

A hand holding a glass ampoule in front of a medical monitor displaying vital signs. The monitor shows a heart rate of 124, blood pressure of 80/50, and a temperature of 37.5. A blue box on the screen displays the time 00:37:40. The background is a blurred medical setting.

BVMed - Datenschutz im Gesundheitswesen

Datenverarbeitung im Unternehmen

30. September 2025- RAin Maria Heil

Agenda



Grundlagen Datenschutz im Unternehmen



Datenkategorien und deren Verarbeitungsmöglichkeiten



Rechtfertigungstatbestände nach der DSGVO



Anforderungen an die Einwilligung nach der DSGVO



Betroffenenrechte



Beispiele für Datenverarbeitung im Unternehmen

WACHSTUMSPOTENZIAL DER GESUNDHEITSDATENWIRTSCHAFT



5,5 Mrd. EUR

Einsparungen für die EU über einen Zeitraum von zehn Jahren durch einen besseren Zugang zu und den Austausch von Gesundheitsdaten im **Gesundheitswesen**



20-30%

zusätzliches Wachstum des digitalen Gesundheitsmarktes



5,4 Mrd. EUR

Einsparungen für die EU über einen Zeitraum von zehn Jahren durch eine bessere Nutzung von Gesundheitsdaten **für Forschung, Innovation und Politikgestaltung**

Viele offene Fragen bei praktischer Umsetzung von Datenschutz

Informationspflichten
bei Vorkommnis-
Meldungen?

Datenverarbeitung in
Klinischen Prüfungen?

Anpassung der
internen Vigilanz-
SOP?

Weitergabe von
Daten an
Krankenkassen?

Schutz von
Vigilanzdaten?

Schwärzung vor
Weitergabe/ Archivierung
von Patientendaten?

Nutzung Secondary
Use-Daten?

Wann liegt eine
Auftragsverarbeitung vor?

Patientendaten an
den MDK?

Controller-Processor-
Konstellationen?

Schutz von
Gesundheitsdaten?

Interne Zugriffsregelungen
auf globale Vigilanz-
Datenbanken?

Globale Vigilanz-
Datenbanken?



Real World vs. Best Practice?



GRUNDLAGEN DATENSCHUTZ IM UNTERNEHMEN

Wo spielt Datenschutz im Unternehmen eine Rolle?

Eigentlich überall!

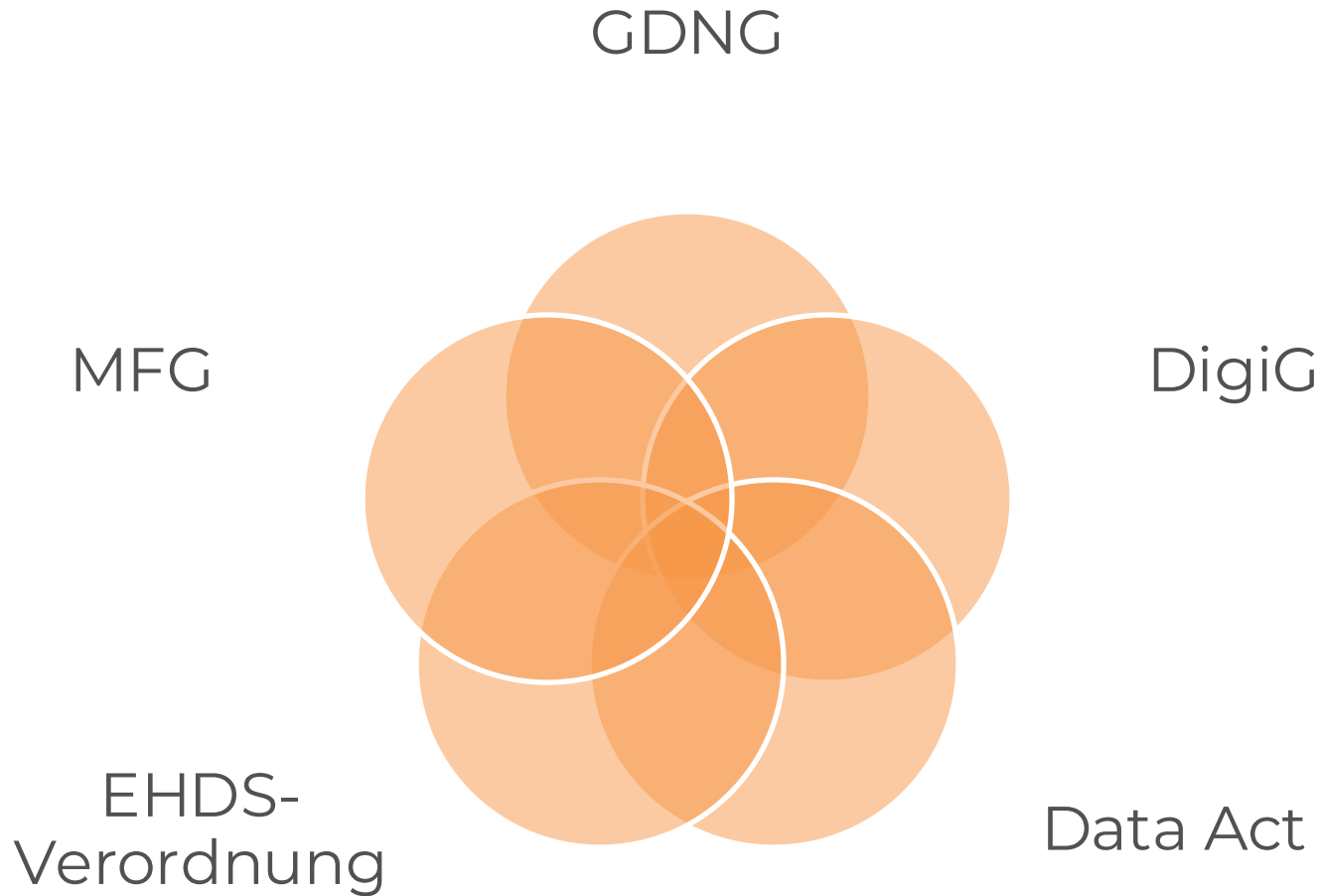


Welche Gesetze muss ich beachten?

- **Datenschutzgrundverordnung (DSGVO)**
- **Bundesdatenschutzgesetz (BDSG)**
- Telemediengesetz/
Telekommunikationsgesetz (TMG/TKG)
- Für öffentliche Stellen:
 - Landesdatenschutzgesetze
- Andere Spezialgesetze, z. B.
 - Gesundheitsdaten (SGB V)
 - Landeskrankenhausgesetze

Herausforderungen Gesundheitsdaten in der EU



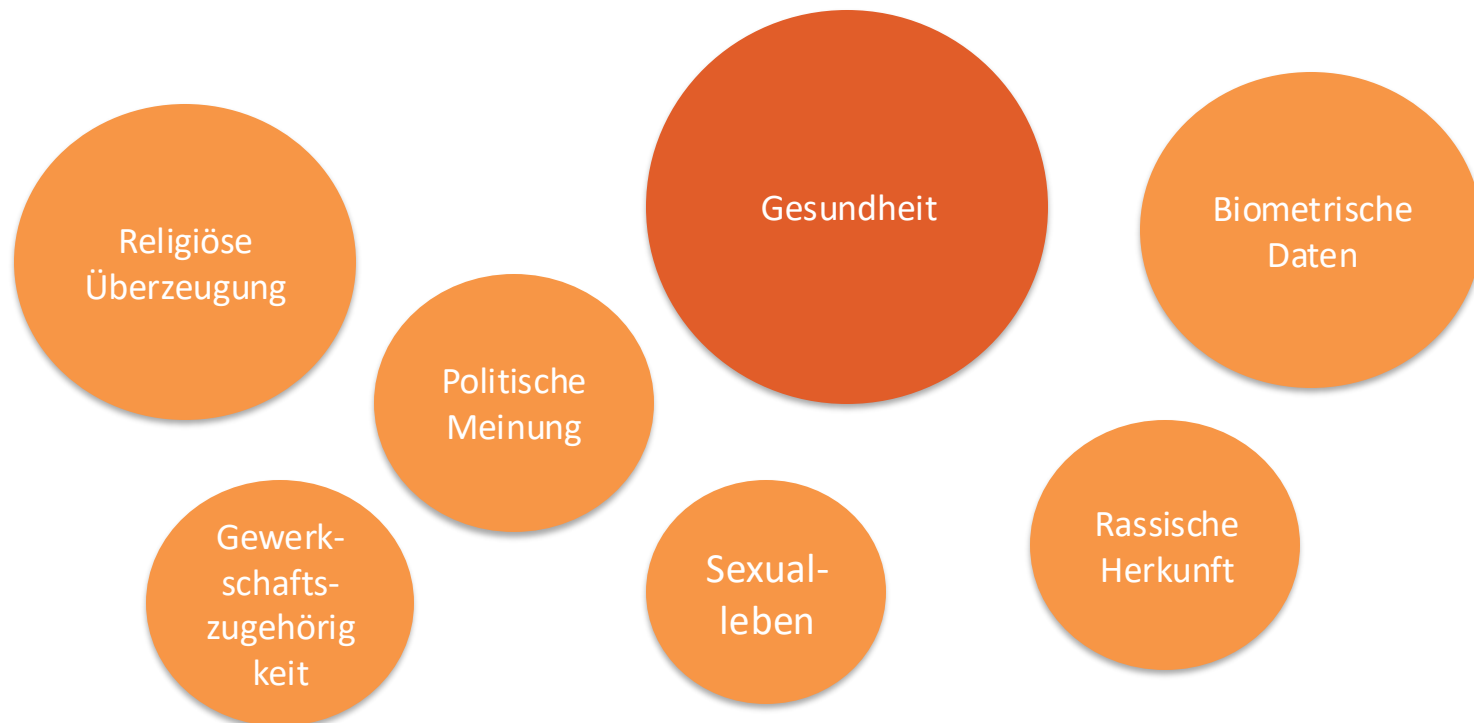


DATENKATEGORIEN UND DEREN VERARBEITUNGSMÖGLICHKEITEN

- „Alle Informationen, die sich auf eine **identifizierte oder identifizierbare natürliche Person** beziehen“



- Personenbezogene Daten, die eines
besonderen Schutzes bedürfen



Sind das jetzt personenbezogene Daten?



DSGVO und BDSG finden
keine Anwendung



DSGVO und BDSG finden
Anwendung

Wann sind Daten anonym?



- Datenschutzgesetze auf anonyme Daten nicht anwendbar
- Wann sind Daten „anonym“
 - Bislang: Anonym sind Daten dann, wenn sich der Personenbezug nicht mit einem verhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft herstellen lässt
 - Andere Ansichten zu restriktiv
- Modell USA HIPAA
- Vollständige Anonymität bei personalisierter Medizin kaum möglich

Wann sind Daten anonym?

- Neue Entwicklung in europäischer Rechtsprechung
- Frühere EuGH-Entscheidungen (z. B. EuGH v. 19. 10. 2016 – Rs C-582/16)
 - IP-Adressen: Personenbezogen, wenn Zusatzwissen Dritter zur Identifikation ausreicht
 - Anonymisierung gilt nur, wenn Identifikation praktisch unmöglich ist
- EuG-Entscheidung (EuG v. 26. 4. 2023 – Rs T-557/20)
 - Anonymisierung = Daten sind für das Unternehmen nicht personenbezogen, wenn es keine Mittel hat, um die Person zu identifizieren
 - Relatives Verständnis der Anonymisierung: Perspektive des Unternehmens zählt
- EuGH-Entscheidung 2023 (EuGH v. 9. 11. 2023 – Rs C-319/22)
 - Relativer Ansatz: Daten gelten als personenbezogen, wenn ein Unternehmen Mittel hat, um sie einer Person zuzuordnen
- Aber EuGH auch 2023 (EuGH v. 7. 3. 2024 – Rs C-604/22)
 - Daten können bereits personenbezogen sein, auch wenn nicht alle Identifizierungsinformationen bei einer einzigen Partei vorliegen

- Begriff Art. 4 Nr. 2 DSGVO
 - Jeder Vorgang oder Vorgangsreihe („*operation or set of operation*“)
 - Mit personenbezogenen Daten
 - Unabhängig davon, ob automatisiertes Verfahren oder nicht
- Unverändert weit (nur geringfügige sprachliche Anpassungen gegenüber Richtlinie)

Datenverarbeitung (Beispiele)

Speichern

Erfassen

Erheben

Auslesen

Bereitstellung

Verwendung

Abfragen

Offenlegung

Verbreitung

Einschränkung

Löschen

Verknüpfung

Organisation

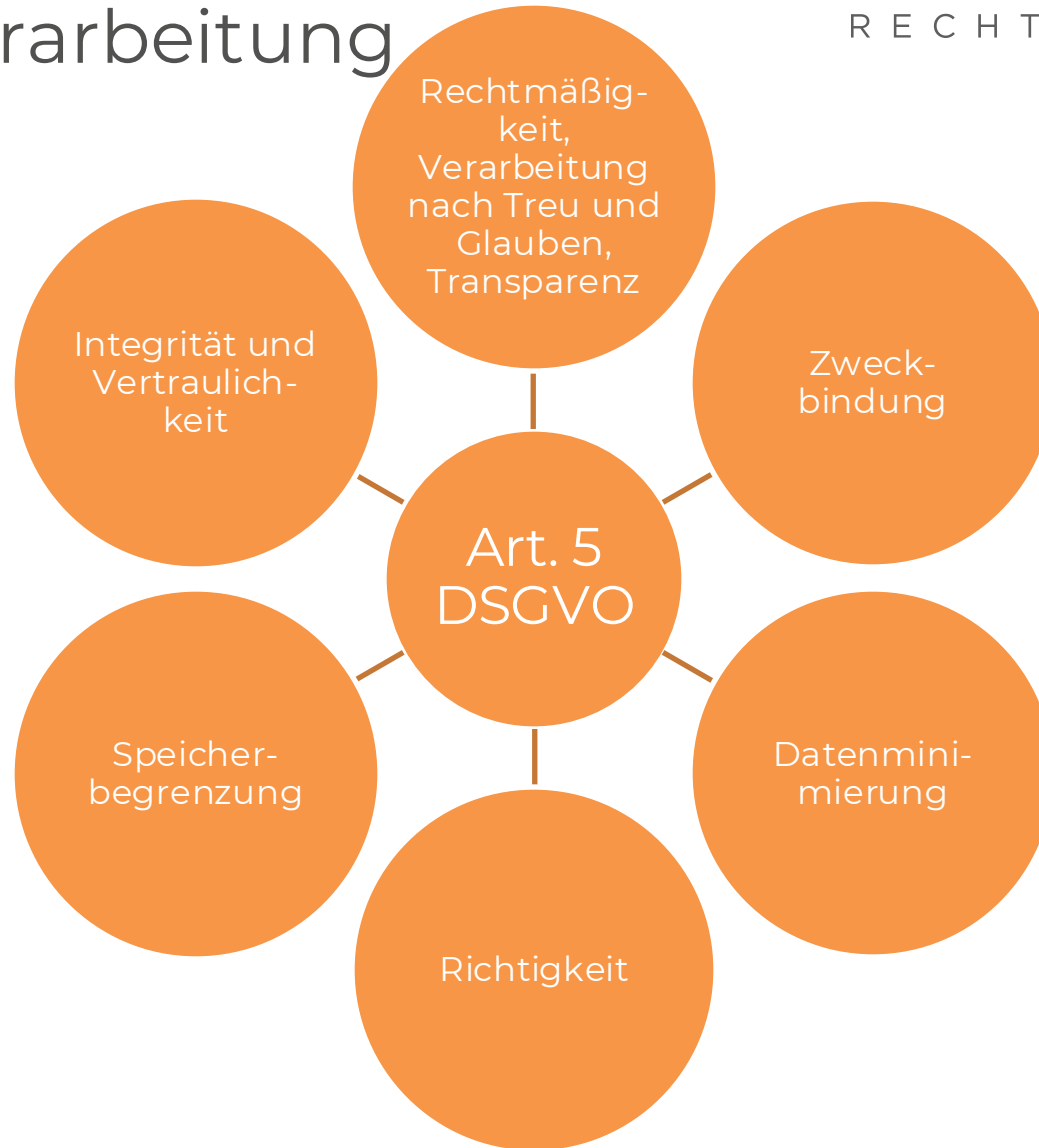
Anpassung

Veränderung

Ordnen

RECHTFERTIGUNGSTATBESTÄNDE NACH DER DSGVO

Prinzipien der Datenverarbeitung



■ **Verbot mit Erlaubnisvorbehalt**

- Art. 6 DSGVO: „Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:“
- Grundsatz: Jede Verarbeitung von personenbezogenen Daten durch ein Unternehmen muss ausdrücklich durch die DSGVO, das BDSG-neu oder ein anderes Gesetz erlaubt sein.
- Sonst: **unzulässig!**

Allgemeine Rechtfertigungsgründe



Besondere Rechtfertigungsgründe

Art. 7 und 8 DSGVO (Anforderungen an einwilligungsbasierte Rechtfertigungen)

Art. 9 DSGVO (Besondere Datenkategorien)

Art.10 DSGVO (Strafurteil)

Art. 11 DSGVO (Verarbeitung ohne Bestimmung der Betroffenen)

Teilweise Öffnungsklauseln in nationales Recht

ANFORDERUNGEN AN DIE EINWILLIGUNG NACH DER DSGVO

Freiwilligkeit

- Autonome und ausdrücklich selbstbestimmte Entscheidung
- Elektronische Einwilligung grds. zulässig (Erwägungsgrund 32)

Informiertheit

- Streng zweckgebunden (Information muss rechtfertigende Verarbeitungszwecke anführen)
- Spätere Zweckänderung nur in Ausnahmefällen möglich (Art. 6 Abs. 4 DSGVO), deshalb sorgfältig entwerfen!
- Generaleinwilligung weiterhin nicht möglich

Ausdrückliche und konkrete Willensbekundung

- Opt-in reicht aus
- Opt-out unzulässig (Erwägungsgrund 32)

Dokumentationspflicht (Beweisbarkeit)

Transparenzgebot beachten

Widerruflichkeit

- Jederzeit mit Wirkung für die Zukunft

Besondere Erfordernisse bei Kindern (Art. 8
DSGVO)

BETROFFENENRECHTE

Rechte der Betroffenen

Durch DSGVO gestärkt

Art. 13, 14 DSGVO

- Informationspflichten, abhängig von Art der Informationserhebung (unmittelbar/mittelbar)

Art. 15 DSGVO

- Auskunftsrecht

Art. 16 DSGVO

- Recht auf Berichtigung

Art. 17 DSGVO

- Recht auf Löschung (einschließlich Recht auf Vergessenwerden)

Art. 18 DSGVO

- Recht auf Einschränkung der Verarbeitung

Art. 20 DSGVO

- Recht auf Datenübertragbarkeit

Art. 21 DSGVO

- Widerspruchsrecht

BEISPIELE FÜR DATENVERARBEITUNG IM UNTERNEHMEN

- Mögliche Rechtfertigung Vertragserfüllung/ Durchführung vorvertraglicher Maßnahmen, z. B.
 - Kontaktdaten
 - Bankverbindung
 - Vertragsinhalte, die für Abwicklung erforderlich sind
- Andere Daten: Einwilligung der Kunden erforderlich, z. B.
 - Persönliche Interessen und Vorlieben
 - Familiäre Verbindungen
- Problem Datensparsamkeit
 - Überprüfung Zugriffsregelungen
 - Zeitliche Grenzen

Beispiel: Die Buchhaltung wird von einer anderen Konzerngesellschaft übernommen.

- Galt bislang nicht, auch in DGSVO nicht aufgenommen
- Aber Erwägungsgrund 48: ggf. interne Verwaltungszwecke als berechtigtes Interesse
- Möglich auch bei Verarbeitung personenbezogener Daten von Kunden und Beschäftigten
- Dokumentation erforderlich

Beispiel: Externer Referent für interne
Fortbildungsveranstaltung, Daten in CRM

- Speicherung von Daten für Vertragsanbahnung und –umsetzung weiterhin zulässig
- Einwilligung erforderlich, wenn
 - Gespeicherte Daten nicht erforderlich für Vertragsumsetzung sind
 - Auch andere Konzerngesellschaften Zugriff auf Daten haben (ggf. Systeme überarbeiten)

Beispiel: Speicherung von Arbeitszeugnissen in Personalakte

- Öffnungsklausel für nationales Recht in Art. 88 DSGVO, umgesetzt in § 26 BDSG-neu
- Datenverarbeitung danach zulässig für
 - Entscheidungen über die Begründung eines Beschäftigungsverhältnisses
 - Durchführung oder Beendigung des Beschäftigungsverhältnisses
 - Ausübung oder Erfüllung der sich aus einem Gesetz oder einer Kollektivvereinbarung (auch Betriebsvereinbarungen) ergebenden Rechte und Pflichten der Interessenvertretung von Beschäftigten

SPEZIALTHEMEN GESUNDHEITSDATENSCHUTZ

Datenschutz in klinischen Prüfungen



Handhabung Datenschutz in klinischen Prüfungen nach Inkrafttreten der DSGVO sehr heterogen



Problem: Durchführung von multinationalen Studien



Rechtfertigung des Datentransfers (datenschutzrechtliche Einwilligung?)



Datenschutzrechtliche Rolle der medizinischen Einrichtungen (controller, joint controller, processor?)

Beispiel: Datenkauf von Behandlungsdaten zur
Weiternutzung im Unternehmen

Anonymi-
sierung

Ursprüngliche
Zweckbe-
stimmung

Broad
Consent/Breite
Einwilligung

Nachträgliche
Einwilligung

Enge
Zweckbindung

Nachträgliche
Einwilligung

Verwendung der EHDS-Daten

Primärnutzung:

Zugang Patienten zu ihren Gesundheitsdaten und Verarbeitung zu Zwecken der Gesundheitsversorgung

Angehörige der Gesundheitsberufe erhalten Zugang zu den Gesundheitsdaten der von ihnen behandelten Patienten

Aufbau einer grenzüberschreitenden Dateninfrastruktur (MyHealth@EU) zur Nutzung von Daten in der Versorgung

Sekundärnutzung:

Ermöglichung der Nachnutzung von Daten für Forschung, Innovation, Patientensicherheit, personalisierte Medizin, amtliche Statistik, Regulierungstätigkeiten

Aufbau einer europäischen Dateninfrastruktur (HealthData@EU) zur grenzüberschreitenden Sekundärnutzung

Daten sind über Datenzugangsstellen zugänglich

Ziele GDNG:

- Ausbau dezentrale Infrastruktur für Gesundheitsdaten
- Bessere Verfügbarkeit und Nutzung von Gesundheitsdaten für Versorgung, Wissenschaft und Innovation (insbesondere Abrechnungsdaten aus Forschungszentrum)
- Readiness für EHDS

Zentrale Datenzugangs-
und Koordinierungsstelle
für Gesundheitsdaten

Weiterentwicklung
Forschungsdaten-
zentrum Gesundheit

Aufbau einer europäisch
anschlussfähigen
Infrastruktur

Verknüpfung von Daten
der Krebsregister mit
Daten des
Forschungsdaten-
zentrums

Weiterentwicklung
Datenfreigabe aus der
ePA, § 363 SGB V

Weiterverarbeitung erhobener
Versorgungsdaten für
bestimmte Zwecke erlaubt:

- Eigenforschung im
medizinischen, rehabilitativen
und pflegerischen Bereich
- Qualitätssicherung und
Patientensicherheit
- Statistische Zwecke
- Gesundheitsberichtser-
stattung

Datenverarbeitung auf allen Ebenen im Unternehmen ein wesentlicher Bestandteil der Arbeit

Auf europäischer und nationaler Ebene viele Gesetzgebungsvorhaben im Fluss, die Einfluss auf zukünftige Datengestaltung haben werden

Datenstrategie im Unternehmen wichtig, Umsetzung und Know-How auf allen Mitarbeitererebenen erforderlich

In Zukunft noch wichtiger: Dokumentation der einschlägigen Erlaubnistatbestände (auch im Hinblick auf mögliche Bußgelder)



VIELEN DANK!

Maria Heil, M.C.L.
Schadowplatz 12
D-40212 Düsseldorf

T +49 211 9099 3665
F +49 211 9099 3699
maria.heil@novacos-law.com
www.novacos-law.com

© 2025 NOVACOS Rechtsanwälte
Heil Hübner Natz Oeben Stallberg Partnerschaft mbB
Sitz Düsseldorf I AG Essen PR 3581

