DSGVO-SCHULUNG

Was bedeutet die DSGVO für Unternehmen und Beschäftigte?

Inproma GmbH | Am Hofe 10 | 42349 Wuppertal | 2024

Inhalts-verzeichnis

Überblick zur Datenschutz-Grundverordnung (DSGVO)

- in den Jahren vor Einführung der DSGVO wurde die Forderung nach einer Neuordnung des europäischen Datenschutzrechts immer lauter
  - rasante technologische Entwicklungen
  - zuvor gültige Datenschutzrichtlinie legte nur einen Mindeststandard fest
  - → uneinheitliches Datenschutzniveau in Europa mit verschiedenster mitgliedstaatlicher Regelungen
  - → Rechtsunsicherheit, welche als Hemmnis für freien Waren- und Dienstleistungsverkehr gesehen wurde
- im Mai 2018 trat die Datenschutz-Grundverordnung (DSGVO) in Kraft
- als Verordnung ist sie in allen Teilen verbindlich und gilt unmittelbar für jeden Mitgliedstaat der EU und des EWR → einheitliches Datenschutzniveau

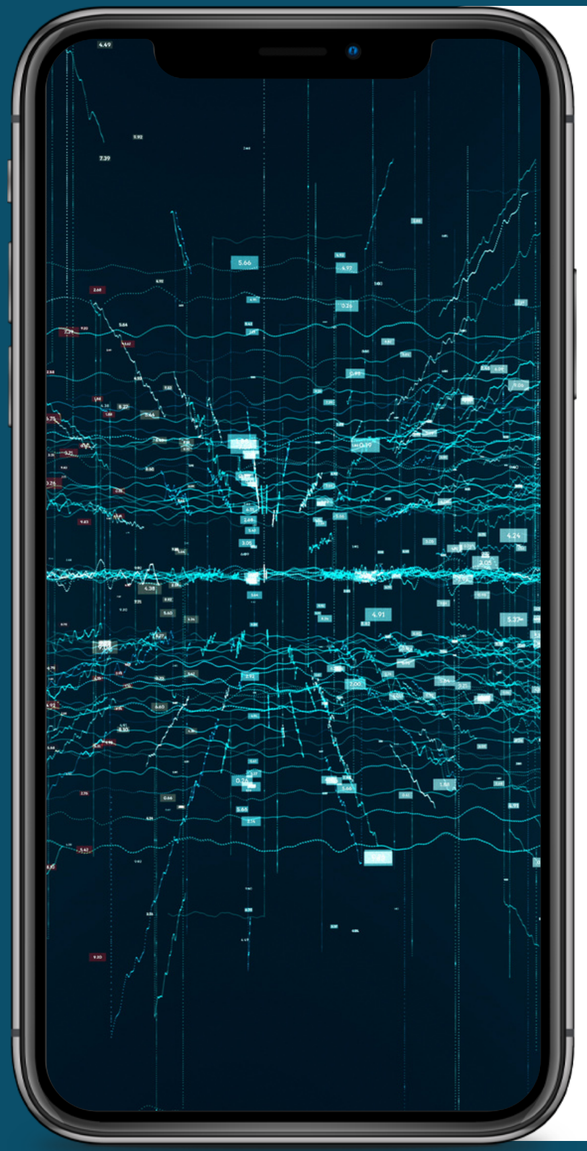
Zweck und Ziele der DSGVO

01 **Schutz der Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere ihrer personenbezogenen Daten**

→ „Recht auf informationelle Selbstbestimmung“

02 **Schutz und Gewährleistung des freien Verkehrs personenbezogener Daten innerhalb der EU**

Wann findet die DSGVO Anwendung?



Die DSGVO unterscheidet zwischen folgenden zwei Anwendungsbereichen:

01 Sachlicher Anwendungsbereich
02 Räumlicher Anwendungsbereich

Sofern beide Anwendungsbereiche geöffnet sind, müssen die Regelungen der DSGVO angewendet werden!

01

Sachlicher Anwendungsbereich

Die DSGVO gilt für…

…die ganz oder teilweise automatisierte Verarbeitung sowie die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder werden sollen

Verarbeitung

- dazu gehört Erhebung, Erfassung, Speicherung, Ordnung, Veränderung, etc.
- Dauer und Intensität spielt keine Rolle

Dateisystem

- jede strukturierte Sammlung personenbezogener Daten
- unabhängig davon, ob Sammlung zentral, dezentral oder nach funktionalen oder geographischen Aspekten geordnet geführt wird

01

Sachlicher Anwendungsbereich

Personenbezogene Daten

- Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen
- **Es wird nicht zwischen personenbezogenen Daten im privaten, öffentlichen oder arbeitsbezogenen Umfeld einer Person unterschieden – es geht immer um die Person selbst.**

Beispiele

- Name
- Geburtsdatum
- Vermögen
- Personalnummer
- Benutzerkennung
- Anschrift
- Gewohnheiten
- Arbeitsleistung
- Fotos
- Krankenakte
- Verhalten in der Organisation
- Onlinedaten (IP-Adresse, Standort)
- Telefonnummer
- Systembezogenes Systemverhalten
- Kundendaten
- physische Merkmale
- Werturteile (Zeugnisse)

02

Räumlicher Anwendungsbereich

Die DSGVO gilt für…

01 **…alle Unternehmen und Organisationen mit Niederlassung in der EU**
→ unabhängig davon, ob die Daten in der EU verarbeitet werden oder nicht

02 **…Organisationen, die nicht in der EU niedergelassen sind, aber die**

- den betroffenen Personen in der EU Waren oder Dienstleistungen anbieten,
- das Verhalten der betroffenen Personen beobachten (z.B. Tracking über Smartwatch/Handy).

Rechtmäßig-keit der Verarbeitung

- Die Erhebung oder Verarbeitung personenbezogener Daten ist grundsätzlich verboten
  → Verbot mit Erlaubnisvorbehalt

- Art. 6 Abs. 1 DSGVO regelt jedoch einige Bedingungen, unter denen eine Verarbeitung rechtmäßig bzw. erforderlich ist

- Unterscheidung zwischen
  a) personenbezogenen Daten und
  b) besondere Kategorien personenbezogener Daten

Allgemeine Kategorien personenbezogener Daten

Unter folgenden Voraussetzungen ist eine Verarbeitung rechtmäßig bzw. erforderlich

- **Einwilligung** der betroffenen Person
- **Vertrag bzw. vorvertragliche Maßnahme** zw. betroffener Person und Datenverarbeiter
- **Interessenabwägungsklausel**
- Verantwortlicher unterliegt einer **rechtlichen Verpflichtung**
- **lebenswichtige Interessen** der betroffenen oder einer anderen natürlichen Person sind zu schützen
- Verarbeitung ist für die Aufgabe **öffentlicher Interessen** oder zur **Ausübung öffentlicher Gewalt** erforderlich

b

Besondere Kategorien personenbezogener Daten

Für die Zulässigkeit der Verarbeitung werden sowohl juristisch als auch technisch/organisatorisch zusätzliche Verpflichtungen an den Verantwortlichen gestellt:

- Erstellung eines Verarbeitungsverzeichnis
- Erforderlichkeit einer Datenschutzfolgenabschätzung
- Benennung eines Datenschutzbeauftragten

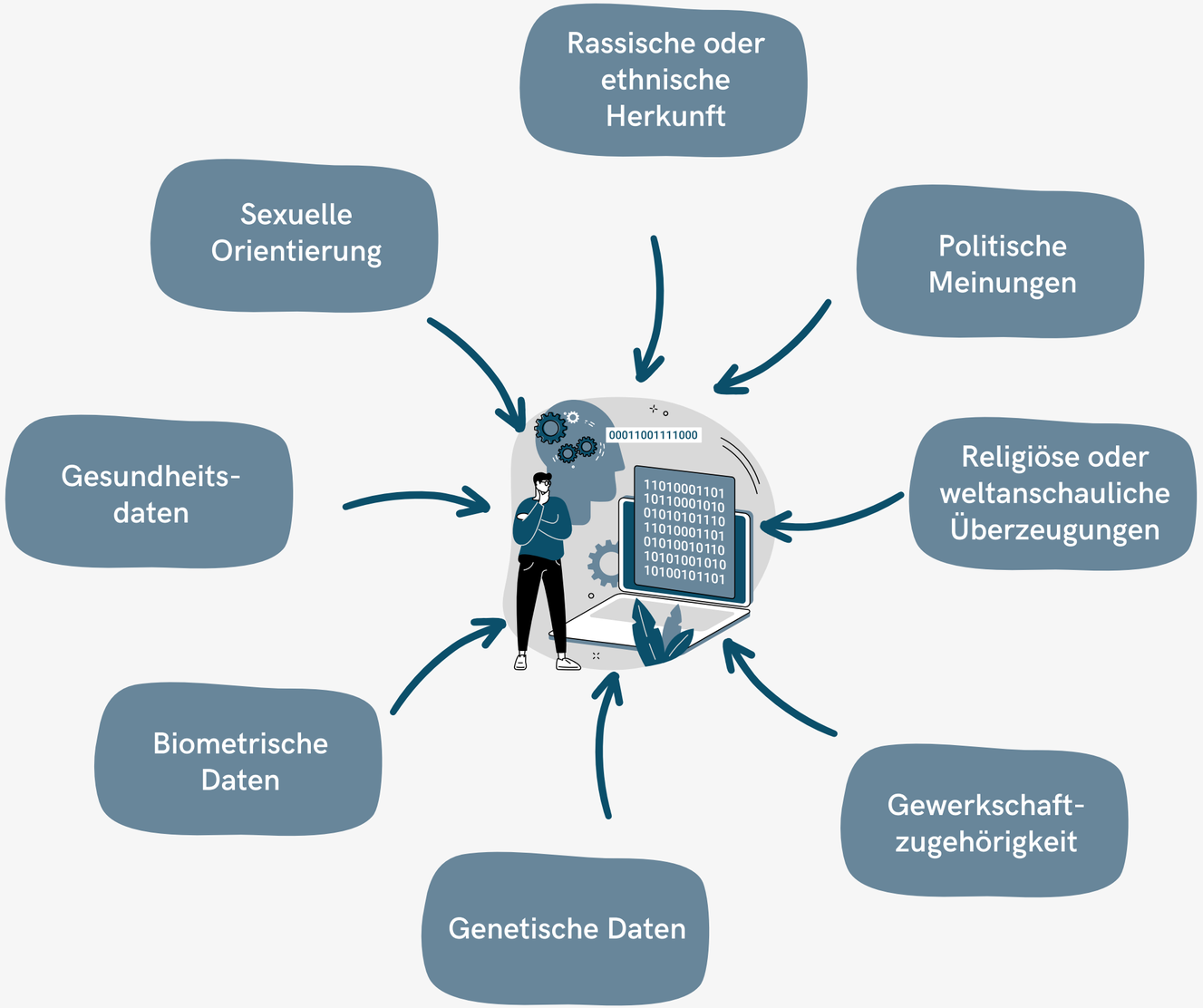
Wieso bedarf es weiteren Vorkehrungen zur rechtmäßigen Verarbeitung besonderer Kategorien personenbezogener Daten?

→ Datenkategorien, die besonders sensibel und schützenswert sind

→ Verarbeitung kann erhebliche Risiken für betroffene Person darstellen

b

Besondere Kategorien personenbezogener Daten



Verantwortlichkeit

Verantwortlicher

- diejenige juristische oder natürliche Person eines Unternehmens, die allein oder gemeinsam mit anderen über Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet
- Verantwortlicher haftet bei Datenschutzverstößen
  - das Unternehmen bzw. die Geschäftsführung
  - Geschäftsführer kann persönlich haften!

Mitarbeiter

- sind verpflichtet, mit personenbezogenen Daten sorgfältig umzugehen und die Regelungen und Bestimmungen des Datenschutzes bei ihrer täglichen Arbeit umzusetzen → Wahrung des Datengeheimnisses (§ 53 BDSG)
  - Mitarbeiter haften nur bei grober Fahrlässigkeit

Grundsätze der DSGVO

1. Rechtmäßigkeit der Verarbeitung
2. Verarbeitung nach Treu und Glauben
3. Transparenz
4. Zweckbindung
5. Datenminimierung
6. Richtigkeit der Datenverarbeitung
7. Speicherbegrenzung
8. Integrität und Vertraulichkeit

Die Einhaltung der Grundsätze muss nachgewiesen werden können!

Recht der betroffenen Person

1. Recht auf Auskunft
2. Recht auf Berichtigung
3. Recht auf Löschung bzw. „Recht auf Vergessenwerden“
4. Recht auf Einschränkung der Verarbeitung
5. Recht auf Datenübertragbarkeit
6. Recht auf Widerspruch

Datenschutz-beauftragter

1. fungiert als Schnittstelle zw. Unternehmen, Aufsichtsbehörde und betroffenen Personen
2. muss vom Verantwortlichen bzw. vom Auftragsverarbeiter an die Datenschutz-Aufsichtsbehörde gemeldet werden
3. tritt im Zusammenhang mit der Verarbeitung personenbezogener Daten als Berater des Verantwortlichen auf
4. dient als Kontrollorgan innerhalb der Organisation
5. ist nicht Verantwortlicher und damit nicht die haftende Person!

Elementare Datenschutz-Anforderungen an Unternehmen

1. Verzeichnis von Verarbeitungstätigkeiten
2. Technische und organisatorische Maßnahmen
3. Datenschutz-Folgenabschätzung
4. Auftragsverarbeitungsvertrag
5. Datenübermittlung in Drittländer
6. Risikoanalyse
7. Datenschutzkonzept
8. Informationspflicht
9. Schulung von Mitarbeitern
10. Meldepflicht bei Datenpannen

Elementare Datenschutz-Anforderungen an Unternehmen

1. Rechtmäßigkeit der Verarbeitung
2. Verarbeitung nach Treu und Glauben
3. Transparenz
4. Zweckbindung
5. Datenminimierung
6. Richtigkeit der Datenverarbeitung
7. Speicherbegrenzung
8. Integrität und Vertraulichkeit

Die Einhaltung der Grundsätze muss nachgewiesen werden können!

1

Verzeichnis von Verarbeitungs-tätigkeiten (VvV)

- hier werden alle Tätigkeiten beschrieben, bei denen personenbezogene Daten erfasst und verarbeitet werden
- dient als wesentliche Grundlage für eine strukturierte Datenschutzdokumentation und als Nachweis für eine rechtmäßige Datenverarbeitung
  - Erfüllung der Rechenschaftspflicht
  - Erfüllung der Dokumentationspflicht
- in der Praxis ist ein VvV in den allermeisten Fällen verpflichtend zu führen

2

Technische und organisatorische Maßnahmen (TOMs)

- Technische Maßnahmen beziehen sich auf Hard-, Software und Netzwerkkomponenten, die zur Datenverarbeitung genutzt werden
  - Datenschutz durch Technikgestaltung („Privacy by Design“)
  - Datenschutz durch Voreinstellungen („Privacy by Default“)

- Organisatorische Maßnahmen richten sich an Ablaufprozesse und die an der Verarbeitung beteiligten Personen, z.B.
  - Aufstellen von Berechtigungskonzepten
  - Schulungen

3

Datenschutz-Folgenabschätzung (DSFA)

- ist durchzuführen, sofern Verarbeitungsvorgänge ein voraussichtlich hohes Risiko für die Rechte und Freiheiten der betroffenen Person haben
- wann ein hohes Risiko vorliegt, muss im Einzelfall überprüft werden, z.B.
  - Videoüberwachung öffentlich zugänglicher Bereiche
  - Verarbeitung besonderer Kategorien personenbezogener Daten

Sinn einer DSFA

- hohes Risiko für betroffene Personen senken durch geeignete Maßnahmen
- Dokumentation und Nachweis der Minimierung des Risikos

4

Auftrags-verarbeitungsvertrag (AV-Vertrag)

- eine Auftragsverarbeitung ist das Verarbeiten personenbezogener Daten durch einen Dienstleister (Auftragsverarbeiter)
- AV-Vertrag soll für Auftraggeber und Auftragnehmer Klarheit über Befugnisse, Weisungen, Zwecke der Verarbeitung, Rechte und Pflichten festhalten
  - dient als Nachweis für Verantwortlichen, sofern es zu Datenschutzverstößen kommt
  - wichtig, da Auftraggeber der Verantwortliche bleibt und somit haftbar ist!

5

Datenübermittlung in Drittländer

- alle Länder, die nicht Mitgliedstaat in EU und EWR sind, gelten als Drittland
- grenzüberschreitende Datentransfers erfordern Schutzmaßnahmen, um in dem entsprechenden Drittland ein mit der DSGVO vergleichbares Datenschutzniveau zu gewährleisten
- eine der folgenden Anforderungen zur Datenübermittlung muss gegeben sein:
  - Angemessenheitsbeschluss der EU (Bescheinigung eines vergleichbaren Datenschutzniveaus im Drittland)
  - geeignete Garantien (z.B. Standardvertragsklauseln)
  - mögliche Ausnahmen (z.B. Einwilligung, Vertrag)

Datenschutzmanagementsystem (DSMS)

- Aufbau eines DSMS hat eine zentrale Bedeutung
- soll die Einhaltung des Datenschutz und der DSGVO über das gesamte Unternehmen hinweg sichern, dokumentieren und fortlaufend verbessern
- insbesondere die Pflicht der DSGVO zur Erfüllung der Dokumentations, Nachweis- und Rechenschaftspflichten machen den Einsatz eines DSMS unverzichtbar
- durch die Pflicht zur Umsetzung technischer Maßnahmen ist der PRO-DSGVO guide als Datenschutzmanagement-Software ebenfalls unvermeidbar

Konsequenzen aus Verstößen

Verstöße gegen die DSGVO werden in zwei Kategorien aufgeteilt

01 **Formeller Verstoß**
→ bis zu 10 Millionen Euro oder bis zu 2 % des gesamten weltweit erzielten Vorjahresumsatzes

02 **Materieller Verstoß**
→ bis zu 20 Millionen Euro oder bis zu 4 % des gesamten weltweit erzielten Vorjahresumsatzes

Vielen Dank für Ihre Aufmerksamkeit

Die Inhalte der Präsentation erhalten Sie noch als Handout. In diesem Handout finden Sie noch weitere und ausführliche Informationen zu einzelnen Punkten.

Bitte unterschreiben Sie unbedingt noch die Bestätigung über Ihre Teilnahme an dieser Datenschutz-Schulung.