten, keine Rechte**

---

10. Verarbeitungsverzeichnis (Art. 30 DSGVO)

Inhalt	Pflicht?
Kategorien personenbezogener Daten	Ja
Zweck der Verarbeitung	Ja
Empfänger	Ja
Löschfristen	Ja
Technische Details (z. B. Patch-Level)?	**Nein – nicht vorgeschrieben**

Problem: - Kein einheitliches Format - Unternehmen wissen oft nicht, ob sie vollständig sind - DSB hat keine Mittel zur Kontrolle

Beispiel Schule:

- **1 DSB für ganz Österreich** (Bildungsministerium)
- **Lehrkräfte dürfen nur dienstliche Software nutzen** (z. B. MS Office)
- **Private Tools (z. B. Excel lokal) → nicht erlaubt** bei sensiblen Daten
- **Sokrates** = offizielle Plattform → **keine Zustimmung für private Tools**

---

11. Ausnahmen von der DSGVO

Fall	Gilt DSGVO?
Persönliche / familiäre Tätigkeiten	Nein
Ein-Personen-Unternehmen (EPU)	Nein (z. B. Friseur, Fotograf)
Bestimmte Berufe	Ca. **80 Berufe in AT ausgenommen**
Polizei / Emergency Response Teams	**Ausnahme** → dürfen **uneingeschränkt zugreifen**

> **Kritik:** DSGVO dient auch **Polizeibehörden** → automatisierter Datenaustausch EU-weit

---

12. Datenschutz als Grundrecht

Rechtsgrundlage	Inhalt
EU-Grundrechte-Charta Art. 8	Schutz personenbezogener Daten
Österreichisches Staatsgrundgesetz	**Weitergehender Schutz** als DSGVO

> **Harmonisierungsziel:** 1. Schutz der Bürger 2. **Freier Datenverkehr in der EU** 3. **EU-weiter Polizeizugriff**

---

13. Technische Compliance & Sachverständige

Privacy by Design / Default

- **Default-Settings = maximale Sicherheit**
- **Zumutbarkeit** → Streitpunkt vor Gericht

Sachverständige

- **Voraussetzungen:**
  - Abgeschlossenes Studium
  - Prüfung **Straf-/Zivilprozessordnung**
  - Fachprüfung (z. B. DSGVO, TKG, Cybercrime)
  - **14-tägiger Kurs**

  - **Prüfung: 4.500 €, 1 Tag**
- **Honorar:** Mindestens **380 €/Stunde** (Ziviltechniker-Honorarverordnung)
- **Gutachten:** Mindestens **300 Stunden → 114.000 €+**
- **Haftung: Vollhaftbar** bei Fehlern

Beispiel Walter Rosenkranz: - Verweildauer auf rechtsradikaler Seite - **Logfile-Auswertung + Chain of Custody** erforderlich - **Manipulation wird sofort angezweifelt**

---

14. Datenpannen & Meldepflicht

- **72-Stunden-Frist**
- **Österreich:** Wochenende dazwischen → **Montag 9 Uhr möglich**
- **Kein Standardformular**
- **Polizei:** Nur **eingeschulte Beamte** (2 Stunden!)

---

15. Geschäftsführerhaftung

Szenario	Haftung
Datenschutzverstoß	**Geschäftsführer**
Arbeitsunfall (z. B. Stolpern)	**Geschäftsführer**
Maturastreich mit Folgen	**Schulleiter** (außer nachweislich außerhalb Dienstzeit)

Prozesssicherheit: - Portier muss **Rundgang dokumentieren** - **Compliance-Beauftragte** überwachen Prozesse

---

16. Wirtschaftliche Aspekte

Leistung	Kosten
Rechtsberatung (Kanzlei)	25.000–30.000 € / Tag
Security Audit	250.000–300.000 €
Sachverständigengutachten	$>$ 100.000 €
NIS-2 / DSGVO-Compliance-Abteilung	20–30 Mitarbeiter bei Großunternehmen

Goldgrube: IT-Security + Datenschutz → **hohe Nachfrage**

---

17. Praktische Tipps des Professors

1. **Kein Outsourcing außerhalb EU** → zu riskant (Beispiel: Kapsch in Kroatien → Reifeprüfungsergebnisse geleakt)
2. **Dokumentation ist alles** → Prozesse, Rundgänge, Verarbeitungsverzeichnis
3. **Sachverständiger werden? → Hohes Einkommen, aber hohe Haftung**
4. **DSGVO = Pyramidenspiel** → viele Berufe, viel Geld, viel Bürokratie
5. **Technische Beweissicherung → Chain of Custody** zwingend

---

18. Fazit

- **DSGVO = Harmonisierung + Durchsetzbarkeit**, aber **weniger technisch präzise** als altes AT-Recht
- **Österreichische Besonderheiten:** Wochenendregelung, politische Datenschutzkommission, dezentrales Verzeichnis
- **Technik entscheidet vor Gericht:** Sachverständige, Logfiles, Beweissicherung
- **Haftung liegt immer beim Geschäftsführer**
- **Datenschutz = Grundrecht**, aber auch **Wirtschaftsfaktor** und **Ermittlungsinstrument**
