Datenschutz/-sicherheit

Sebastian Straub

Institut für Innovation und Technik (iit)

Mit der Begleitforschung für die Programme Smarte Datenwirtschaft und KI-Innovationswettbewerb des Bundesministeriums für Wirtschaft und Energie ist das Institut für Innovation und Technik (iit) in der VDI/VDE Innovation + Technik GmbH zusammen mit dem KI Bundesverband e.V. und der LoeschHundLiepold Kommunikation GmbH (LHLK) beauftragt.

Anwendungsbereich der DSGVO

Verarbeitung von personenbezogenen Daten

Anonyme Daten

Anonymisierte Daten

Pseudonymisierte Daten

Vorsicht bei Annahme von Anonymität!

Personenbezogen Daten Informationen, die sich auf eine identifizierbare oder identifizierte Person beziehen

Verbot mit Erlaubnisvorbehalt

Die Verarbeitung von (...) Gesundheitsdaten einer natürlichen Person ist untersagt
(Art. 9 Abs. 1 DSGVO)

Gesundheitsdaten beziehen sich auf körperliche oder geistige Gesundheit einer Person

Ausnahmen:

- Ausdrückliche Einwilligung der betroffenen Person (Art. 9 Abs. 2 lit. a)
- Versorgung im Gesundheitsbereich (Art. 9 Abs. 2 lit. h)
  medizinische Behandlungen, unter Voraussetzungen des Art. 9 Abs. 3, insbesondere Verpflichtung zur Geheimhaltung
- Öffentliches Gesundheitswesen (Art. 9 Abs. 2 lit. i)
  öffentliches Interesse im Zusammenhang mit Gefahrenabwehr im Gesundheitsbereich und zur Qualitätssicherung bei der Gesundheitsversorgung
- Archivzwecke, Forschung, Statistik, Art. 9 Abs. 2 lit. j
  auf rechtlicher Grundlage und mit angemessenen Schutzmaßnahmen

Allgemeine Öffnungsklausel für eigene nationale Regelungen, wenn Gesundheitsdaten betroffen sind
(Art. 9 Abs. 4 DSGVO)

Nationale Rechtsgrundlagen

Bund	Länder
Bundesdatenschutzgesetz (BDSG)	Krankenhausgesetze (kirchliches Recht bei Krankenhäusern in kirchlicher Trägerschaft)
Sozialgesetzbücher (SGB)	Krebsregistergesetze
Infektionsschutzgesetz (InfSchG)	Gesundheitsdienstgesetze
Transplantationsgesetz (TPG)	Psychisch-Kranken-Gesetze
Medizinproduktegesetz (MPG)	Maßregelvollzugsgesetze
Transfusionsgesetz (TFG)	…weitere
Versicherungsvertragsgesetz (VVG)	
…weitere	

Aufgrund der fragmentierten Rechtslage wird häufig auf Einwilligung zurückgegriffen

Einwilligung

Freiwilligkeit

- echte Wahl muss gegeben sein
- Verbot von Koppelung

Bestimmtheit

- nicht pauschal
- Erkennbarkeit welche Daten zu welchem Zweck und durch wen verarbeitet werden

Informiertheit

- Kenntnisnahme des Inhalts ist zumutbar möglich
- Erklärung ist verständlich (inhaltlich, sprachlich) und hervorgehoben

Widerrufbarkeit

- Recht Einwilligung jederzeit zu widerrufen
- Rechtmäßigkeit der bisherigen Verarbeitung bleibt unberührt
- Pflicht zur Löschung, wenn keine einer anderweitigen Rechtsgrundlage vorhanden

Sonderfall Broad Consent
Einwilligung für bestimmte Bereiche wissenschaftlicher Forschung

Zusätzlich sind ärztliche Schweigepflicht und Sozialgeheimnisschutz beachten

Grundsatz der Zweckbindung

Zweckbindung	Verbot der Weiterverarbeitung	Forschungsprivileg
• Personenbezogene Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke erhoben werden	• Eine Weiterverarbeitung zu anderen Zwecken ist nicht gestattet, wenn kein anderer legitimer Zweck vorliegt oder die Zwecke nicht miteinander vereinbar/kompatibel sind (Zweckkompatibilitätstest)	• Die Weiterverarbeitung (Zweckänderung) für öffentliche Zwecke wie zum Beispiel wissenschaftlicher Art (Forschung) ist privilegiert und es wird vermutet, dass sie als vereinbar mit ursprünglichen Zwecken gilt

Broad Consent

- Broad Consent: Möglichkeit Einwilligung für **bestimmte Bereiche wissenschaftlicher** Forschung zu geben, wenn dies unter Einhaltung der anerkannten ethischen Standards der wissenschaftlichen Forschung geschieht (Erwägungsgrund 33)
- Die Einwilligung zur Verarbeitung personenbezogener Daten zu Forschungszwecken kann für ein bestimmtes Vorhaben oder für **bestimmte Bereiche der wissenschaftlichen Forschung** erteilt werden (§ 67b SGB X)

IT-Sicherheit

- Art. 32 DSGVO: Um ein angemessenes Schutzniveau zu erreichen sind geeignete **technische und organisatorische Schutzmaßnahmen** im Wege einer eigenständigen Risikobewertung zu bestimmen
- IT-Sicherheitsgesetz (1.0)
  - Adressaten: Krankenhäuser, Hersteller von Medizinprodukten, Arzneimittelhersteller, Apotheken
  - Pflichten greifen erst bei Erreichen von bestimmten Schwellenwerten
  - Einhaltung des Stands der Technik
  - Zwischenfälle mit erhöhtem Risikopotential lösen Meldepflichten aus
  - IT-Sicherheitsgesetz 2.0
    - Erweiterung auf KRITIS-Kernkomponenten
    - Pflicht zur Einführung von Intrusion Detection Systemen (IDS)