

Klinische Register

Fachtagung Datenschutz im Gesundheitswesen 2020

Referent: David Koeppe

Betrachtungsgegenstand

Insbesondere im klinischen Umfeld ist es üblich, fachrichtungsbezogene und überbetriebliche Behandlungsdatensammlungen anzulegen. Diese Register dienen meist der Qualitätssicherung, z.B. im Rahmen von Zertifizierungsverfahren, und werden oft durch bzw. im Auftrag medizinischer Fachgesellschaften betrieben.

Agenda

- Rechtlicher Rahmen
 - Rechtmäßigkeit
 - Bedingungen

- Ausgestaltungsoptionen
 - Getrennte Verantwortlichkeiten
 - Gemeinsame Verantwortung
 - Auftragsverarbeitung

Rechtlicher Rahmen

Rechtmäßigkeit I

Qualitätssicherung:

„(...) die Verarbeitung ist (...) zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten (...) erforderlich“

- Rechtmäßigkeit ist gemäß Art. 9 Abs. 2 lit. i DS-GVO i.V.m. § 22 Abs. 1 lit. c BDSG möglich.

Rechtmäßigkeit II

Forschung:

„die Verarbeitung ist (...) für wissenschaftliche oder historische Forschungszwecke (...) erforderlich“

- *Rechtmäßigkeit ist gemäß Art. 9 Abs. 2 lit. j DS-GVO i.V.m. § 27 BDSG und Art. 89 DS-GVO möglich.*

Bedingungen für die QS I

Art. 9 Abs. 1 lit i DS-GVO:

Europäisches oder nationales Recht muss
„angemessene und spezifische Maßnahmen zur
Wahrung der Rechte und Freiheiten der
betroffenen Person, insbesondere des
Berufsgeheimnisses, vorsehen“

Bedingungen für die QS II

Daher § 22 Abs. 2 BDSG:

- angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person
- Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen können dazu insbesondere gehören:

Bedingungen für die QS III

Fortsetzung § 22 Abs. 2 BDSG:

1. technisch organisatorische Maßnahmen, um sicherzustellen, dass die Verarbeitung gemäß der Verordnung (EU) 2016/679 erfolgt,
2. Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind,
3. Sensibilisierung der an Verarbeitungsvorgängen Beteiligten,
4. Benennung einer oder eines Datenschutzbeauftragten,
5. **Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der verantwortlichen Stelle und von Auftragsverarbeitern,**
6. **Pseudonymisierung personenbezogener Daten,**
7. **Verschlüsselung personenbezogener Daten,**
8. Sicherstellung der Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten, einschließlich der Fähigkeit, die Verfügbarkeit und den Zugang bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,
9. zur Gewährleistung der Sicherheit der Verarbeitung die Einrichtung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen oder
10. **spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung für andere Zwecke die Einhaltung der Vorgaben dieses Gesetzes sowie der Verordnung (EU) 2016/679 sicherstellen.**

Bedingungen für die QS IV

Spezialgesetzliche Anforderungen, z.B. der Landeskrankenhausgesetze

Beispiel Berlin (§ 24):

Sofern nicht anonymisiert/pseudonymisiert: zur
Qualitätssicherung der Behandlung nur an
eine/n Ärzt*in oder ärztlich geleitete Stelle

Bedingungen für die QS IV

Spezialgesetzliche Anforderungen, z.B. der Landeskrankenhausgesetze

Beispiel Berlin (§ 24):

Sofern nicht anonymisiert/pseudonymisiert zur
Qualitätssicherung der Behandlung nur an
eine/n Ärzt*in oder ärztlich geleitete Stelle

Die große Frage

Einwilligungserfordernis?

Ist dann anzunehmen, wenn die gesetzlichen Anforderungen für das Vorliegen der Rechtmäßigkeit nicht (zur Gänze) erfüllt werden. Bsp.:

- Zertifizierung als Marketing-, nicht als QS-Instrument („verfehlt“ Zweck)
- Fehlende Anonymisierung, unzureichende Pseudonymisierung (Schaffung einer Offenbarungsbefugnis)

Ausgestaltungsoptionen

Maßgabe: Registergestaltung

Geschäftsmodell des Registerbetreibers ist entscheidend

- i.d.R. 1-n Beziehungen zu Datenlieferanten
- Festlegung der Mittel und Zwecke erfolgt langfristig
- Gewährung von Betroffenenrechten
- (datenschutzrechtliche) Einbindung eines technischen Dienstleisters

Getrennte Verantwortlichkeiten

Übermittlung mit klarem Verantwortungsübergang

- Für Datenlieferanten vorteilhaft
- Betroffenenrechte bleiben (angesichts von Pseudonymisierung/Anonymisierung) grds. auf der Strecke (Art. 11 DS-GVO)

Gemeinsame Verantwortung

Datenlieferant bleibt dauerhaft in der (Mit-) Verantwortung für eingemeldete Daten

- Gewährleistung der Betroffenenrechte gut möglich
- Bevorzugte Ausgestaltung für die Registerführung

Auftragsverarbeitung

Registerbetreiber als Auftragsverarbeiter

- i.d.R. untauglich, da vollumfängliche Verantwortung des Einmeldenden fiktiv
- Widersprüchliche Weisungen unterschiedlicher Einmelder gefährden Konsistenz des Registers
- Absenz registereigener Verarbeitungszwecke in der Praxis unwahrscheinlich

Technischer Dienstleister

Betreiber der technischen Plattform

- Einbindung sollte als Auftragsverarbeitung erfolgen
- Verantwortlich: Registerbetreiber

Fazit

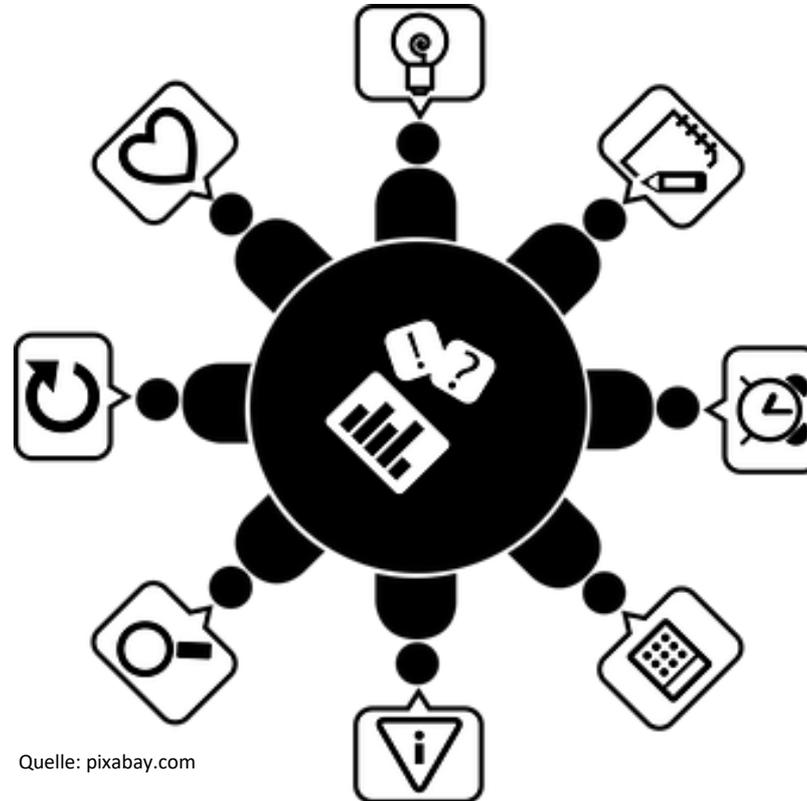
Datenschutz ist auch in der QS kein Anhängsel

- Das Medizinische Anliegen hat sich in einem (datenschutz-)rechtlichen Rahmen zu bewegen
- Ausgestaltung der Aufbau - und Ablauforganisation determiniert die Datenschutzorganisation
- ... und: Betroffeneninformation!

Zum Nachlesen

Praxishilfe „Klinische Register und Datenschutz“:
[https://www.gesundheitsdatenschutz.org/html/
klin_register.php](https://www.gesundheitsdatenschutz.org/html/klin_register.php)

Diskussion



Quelle: pixabay.com