

# Skriptum: DSGVO – Ergänzungen zu Rechten, Ausnahmen, Profiling & Umsetzung

**Thema:** Datenschutz-Grundverordnung (DSGVO) – Rahmenbedingungen, Durchsetzung, Profiling, Polizeizugriffe & technische Pflichten

---

## DSGVO-Rahmenbedingungen & Ausnahmen

Aspekt	Details
<b>Gefahr für Demokratie</b>	Verarbeitung personenbezogener Daten (z. B. politische Einstellungen) erlaubt, inkl. Weitergabe – z. B. Meinungs- und Forschungsinstitute. - Wer entscheidet über “Gefahr”? Nicht geklärt; potenziell Regierung.
<b>Politische Parteien</b>	Verarbeitung für Mitgliederverwaltung; Weitergabe an nahestehende Organisationen (z. B. Autofahrerclubs, Sportvereine, Rettungssysteme). - Kritik: Oft “Stuss”; führt zu ungewollter Weitergabe.
<b>Mitteilung an Betroffene</b>	Bei Erhebung mitteilen (meiste Verurteilungen hier, da oft ignoriert). - Ungültig: Kleingedrucktes (z. B. Rückseite Rechnung in 2-Punkt-Schrift).
<b>Ausnahmen von Mitteilung</b>	- Gesetzliche Regelungen (z. B. EVN-Rechnungen). - Berechtigtes Interesse Dritter. - Öffentliche Zugänglichkeit (z. B. freiwillig publizierte Adresse – kopierbar ohne Widerspruch).
<b>Medizinische Notfälle</b>	- Nur <b>Notarzt</b> darf Daten erfassen/verarbeiten (z. B. Blutgruppe anfragen). - <b>Sanitäter</b> verboten – Klage möglich, auch bei “Hilfe” (mehrfach passiert). - Beispiel: Öffentlicher Wortwechsel → Presse erfährt chronische Krankheit einer prominenten Person → Skandal.

---

## Durchsetzungsrechte & Prozesse

- **Recht auf Berichtigung/Löschung:**
  - Eingeschrieben auffordern (Firma hat 8 Wochen).
  - Bei Ignoranz: Datenschutzbehörde (weitere 8 Wochen pro Schritt).
  - Gesamt: Bis zu 48 Wochen ( $6 \times 8$ ) – oft Aufgabe durch Frustration.
  - Erfolg: Erlass + Strafen (2.000–10.000 €) – “zahnlos”.
- **Widerspruch bei öffentlicher Gewalt:**
  - Kein Widerspruch möglich (z. B. Polizei, Gerichte, Strafvollzug).
  - Rechtsgrundlage überwiegt.

---

## Profiling – Verbote & Ausnahmen

Definition	Beispiele	Regelung
<b>Profiling</b>	Erstellung von Bewegungsprofilen (z. B. in Mobilfunk, WLAN, IT-Netzen). - Digitale Fingerabdrücke (ohne Namen, aber rückführbar).	- Grundsätzlich <b>verboten</b> (fällt unter DSGVO; ähnlich Pseudonymisierung). - Firmen/Detektive dürfen nicht (keine Auskunft ohne Gerichtsbeschluss).
<b>Ausnahmen</b>	- Strafverfolgung: z. B. Täter in gleicher Funkzelle bei Verbrechen. - Gerichtliche Anordnung: Zur Klage/Verteidigung.	- Beweismittel: Richter entscheidet Zulässigkeit (Strafprozessordnung). - Muss “würdig” sein; Ablehnung nur mit Begründung.

- **Relevanz für IT:**
  - IP-Adressen, Telefonnummern, Social Media, Avatare = personenbezogene Daten.
  - Konflikt bei Security Audits: § 126 A/B StGB + DSGVO-Verstoß (außer CERT-Status).

---

## Polizeizugriffe & EKIS-System

- **EKIS (Erkennungsinformationssystem):**
  - In jedem Polizeifahrzeug: Zugriff auf Nummernschilder, Telefonnummern, Zulassungen, Wohnungen, Verurteilte, Hafttäter.
  - **Keine Protokollierung von Lesezugriffen** (trotz DSGVO).

- Missbrauch: Gerüchteweise für private Zwecke (z. B. “Bedrucker” checken).
- **Missbrauchsbeispiele:**
  - Polizisten in Freizeit: Uniform tragen, Dienstausweis missbrauchen – verboten.
  - Fall: Ehemann auf Dienstreise; Kollegen “passen auf” – Uniform im Wirtshaus, falsche Festnahme (Tischler statt Liebhaber), Schusswechsel, Aufdeckung durch WEGA.
  - Rache: Nach Freispruch maximale Ausnutzung (z. B. bei früherem Angriff auf Kollegen).
- **“Verdächtig”-Kriterium:**
  - Nicht geregelt; Entscheidung des Streifenpolizisten (Parkzettelverkäufer-Jargon).
  - Maßnahmen: Ausweiskontrolle (Pflicht zum Mitführen), Durchsuchung (z. B. weiße Flecken = Drogen?), Sicherheitsverwahrung (24 Stunden ohne Richter).
  - Über 24 Stunden: Haftrichter entscheidet.
  - Wiederholung: Möglich, aber unverhältnismäßig (schon passiert).
- **Transparenz international:**
  - 80% nördlicher Länder: Polizeitransparenzgesetz (Veröffentlichung von Anfragen pro Dienststelle).
  - Kanada: SMS bei Anfrage (ohne Details).
  - Österreich: Diskussion nach Fall des Amtsverschwiegenheitsgesetzes – Bürger könnte Anfragen einsehen.
- **Polizeigesetze:**
  - Polizeisicherheitsdienstgesetz: Vorfeld/Straftat-Vermeidung.
  - Schöffen entscheiden bei Konflikten (nicht Richter); Richter kann “Fehlentscheidung” korrigieren.

---

## Verantwortlichkeiten & Umsetzungspflichten

Pflicht	Details	Ausnahmen/Reformen
<b>Risikoanalyse</b>	Verpflichtend (Eintrittswahrscheinlichkeit von Bedrohungen: Verlust, Diebstahl, Manipulation, Löschung).	Immer; Reform: Alle 24 Monate aktualisieren.
<b>Verarbeitungsverzeichnis</b>	Nachrichtendaten verarbeitet.	Nur > 250 Mitarbeiter.

Pflicht	Details	Ausnahmen/Reformen
<b>TOMs</b> ( <b>Technis-</b> <b>che/Organisatorische</b> <b>Maßnahmen</b> )	Gegenmaßnahmen basierend auf Schuldyse.	- Keine Periodizität (aktuell vergilbte Dokumente). - Protection by Design.
<b>Datenschutzbeauftragter</b>	<b>Pragter</b> /Überwachung	Nur bei Größe; Seit 2024: 60-Stunden-Lehrgang, Prüfung $\geq 70$ , keine Wiederholungspflicht, kein DSG-Kennntniszwang.

- **Zertifizierung:** Verfahren erforderlich; Nachweis der Einhaltung.

## Praktische Beispiele & Konsequenzen

Beispiel	Beschreibung	Konsequenzen
<b>Notendatenbank-Hack</b>	Österreichisches Unternehmen outsourcet an östliches Rechenzentrum; Data Breach → Reifeprüfungsnoten online (3 Bundesländer).	DSGVO-Verstoß; Preisgründe ignoriert.
<b>Schulserver-Lücke</b>	Fehlende Verzeichnissicherheit → Schüler schließen auf andere Klassen (Noten + sensible Daten).	Herabwürdigung; Subsummierung von Paragraphen (Datenschutz + Beleidigung).
<b>Sicherheitsgutachten</b>	A4-Seite mit Fehlern (Gabelstaplerfahrer mit Migrationshintergrund).	Gerichte fordern bei Großunternehmen/öffentlichem Interesse Sachverständigen/Ziviltechniker (nicht "Hans die Wurst").

- **Sachverständiger vs. Ziviltechniker:**
  - **Sachverständiger:** Strafprozess; Gericht bestellt (Register, Ausbildung: Studium, Prüfungen).
  - **Ziviltechniker:** Zivilprozess; Gleiche Person/Ausbildung möglich, aber Fokus auf Zivilrecht.
  - Privat einholbar für Gutachten.

## Fazit

- **DSGVO = Nicht nur Schutz:** Harmonisierung, aber Ausnahmen für Parteien/Polizei; Hauptziel: Automatisierter Datenaustausch.
- **Durchsetzung schwach:** Lange Fristen, geringe Strafen.
- **Profiling/IT-Relevanz:** Strenge Verbote, aber gerichtliche Ausnahmen; Konflikte bei Audits.
- **Polizei-Transparenz:** Österreichisch fadenscheinig; internationale Modelle transparenter.
- **Umsetzung:** Risikoanalysen/TOMs essenziell; Reformen für Aktualität notwendig.