



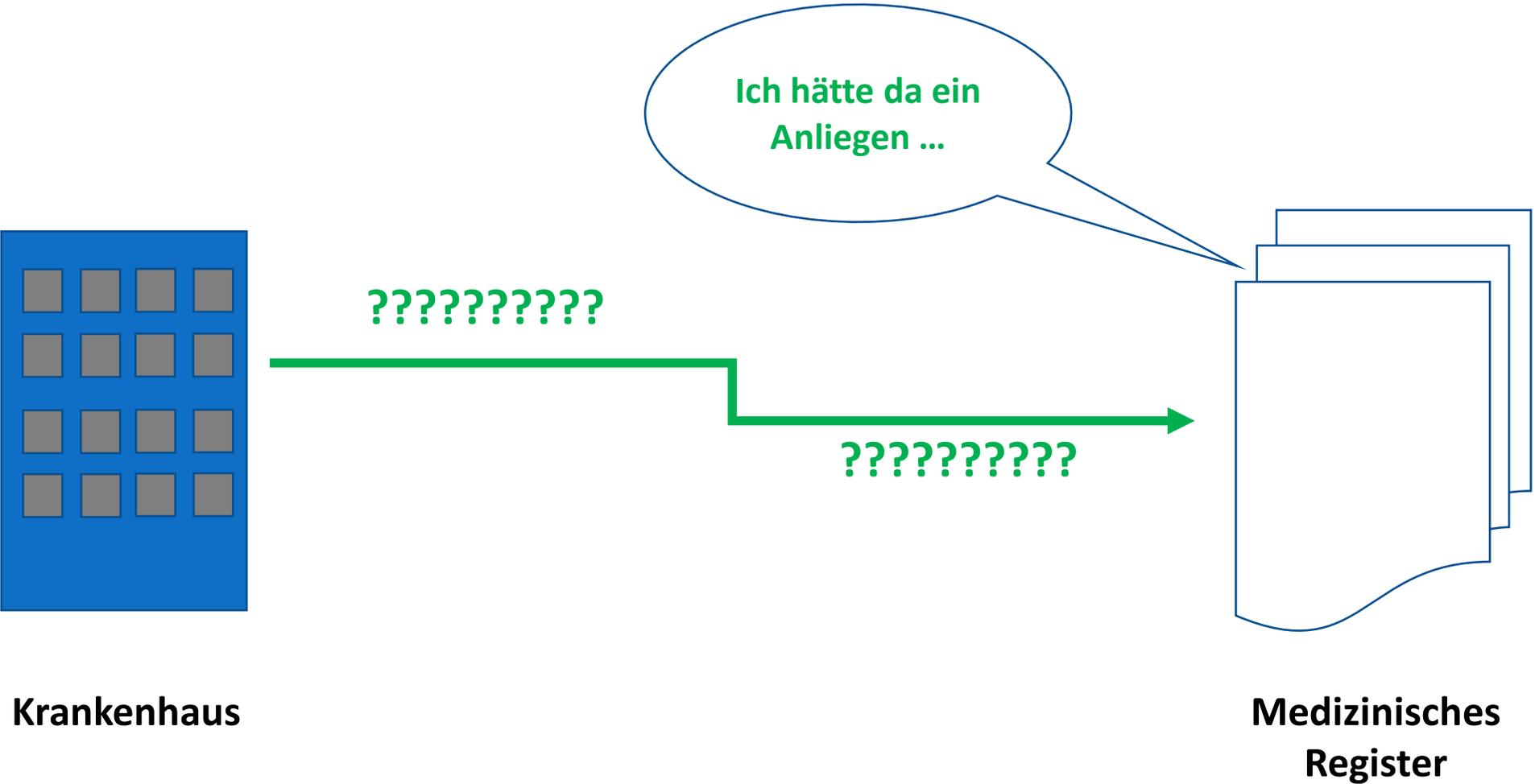
Integrierter
Datenschutz



Klinische Register und Datenschutz: Patientendaten – Woher nehmen?

Andrea Backer-Heuveldop | ds² Unternehmensberatung GmbH & Co. KG

Die einen haben sie – die anderen wollen sie: Patientendaten



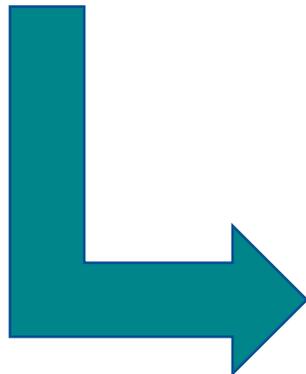
Allgemein zu beachten

Schutz besonderer Kategorien personenbezogener Daten:

Art. 9 DS-GVO:

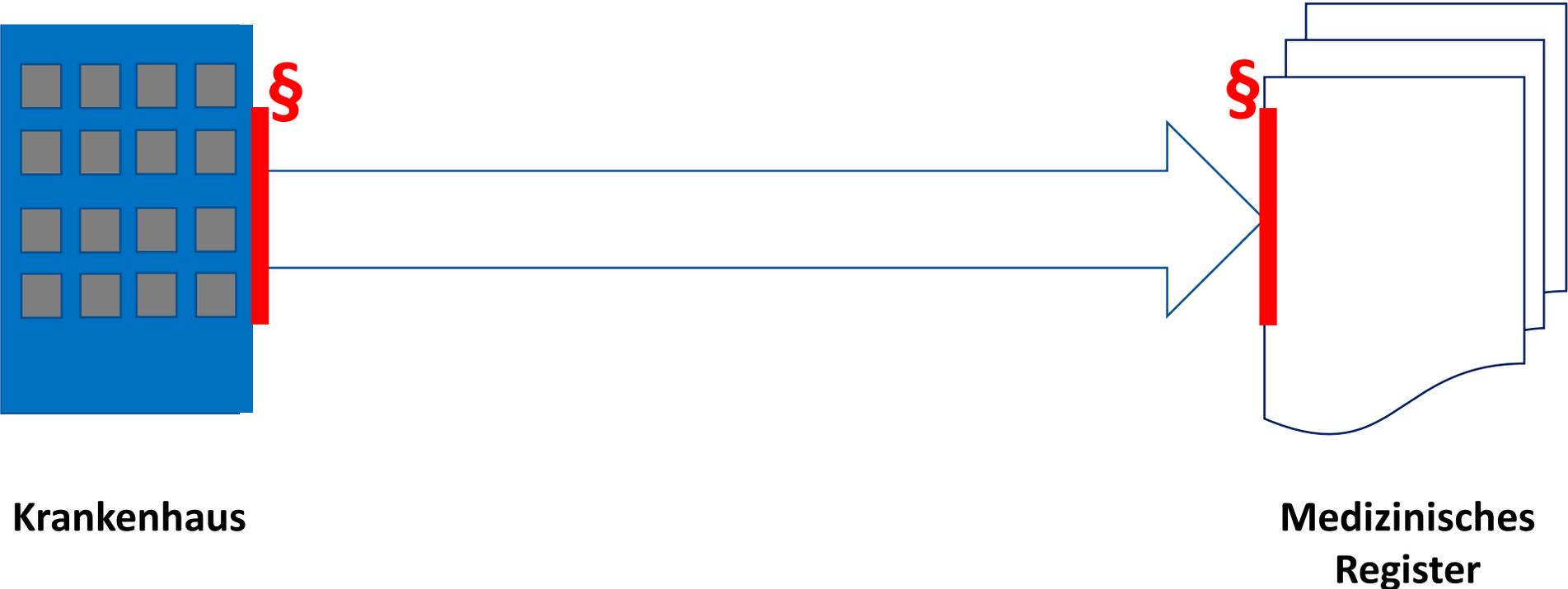
„(1) Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie **die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten** oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person **ist untersagt.**“

(2) Absatz 1 gilt nicht in folgenden Fällen: ...



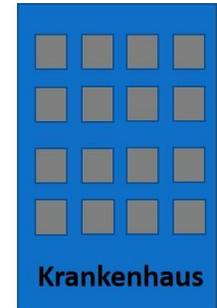
Ohne Erlaubnis keine Zulässigkeit der Verarbeitung dieser Daten
(gesetzliche Grundlage oder Einwilligung der betroffenen Person)

Patientendaten in klinischen Registern – aber zulässig!



Im Krankenhaus vor der Weitergabe der Daten zu beachten

- Aktuell keine bundesweit einheitlich geltende spezialgesetzliche Befugnisnorm für eine Weitergabe an jegliches Register
- Ausnahmetatbestände für die Verarbeitung von Patientendaten im Krankenhaus und die Weitergabe / Offenlegung an Dritte richtet sich in aller Regel nach dem für die jeweilige Klinik geltenden Landesrecht und den darin angeführten Zwecken, hier:
 - Qualitätssicherung in der stationären Versorgung (i. d. R. Einwilligung)
 - sowie Forschungszwecke (ggf. Forschungsprivilegierung ohne Einwilligung)
- ggf. sind die Vorgaben aus dem Landesrecht selbst dann einzuhalten, wenn eine Einwilligung der betreffenden Patienten vorliegen sollte
- ggf. Anforderungen an eine datenschutzkonforme Einwilligung
- Übersichten über die einschlägigen Regelungen in den verschiedenen Landesgesetzen und Anforderungen für ausgewählte Szenarien finden sich in der Praxishilfe für medizinische Register und datenliefernde Krankenhäuser „Landesrechtliche Anforderungen an medizinische Register: Was zu beachten ist“



Vom Register vor Empfang und Weiterverarbeitung zu beachten

- Aktuell keine bundesweit einheitlich für alle Register geltende spezialgesetzliche Befugnisnorm für die Erhebung und Verarbeitung durch das Register
- Sofern im Einzelfall keine spezialgesetzliche Rechtsgrundlage vorliegt, in der Regel ausdrückliche Einwilligung erforderlich
- Vorliegen eines Ausnahmetatbestands für die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 DS-GVO, hier Gesundheitsdaten für
 - den Zweck der Qualitätssicherung § 22 Abs. 1 lit. c BDSG
 - Forschungszwecke § 27 BDSG i. V. m. Art. 9 Abs. 2 lit. j DS-GVO
 - ausdrückliche Einwilligung gem. Art. 9 Abs. 2 lit. a DS-GVO
- Übersichten über die einschlägigen Regelungen und Anforderungen für ausgewählte Szenarien finden sich in der Praxishilfe für medizinische Register und datenliefernde Krankenhäuser „Landesrechtliche Anforderungen an medizinische Register: Was zu beachten ist“



Bundesweit tätige Register | Zweck: Qualitätssicherung

Rechtsgrundlage für die Übermittlung von Patientendaten durch das Krankenhaus an das Register: i. d. R. mangels Privileg die Einwilligung der Patienten

Rechtsgrundlage für die Qualitätssicherung des Registers: § 22 Abs. 1 lit. c BDSG i. V. m. Art. 9 Abs. 2 lit. i DS-GVO



Zu beachtende Voraussetzungen:

1. Verarbeitung erfolgt aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit,
2. Berufsrechtliche und strafrechtliche Vorgaben zur Wahrung des Berufsgeheimnisses werden eingehalten
3. Verarbeitung zu diesen Zwecken muss erforderlich sein
4. Angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gemäß § 22 Abs. 2 S. 2 BDSG existieren

Bundesweit tätige Register | Zweck: Forschung

Rechtsgrundlage für die Übermittlung von Patientendaten durch das Krankenhaus an das Register: i. d. R. mangels Privileg die Einwilligung der Patienten

Rechtsgrundlage für Forschungsvorhaben des Registers: § 27 BDSG i. V. m. Art. 9 Abs. 2 lit. j DS-GVO: § 22 Abs. 1 lit. c BDSG i. V. m. Art. 9 Abs. 2 lit. i DS-GVO



Zu beachtende Voraussetzungen:

1. Nachweis über wissenschaftliche oder historische Forschung liegt vor,
2. Verarbeitung der Daten zu diesen Zwecken ist erforderlich,
3. die Interessen des Registers an der Verarbeitung überwiegen die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung erheblich,
4. angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gemäß § 22 Abs. 2 S. 2 BDSG existieren und
5. Daten wurden anonymisiert oder, falls nicht möglich, pseudonymisiert

Datenschutzkonforme Einwilligungen

„**Einwilligung**“ der betroffenen Person:

jede **freiwillig** für den bestimmten Fall, **in informierter Weise** und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. [Art. 4 Nr. 11 DS-GVO]



Die DSGVO, das BDSG und bereichsspezifische Vorgaben enthalten eine Reihe an Bestimmungen bezüglich der Anforderungen an datenschutzrechtliche Einwilligungen.

Anforderungen an datenschutzkonforme Einwilligungen

- **Allgemeine Anforderungen an die Einwilligung: Art. 7 DSGVO**
- Umfangreiche Nachweispflicht aus Art. 7 Abs. 1 DSGVO
- Besondere Anforderungen an die Einwilligung Minderjähriger:
 - Zu beachtende feste Altersgrenze für die Einwilligungsfähigkeit bei Inanspruchnahme von Diensten der Informationsgesellschaft: Art. 8 Abs. 1 DSGVO (z. B. Einwilligungen im Rahmen der Nutzung von Gesundheitsapps)
 - Zu beachtende Anforderungen an die Einsichts- und Urteilsfähigkeit Minderjähriger bei anderen Einwilligungen in Einzelfallbetrachtung



Anforderungen an datenschutzkonforme Einwilligungen

- Widerrufsmöglichkeit:
 - jederzeit mit Wirkung für die Zukunft
 - durch den Widerruf wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt.
 - Information über Widerrufsmöglichkeit muss vor Abgabe der Einwilligung erfolgen
 - Widerruf muss so einfach sein wie Einwilligungserteilung
- **Cave: bei besonderen Kategorien pbD muss eine Einwilligung für einen oder mehrere festgelegte Zwecke ausdrücklich erteilt werden!**
- Broad Consent: nur für bestimmte Bereiche wissenschaftlicher Forschung (vgl. EWG 33)



Herausforderungen datenschutzkonformer Einwilligungen

- Einwilligungsmanagement:
 - Durchleitung eingegangener Widerrufe durch das einholende Haus an das Register
 - Nachweisbarkeit der Einwilligung für alle Beteiligten
 - Geltungsdauer: ggf. Löschung veralteter Einwilligungserklärungen
 - Berücksichtigung der Anforderungen und Etablierung von Kontrollen
- Hürden spezieller Szenarien
 - Einwilligungsunfähige Patienten / vor Erteilung einer Einwilligung verstorbene Patienten
 - Erforderlichkeit von Vollerhebung
- Praxishilfe Die datenschutzrechtliche Einwilligung: Freund (nicht nur) des Forschers



Anonymisierung / Pseudonymisierung – Mittel der Wahl?

- Regelfall in Registern: Verarbeitung pseudonymisierter Daten
- „Pseudonymisierung“ die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden [Art. 4 Nr. 5 DS-GVO]
 - Re-Identifizierungsrisiken umso größer, je feiner und umfangreicher der Datensatz



Anonymisierung / Pseudonymisierung – Mittel der Wahl?



- Anonyme Daten außerhalb des Geltungsbereichs der DS-GVO, aber
 - ggf. Zwecke mit anonymisierten Daten aus medizinischen Gründen nicht erreichbar, wenn Follow-Up-Daten zugeordnet werden müssen
 - Überprüfung bei Zertifizierung im beteiligten Haus eine Re-Identifikation erfordern
 - Notwendigkeit der Verknüpfungen von Datenbeständen erfordert Erhalt der Zuordnungsmöglichkeit / Identitätsmanagement

Weitere Herausforderungen durch die Datenschutzbrille

- Methodik der Pseudonymisierung und Anonymisierung
- Ausgestaltung des Identitätsmanagements und der Re-Identifikationsmöglichkeiten
- Anonymisierung und Pseudonymisierung sind Verarbeitungen im Sinne von Art. 4 Nr. 2 DS-GVO dar (Rechtsgrundlage erforderlich!)
- Arbeitshilfe zur Pseudonymisierung/Anonymisierung





Integrierter
Datenschutz



Herzlichen Dank für die Aufmerksamkeit!

Fragen oder Anregungen? – Bitte melden Sie sich gerne:
ds² Unternehmensberatung GmbH & Co. KG
Berliner Straße 1
49201 Dissen

Andrea Backer-Heuveldop: +49 (5421) 30 89 515
Andrea.heuveldop@ds-quadrat.de