

**DSGVO**  
**Datenschutz-Grundverordnung**  
Gültig ab 25.Mai 2018

Mehr Eigenverantwortung für den Verantwortlichen im Sinne der EU-DSGVO, die DSGVO regelt den Umgang mit personenbezogenen Daten neu und einheitlich für die EU

Gibt es eine Übergangsfrist?

Die DSGVO normiert, dass bestehende Datenverarbeitungen innerhalb von zwei Jahren ab Inkrafttreten der DSGVO (das war der 25. Mai 2016) mit ihr in Einklang zu bringen sind. D.H., dass bestehende Datenverarbeitungen ab dem 25. Mai 2018 „DSGVO-konform“ sein müssen

Wer ist von der DSGVO betroffen:

Die DSGVO gilt für Großunternehmen/Konzerne, wie für Einpersonbetriebe, Behörden und öffentlichen Stellen.

**Grundsätzlich ist jede Verarbeitung von „personenbezogenen Daten“ verboten**

Die Rechtmäßigkeit der Verarbeitung wird im Art. 6 DSGVO geregelt:

- a. Einwilligung der betroffenen Person
- b. die Verarbeitung ist für eine Vertragserfüllung notwendig
- c. es gibt eine rechtliche Grundlage
- d. lebenswichtige Interessen
- e. wichtig für das öffentliche Interesse
- f. die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten notwendig, sofern die Grundrechte bzw. Grundfreiheit nicht überwiegen (der Punkt f gilt nicht für Behörden)

Neue Bezeichnungen in der DSGVO

**Verantwortlicher (Art4 Z7) (Auftraggeber DSG2000)**

Ist die Person, Behörde, Einrichtung oder andere Stelle die über die Zwecke und Mittel der Verarbeitung entscheidet.

Z.B. die Schule die eine Anwendung mit persönlichen Daten erstellt und entscheiden muss auf Grund welcher gesetzlichen Grundlage oder anderen Basis diese Anwendung laufen darf.

**Auftragsverarbeiter (Art4 Z8) (Dienstleister DSG2000)**

„Auftragsverarbeiter“ ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen bearbeitet.

z.B. die IT-Abteilung des Landes die für die Schulen die Server bzw. Datenbank für die e\*SA-Daten zur Verfügung stellt.

## **Betroffener**

Der Betroffene ist der dessen personenbezogene Daten verarbeitet werden.

Rechte des Betroffenen:

- Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person
- Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden
- Auskunftsrecht
- Recht auf Berichtigung
- Recht auf Löschung ("Recht auf Vergessenwerden")
- Recht auf Einschränkung der Verarbeitung
- Recht auf Datenübertragbarkeit
- Widerspruchsrecht

## Einige Neuerungen der DSGVO

personenbezogene Daten:

identifizierte oder identifizierbare natürliche Personen. Standortdaten, Online-Kennung oder anderen „besonderen Merkmalen“

Datensicherheit:

Stand der Technik, Implementierungskosten, Art, Umfang, Umstände und Zweck der Verarbeitung, Eintrittswahrscheinlichkeit und Schwere des Risikos geeignete technische und organisatorische Maßnahmen Pseudonymisierung Verarbeitung ohne Zuordnung zu einer spezifischen Person (gesonderte Aufbewahrung des Personenbezugs) Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme. (Firewalls, Zugangsbeschränkungen, Redundanzen) Wiederherstellbarkeit (Backup) Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen.

Zweckgebundenheit:

Die Rechtmäßigkeit der Verarbeitung (Art. 6 DSGVO)

Dokumentationspflicht: Jede Anwendung in der personenbezogene Daten verarbeitet werden ist zu dokumentieren (welche Daten verarbeitet werden, wer Zugriff hat, ob Daten weiter gegeben werden und an wen, usw.

Datenminimierungspflicht:

Personenbezogene Daten dürfen nur so lange gespeichert werden, wie es für die Zwecke, für die sie verarbeitet werden erforderlich ist.

Meldepflicht gegenüber dem Betroffenen:

Nicht bei verschlüsselten Daten, nicht bei überdurchschnittlich hohem Aufwand (stattdessen öffentliche Bekanntmachung)).

Meldepflicht gegenüber der Datenschutzbehörde:

Binnen 72 Stunden, außer die Verletzung führt zu keinem Risiko für die Rechte und Freiheiten der Betroffenen. die Meldung muss beinhalten: Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen

Einwilligung:

Nachweis einer Einwilligung

## Was wird durch die DSGVO geschützt:

Die Datenschutz-Grundverordnung schreibt den Schutz von Personen deren Daten verarbeitet werden vor. Nicht die Daten per se!

Die Verarbeitung personenbezogener Daten aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zu eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer Person ist untersagt.

Insofern sind nur drei weitere Datenkategorien hinzugekommen: die genetischen und biometrischen Daten sowie die sexuelle Orientierung

### Genetische Daten (Art 4 Z 13)

„Genetische Daten“ sind personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betroffenen natürlichen Person gewonnen wurden.

### Biometrische Daten (Art 4 Z 14)

„Biometrische Daten“ sind mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen und verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder und daktyloskopische Daten.

### Schutzklassen:

#### Gering:

- Daten, die aus öffentlichen Quellen entnommen werden können und kein schutzwürdiges Interesse des Betroffenen überwiegt.
- Adressdaten aus öffentlichen Telefonverzeichnissen
- Unbedenkliche Mitgliederverzeichnisse, etc.

#### Mittel:

- Vertragsdaten
- Auftragsdaten
- Bonitätsprüfungen
- Personaleinsatzplanung
- Kontaktdaten von Mitarbeitern (z.B. priv. Rufnummer)
- Daten zum Beschäftigungsverhältnis
- Interne Rufnummernübersicht, etc.

#### Hoch:

- Rassistische und ethnische Herkunft
- Politische Meinungen
- Religiöse und philosophische Überzeugungen
- Gewerkschaftszugehörigkeit

- Gesundheit und Sexualleben
- Angaben zu Ordnungswidrigkeiten oder Strafdaten
- Daten, die einem Berufsgeheimnis unterliegen (Ärzte, Rechtsanwälte, Sozialarbeit, etc.)
- Angaben zu Bank- oder Kreditkartenkonten
- Daten, die dazu geeignet sind, die Persönlichkeitsmerkmale eines Betroffenen zu bewerten
- Daten zu Leistungs- und Verhaltenskontrollen

Kind (Art 8 Abs 1)

Für die Rechtmäßigkeit der Einwilligung eines Kindes bei einem Angebot von Diensten der Informationsgesellschaft legt die DSGVO eine Altersgrenze von 16 Jahren fest.

Die EU-Mitgliedstaaten können aber niedrigere Altersgrenzen vorsehen, allerdings nicht unter das vollendete 13. Lebensjahr. **Das österreichische Datenschutzgesetz (DSG) i.d.F. des Datenschutz-Anpassungsgesetzes 2018 setzt diese Altersgrenze mit dem vollendeten 14. Lebensjahr fest.**