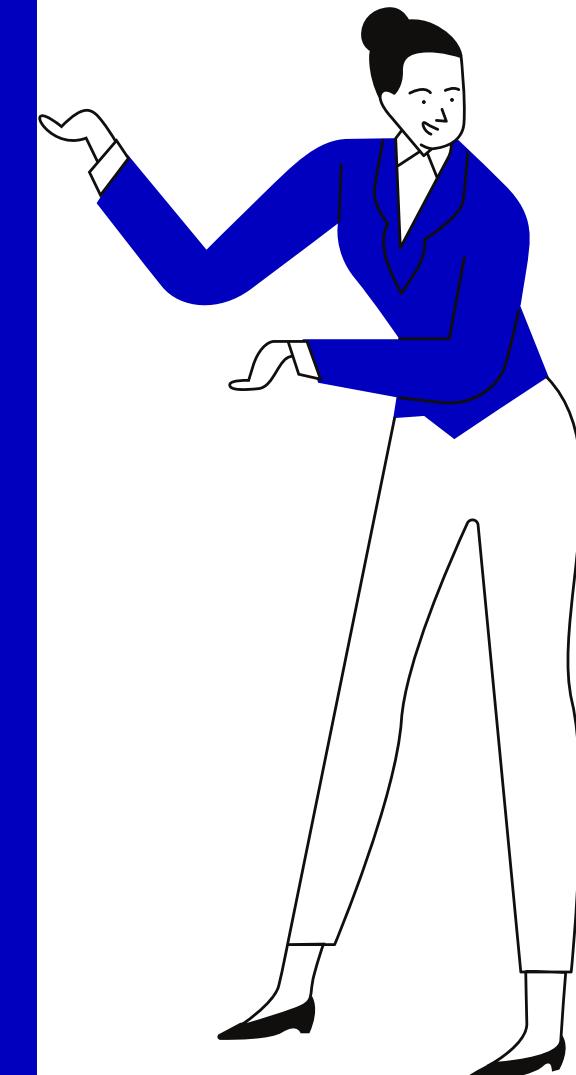
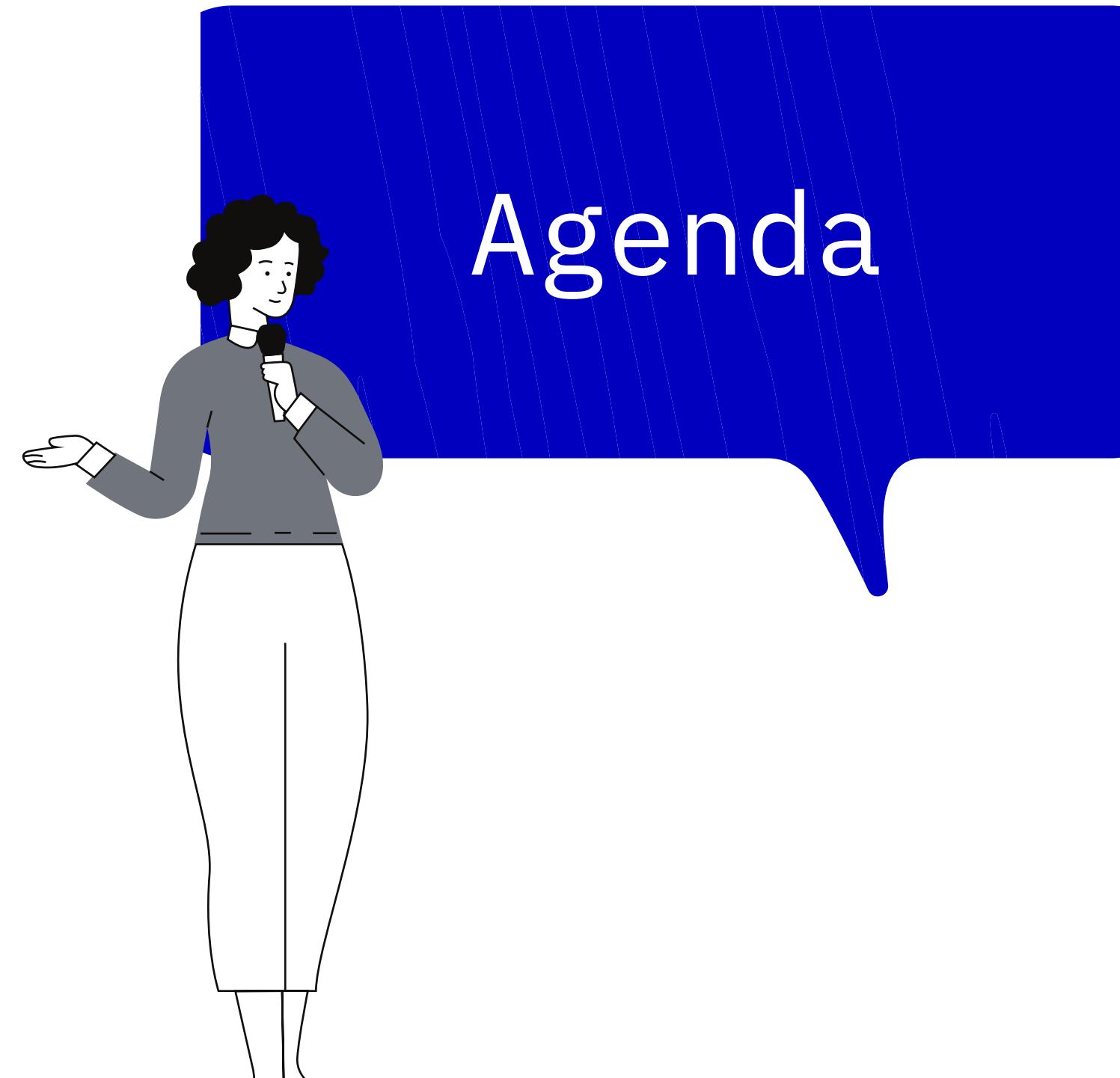


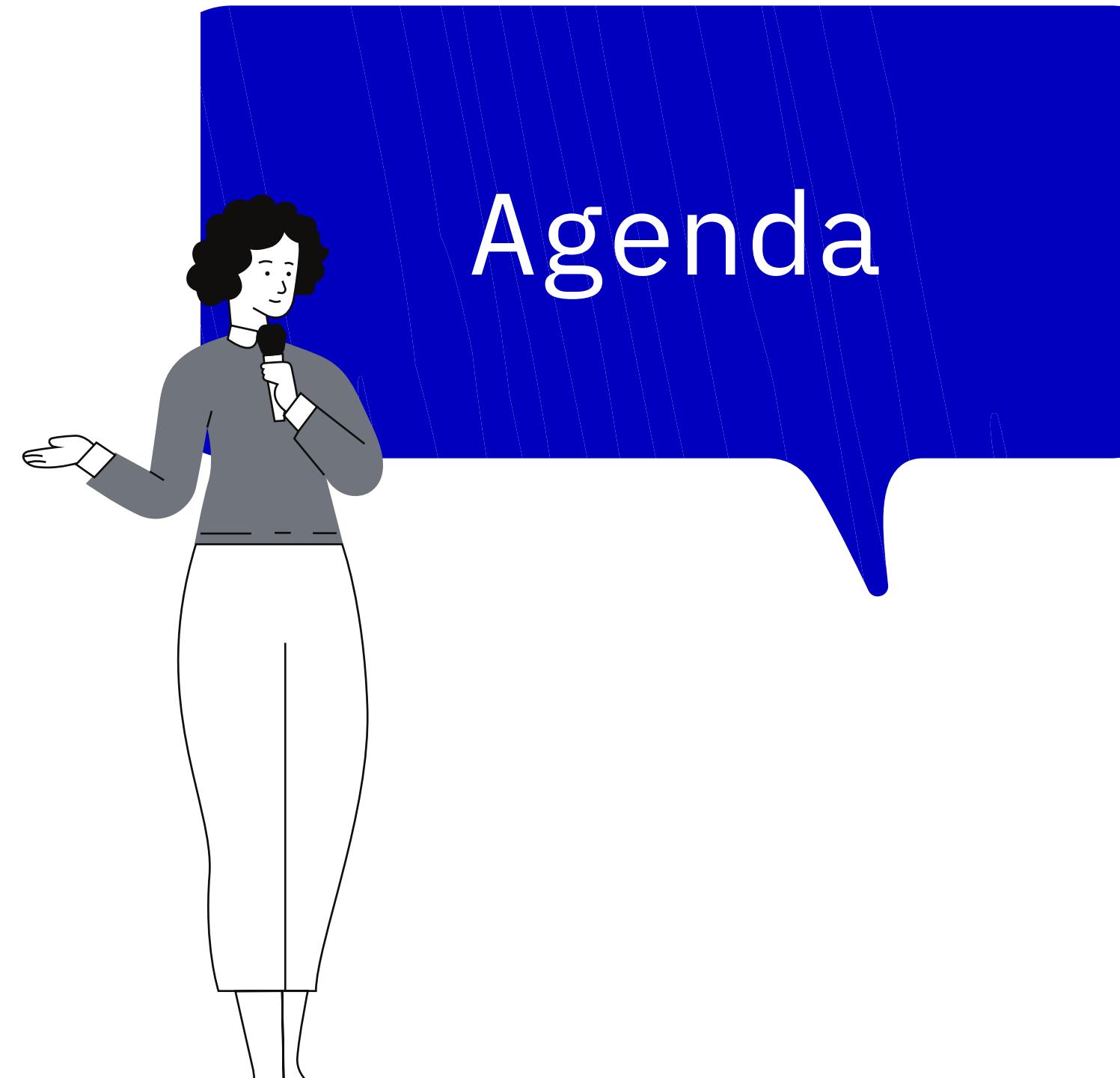
Datenschutz und rechtliche Grundlagen

Allgemeine gesetzliche Grundlagen -
Teil I



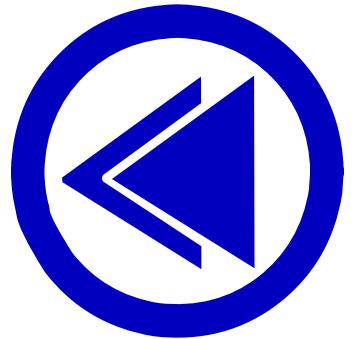


- 1** Wiederholung vom Vortag
- 2** Was ist Datenschutz?
- 3** Datenschutzunterschiede
- 4** Medizinische Daten und Datenschutz
- 5** Begriffsbestimmungen



- 1** Wiederholung vom Vortag
- 2** Was ist Datenschutz?
- 3** Datenschutzunterschiede
- 4** Medizinische Daten und Datenschutz
- 5** Begriffsbestimmungen

Ihr seid dran: Wiederholung vom Vortag



Gehe auf www.menti.com

Oder folge dem Link:

<https://www.menti.com/9db85d43re>





- 1 Wiederholung vom Vortag
- 2 Was ist Datenschutz?
- 3 Datenschutzunterschiede
- 4 Medizinische Daten und Datenschutz
- 5 Begriffsbestimmungen

Was ist Datenschutz?



Datenschutz bezeichnet den Schutz des Einzelnen vor dem Missbrauch personenbezogener Daten

- Im Fokus: Daten, die in einem unmittelbaren bzw. mittelbaren Zusammenhang zu einer bestimmten Person stehen
 - Z.B. Name, Adresse, Geburtsdatum, Telefonnummer etc.
- Schutz des **Persönlichkeitsrechts** bei der Datenverarbeitung
- Schutz der eigenen **Privatsphäre** eines Menschen



Der Datenschutz in Deutschland ist hauptsächlich durch zwei Gesetze geprägt

Datenschutz-Grundverordnung



Neues Bundesdatenschutzgesetz

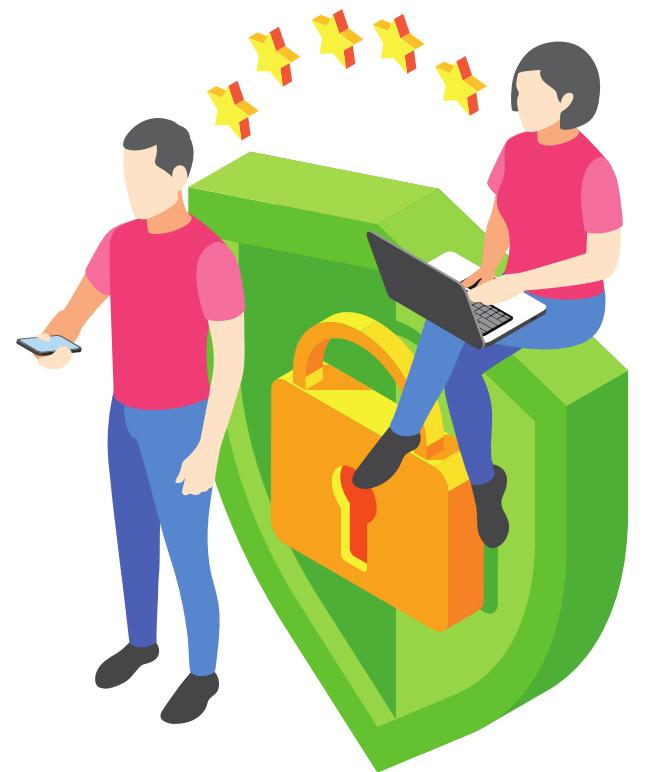


- Vorgaben für eine rechtmäßige Datenverarbeitung
- Bestimmung von Sanktionsmöglichkeiten für Verstöße gegen gesetzliche Vorgaben



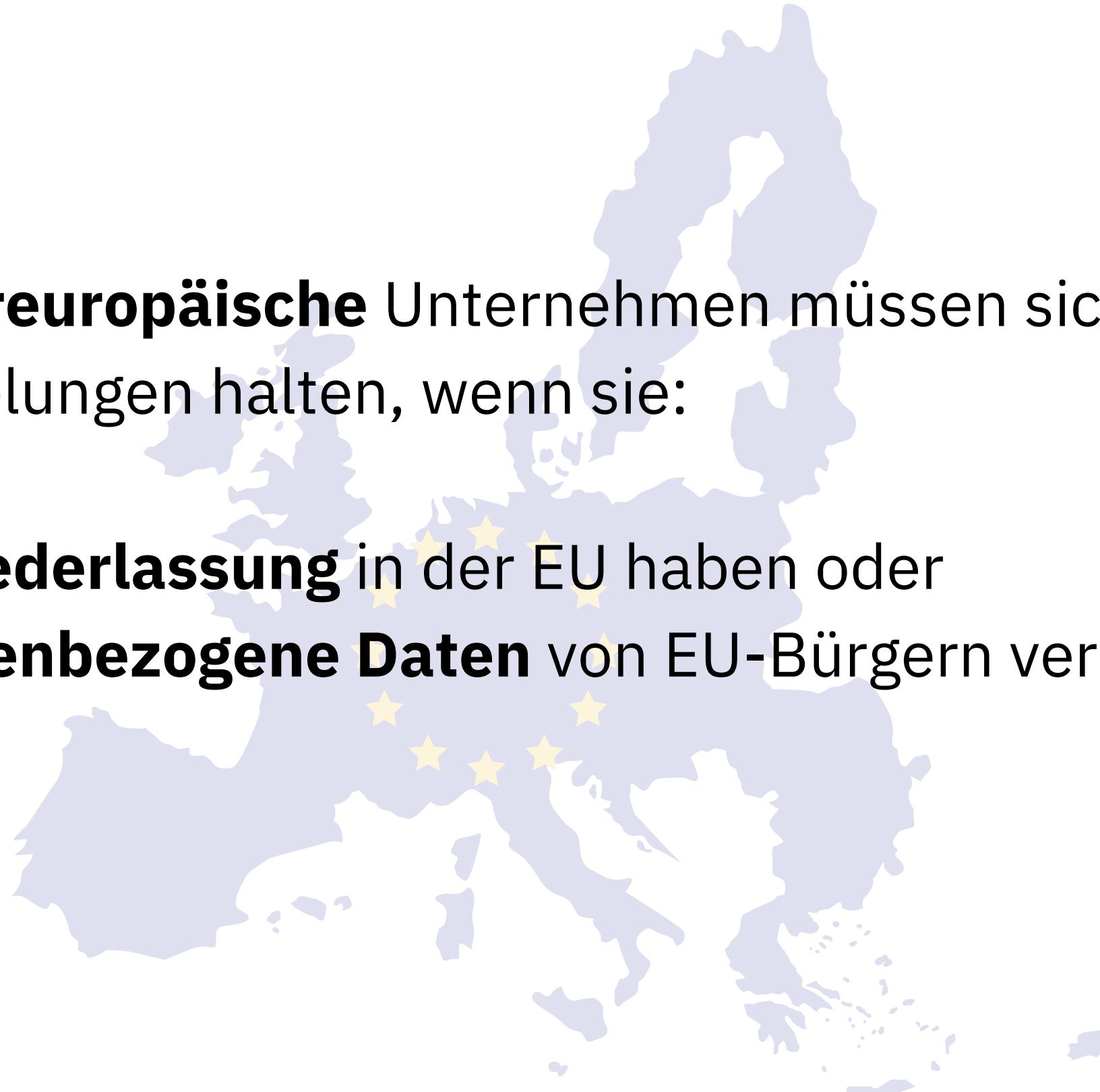
Vor der DSGVO galt in Deutschland das alte Bundesdatenschutzgesetz

- Inkrafttreten der DSGVO:
 - 25. Mai 2018
 - Zeitgleich trat die neue Verfassung des BDSG in Kraft (BDSG-neu)
- Dient der **Vereinheitlichung** des Datenschutzrechts innerhalb der EU
 - Bisher galten überall **verschiedene Datenschutzgesetze** und Standards
- Das Datenschutzrecht soll datenschutzfreundlicher für die betroffenen Nutzer werden
 - Der Bürger erhält **Hoheit** über seine Daten zurück



Die Datenschutzverordnung gilt für alle Unternehmen,
die in der EU ansässig sind

- Auch **aussereuropäische** Unternehmen müssen sich an die neuen Regelungen halten, wenn sie:
 - Eine **Niederlassung** in der EU haben oder
 - **Personenbezogene Daten** von EU-Bürgern verarbeiten



Wichtigster Anknüpfungspunkt sind personenbezogene Daten

Personenbezogene Daten sind:

- Alle Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen

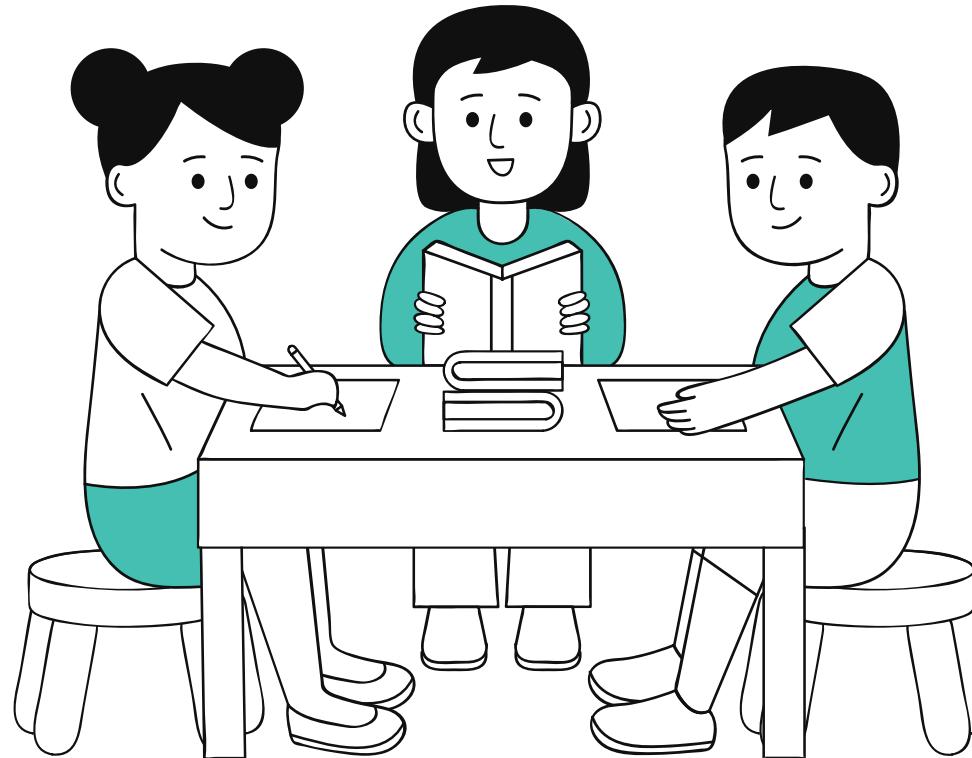


Wann ist eine Person identifizierbar?

- Wenn sie direkt oder indirekt identifiziert werden kann
 - Z.B. mittels Zuordnung einer Kennung wie Namen, Kennnummer, Standortdaten
 - Die Möglichkeit der Identifizierung reicht hier aus!



Jetzt seid ihr dran:
Was sind personenbezogene Daten?



Breakout-Session: (10 min)

- Erarbeite in Deiner Gruppe Beispiele für personenbezogene Daten.
- Teilt eure Ergebnisse anschließend mit dem gesamten Kurs.



- 1 Wiederholung vom Vortag
- 2 Was ist Datenschutz?
- 3 Datenschutzunterschiede
- 4 Medizinische Daten und Datenschutz
- 5 Begriffsbestimmungen

Gruppenaufgabe zum Datenschutz

Findet Länder, die beim Thema Datenschutz negativ sowie positiv herausstechen.

Wo sind die Unterschiede?

Was unterscheidet die schlechter gestellten Länder von den besser gestellten?

Was für Beispiele könnt ihr nennen?

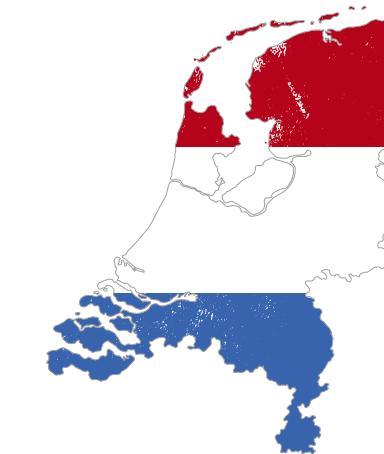
Größe: 4 Gruppen

Zeit: 30 Minuten



Deutschland ist in Sachen Datenschutz mit an der Spitze

- In Europa sind die Gesetze besonders streng
- Die schärfsten und umfassendsten Vorgaben gibt es in (2014):
 - Deutschland
 - Großbritannien
 - Niederlanden
 - Spanien



Andere Länder und Staaten sind nicht so gut aufgestellt

- Schwache Datenschutz-Gesetze in Asien, Afrika, Russland und Südamerika
- Asiatische Länder (besonders Hongkong):
 - Schwache Gesetzgebung
 - Keine gesetzliche Handhabe gegen Datenzugriff durch Regierungen oder Behörden
- Afrika, Russland und Südamerika:
 - So gut wie keine Gesetze zur Datensicherheit
 - Auch personenbezogene Daten sind hier ungeschützt



In den USA gibt es auch kein allgemeines und umfassendes Datenschutzgesetz

- Eigene Gesetze für unterschiedliche Branchen
- Der EU-US Privacy Shield
 - Informelle Absprache bzgl. Datenschutzrecht
 - Regelt den Schutz personenbezogener Daten, die aus einem Mitgliedsstaat der Europäischen Union in die USA übertragen werden
 - Aktuell: Die Vereinbarung für den Datenaustausch zwischen Europa und den USA ist vom höchsten EU-Gericht gekippt worden





- 1** Wiederholung vom Vortag
- 2** Was ist Datenschutz?
- 3** Datenschutzunterschiede
- 4** Medizinische Daten und Datenschutz
- 5** Begriffsbestimmungen

Krankenhäuser als kritische Infrastruktur

- Risiken durch zunehmende IT-Abhängigkeit
- Krankenhäuser mit mehr als 30.000 vollstationären Behandlungsfällen pro Jahr als kritische Anlagen im Bereich der stationären Versorgung.
- Krankenhäuser wichtiger Teil aufgrund der herausragenden Bedeutung für das Wohlergehen der Bevölkerung
 - Besondere Verpflichtung, die Verfügbarkeit der Dienstleistungen sicherzustellen
 - Klarheit über potenzielle Risiken
 - Entwicklung geeigneter Strategien



Informationen über den gesundheitlichen Zustand gehören zur besonderen Art personenbezogener Daten

- Unterliegen in besonderem Maße dem Datenschutz
- Besonders wichtig: korrekter und sicherer Umgang mit solch sensiblen Informationen
- Unterbindung von Missbrauch der sensiblen Informationen
 - Geeignetes Datenschutzkonzept ist für jedes Krankenhaus und Arztpraxis unerlässlich
 - Schulung des Personals



Art. 9 DSGVO - Verarbeitung besonderer Kategorien personenbezogener Daten

“

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 zur eindeutigen Identifizierung einer natürlichen Person, **Gesundheitsdaten** oder Daten zum **Sexualleben** oder der sexuellen Orientierung einer natürlichen Person ist untersagt.

”



Die Definition von Gesundheitsdaten ist in Art. 4 DSGVO zu finden

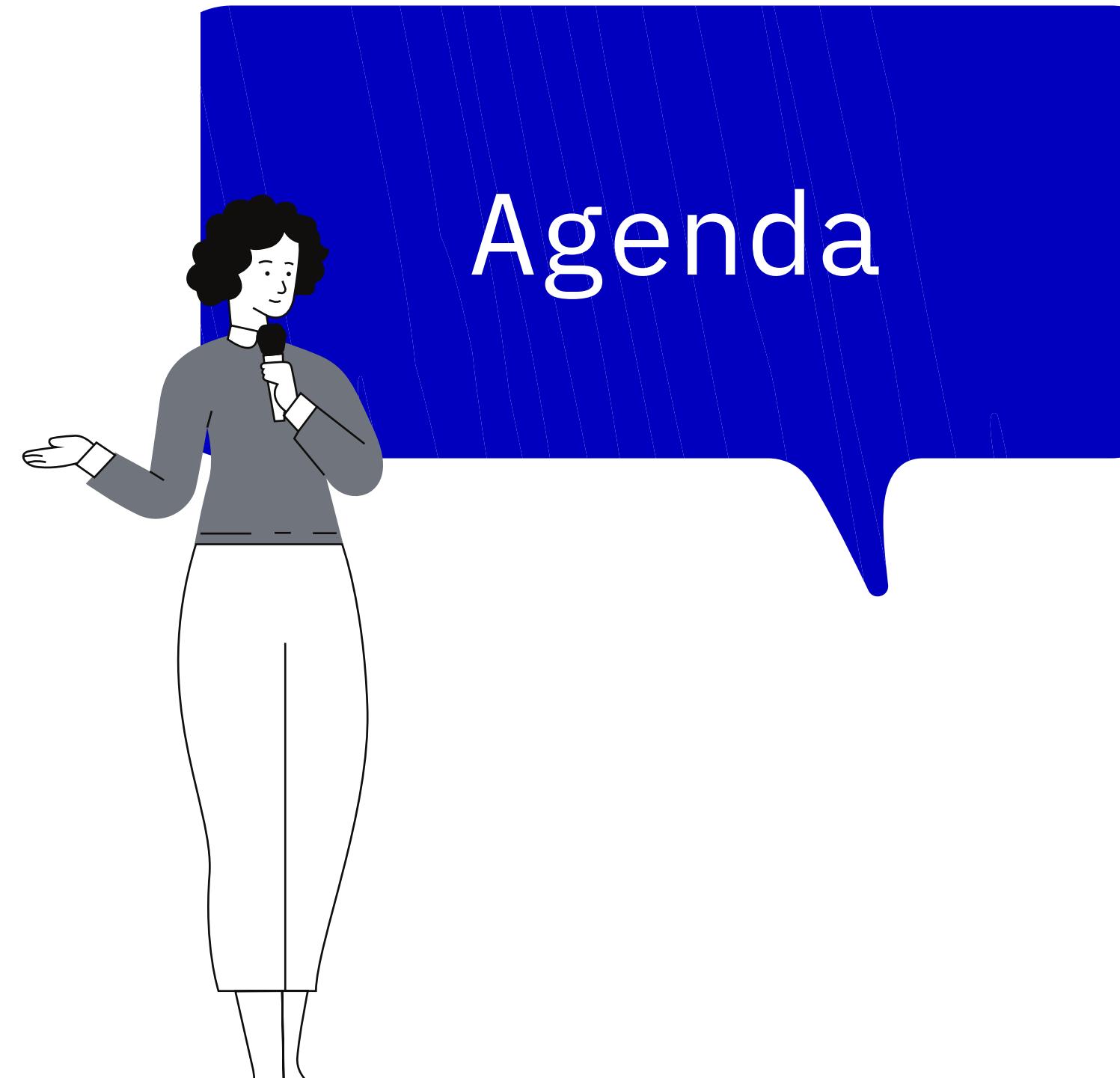
“ Gesundheitsdaten sind personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen beziehen und aus denen Informationen über deren **Gesundheitszustand** hervorgehen.”



Gesundheitsdaten sind extrem persönlich und erfordern höchste Schutzmaßnahmen

- Gesundheitsdaten sind extrem persönlich
- Nur den Betroffenen gehen seine Gesundheitsdaten etwas an
- Konsequenzen bei Missbrauch:
 - Negative Reaktion des sozialen Umfelds
 - In manchen Kulturen Ausgrenzung aus der Familie
 - Stigmatisierung bei bestimmten Krankheiten
 - Konsequenzen im Beruf





- 1** Wiederholung vom Vortag
- 2** Was ist Datenschutz?
- 3** Datenschutzunterschiede
- 4** Medizinische Daten und Datenschutz
- 5** Begriffsbestimmungen

Die Verarbeitung der Daten ist in der DSGVO geregelt

Datenverarbeitung bedeutet:

- Erheben, Erfassen, Organisation, Ordnen,
- Speicherung
- Anpassung oder Veränderung
- Auslesen, Abfragen, Verwendung
- Offenlegung durch Übermittlung oder Verbreitung
- Abgleich oder Verknüpfung, Einschränkung
- Löschen oder Vernichtung

von personenbezogenen Daten



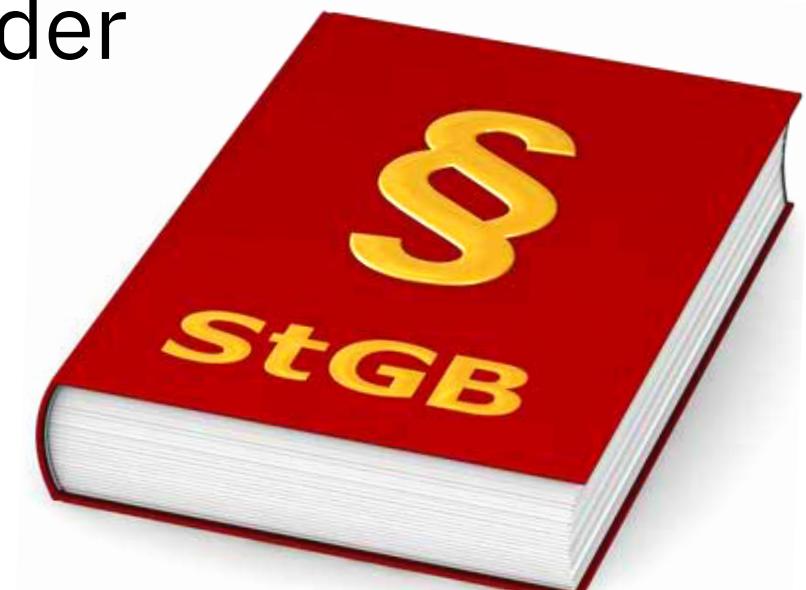
Die Speicherung von besonderen Arten personenbezogener Daten nur in Ausnahmefällen erlaubt

- Speicherung, Verarbeitung und Nutzung nur in **Ausnahmefällen**
- Kreis der Befugten ist kleiner als bei anderen Informationen
- Gesundheitsdaten dürfen nur dann erhoben werden, wenn der Betroffene **einstimmt** oder dies **gesetzlich gestattet** ist
 - z.B. wenn das überlebenswichtige Interesse des Betroffenen dadurch gewahrt würde



Die Weitergabe medizinischer Daten an Dritte ist in der Regel nicht zulässig

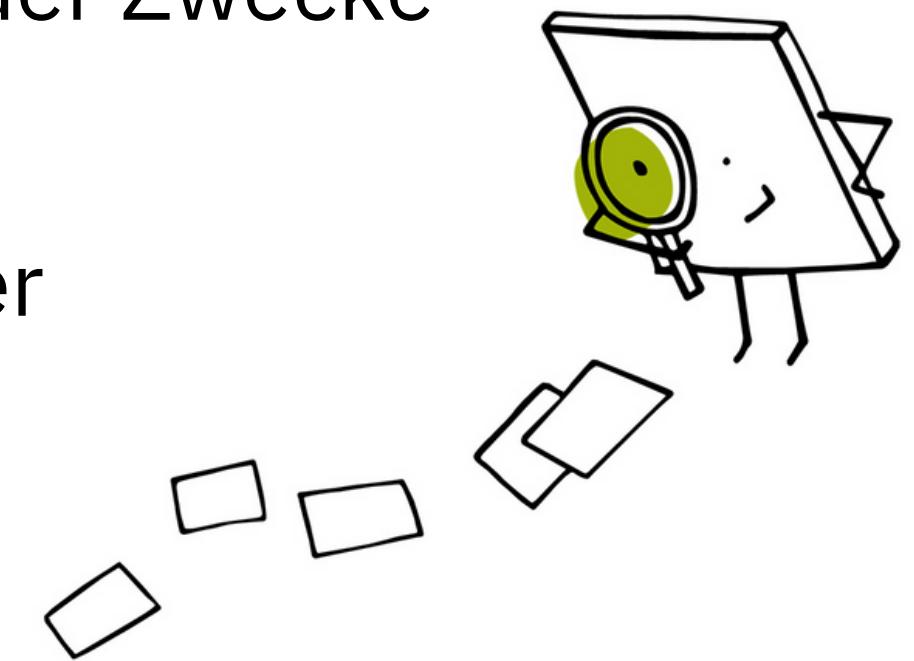
- Informationen der Ärzte und Krankenhauspersonal unterliegen dem **Berufsgeheimnis**
- Wahrung der **Verschwiegenheitspflicht**
- Verstoß ist **strafrechtlich** relevant
 - Gemäß § 203 Strafgesetzbuch kann eine unberechtigte Preisgabe von Daten, die einem besonderen Berufsgeheimnis unterliegen, mit einer Freiheitsstrafe bis zu einem Jahr oder einer Geldstrafe geahndet werden



Einrichtungen des Gesundheitswesens müssen eine Datenschutz-Folgenabschätzung durchführen

Zu einer Datenschutz-Folgenabschätzung gehören vier Aspekte, die entsprechend dokumentiert und verschriftlicht werden müssen:

- Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung der Gesundheitsdaten
- Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge
- Risikobewertung
- Maßnahmenplanung



Technisch organisatorische Maßnahmen sind bei personenbezogenen Daten wichtig

- TOM = Technische und organisatorische Maßnahmen
- § 9 Bundesdatenschutzgesetz (BDSG):
 - Alle Stellen, die personenbezogene Daten verarbeiten, erheben oder nutzen verpflichtet, TOM zu treffen
- Zur Gewährleistung, dass die Sicherheits- und Schutzanforderungen des BDSG erfüllt sind

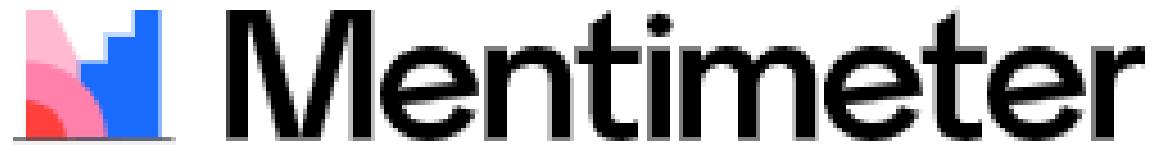


Anlage zu § 9 BDSG bestimmt die Anforderungen an die TOMs

- Pseudonymisierung und Verschlüsselung personenbezogener Daten
- dauerhafte Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung
- Verfügbarkeit der personenbezogenen Daten
- Wiederherstellung des Zugangs zu den personenbezogenen Daten bei einem physischen oder technischen Zwischenfall
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen



Jetzt seid ihr dran:
Um welche Maßnahme handelt es sich?



Gehe auf www.menti.com

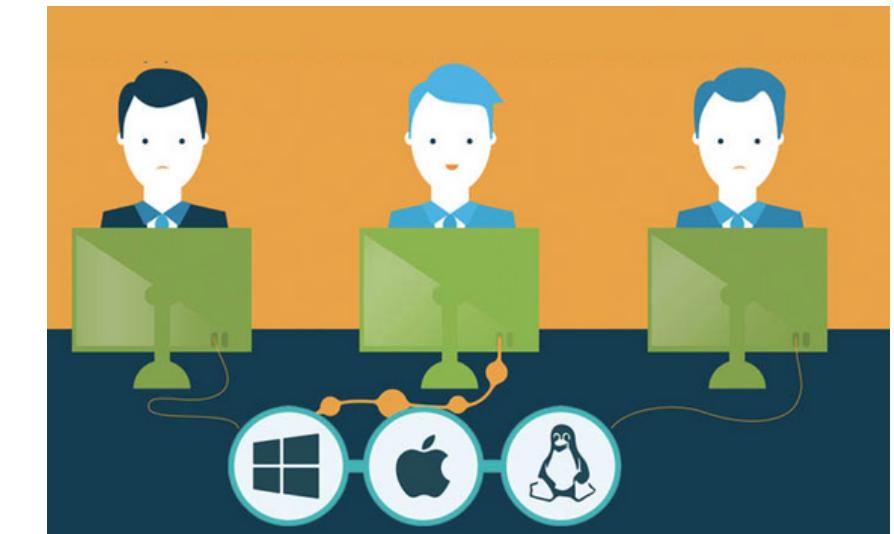
Oder folge dem Link:
<https://www.menti.com/7v51z1bv71>



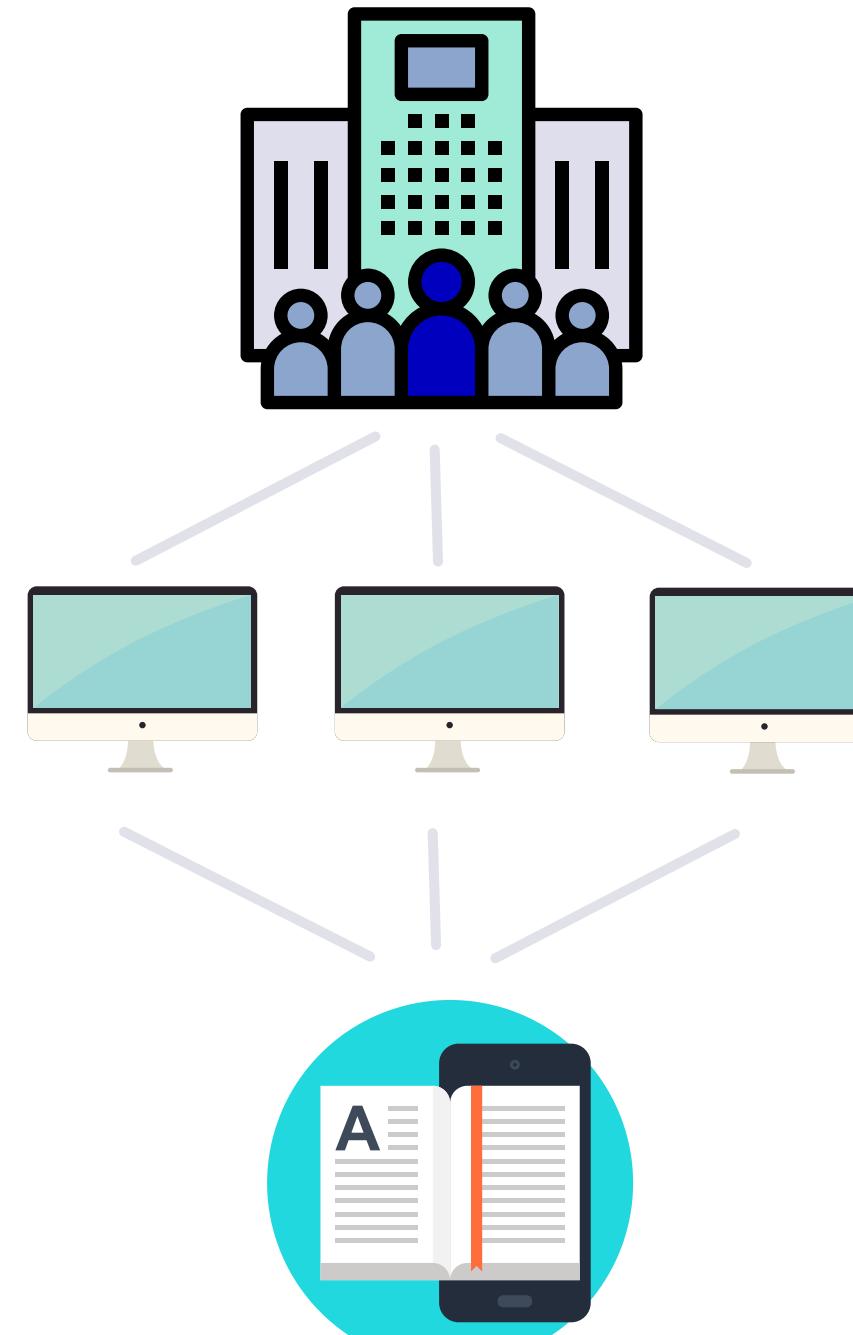
Verzeichnis nach Art. 30 DSGVO ist das Verzeichnis von Verarbeitungstätigkeiten

Ein Verzeichnisdienst

- Stellt in einem Datennetz Informationen über beliebige Objekte in einer definierten Art zur Verfügung
- In einem Objekt können zugehörige Attribute gespeichert werden
 - Z.B Name und Vorname des Benutzers, Personalnummer etc.
- Verwendung der Daten auf verschiedenen Rechnern und Applikationen
- Verwaltung des Verzeichnisdienstes und der Daten von zentraler Stelle



Ein Beispiel zum Verzeichnisdienst in der IT



- Unternehmen mit 100 Mitarbeitern
- Anmeldung aller Mitarbeiter an allen Firmen-Rechnern
- Dürfen aber nur die Ressourcen nutzen, auf die sie Zugriff haben
- Speicherung der Informationen zentral in einem Verzeichnisdienst
- Sonst müsste es 100 Benutzerkonten auf 100 Rechnern mit unterschiedlichen Rechten geben



Der Verzeichnisdienst bietet viele Vorteile



- Erleichterung beim Anlegen und Verwalten der Benutzerkonten
 - Bei Passwortänderung
 - Eine zentrale Änderung
 - Bei Verteilung der Berechtigungen
 - Einrichtung von unterschiedlichen Gruppen (Domäne) mit unterschiedlichen Berechtigungen



Weiterführende Literatur



- Europäische Datenschutz-Grundverordnung
- Orientierungshilfe zum Gesundheitsdatenschutz
- Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT



Mittagspause

12.00 Uhr - 13.00 Uhr



HY!