vogel—partner
RECHTSANWÄLTE

Big Data und medizinische Forschung im Lichte der DSGVO

Datenschutz in der Medizin – Update 2018

Dr. Uwe K. Schneider

Wiesbaden, 22. März 2018

Dr. Uwe K. Schneider

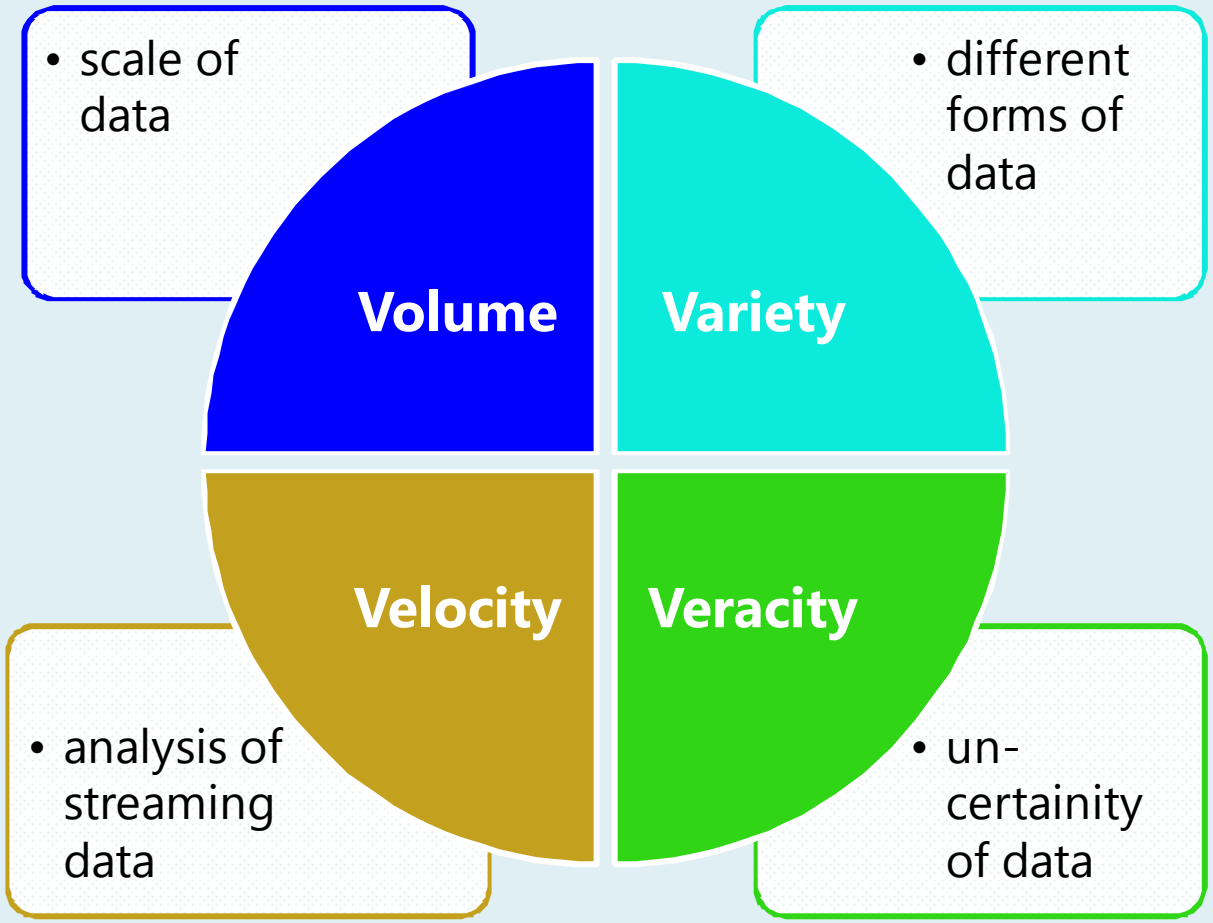
Rechtsanwalt
Fachanwalt für IT-Recht
Fachanwalt für Medizinrecht
Betrieblicher Datenschutzbeauftragter

Studium in Tübingen
Referendariat in Karlsruhe und Brüssel
Promotion an der Universität Tübingen zum Thema „Einrichtungsübergreifende elektronische Patientenakten“

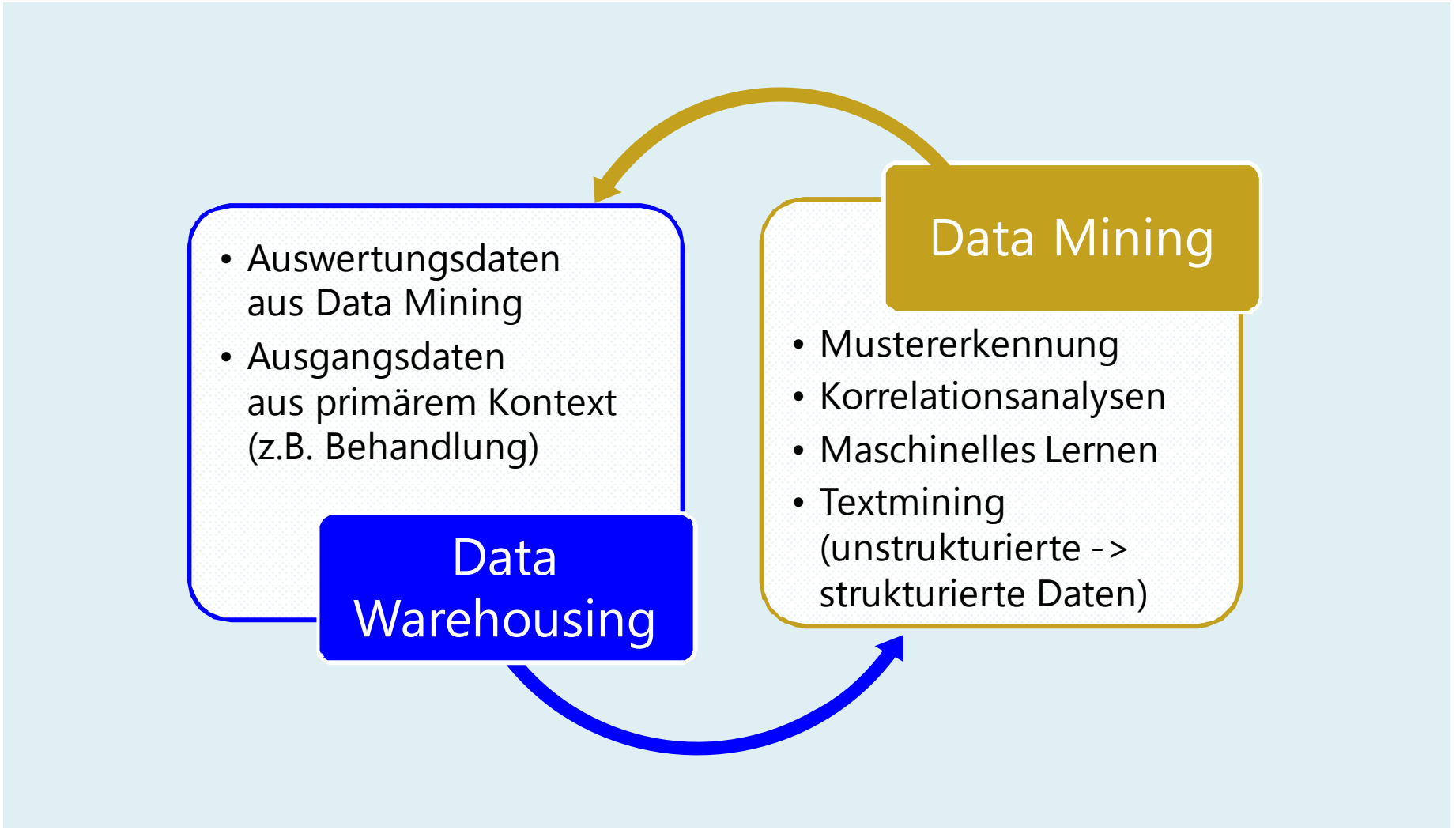
von 2007 bis 2011 Rechtsanwalt bei Bartsch und Partner in Karlsruhe

seit Juli 2011 Partner bei Vogel & Partner in Karlsruhe

Was ist Big Data?



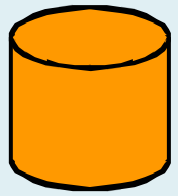
Wie verarbeitet man Big Data?



Was nutzt Big Data der medizinischen Forschung?

Bessere Fundierung bestehender Forschungsansätze

- mit mehr Daten (nicht nur Studien, auch aus Regelbehandlung)
- in Data Warehouse / medizinischem Register
- und effizienteren Auswertungsverfahren (Data Mining)



Generierung neuer Forschungsansätze

- automatisierte Generierung von Hypothesen
- basierend auf erkannten Mustern/Korrelationen durch Data Mining

⇒ **Chancen**

- für den Fortschritt der medizinische Forschung
- für neue Erkenntnisse über Krankheiten, Diagnostik und Therapie
- für den längerfristigen Verbesserung der medizinischen Versorgung

Welche Risiken birgt Big Data in der Medizin?

Richtigkeit der Daten bzw. Auswertungen?

- Korrelation ≠ Kausalität
- Wahrscheinlichkeit ≠ Wirklichkeit
- nur Indizien
- ersetzen keine kritische Auseinandersetzung durch Menschen

Schutz vor Belästigung & Benachteiligung durch Vertraulichkeit

- z.B. durch Krankenversicherungen oder Arbeitgeber bei Datenleck
  - Nichtabschluss / Kündigung von Verträgen
  - Zuschläge auf Prämien für (vermeintliche od. tatsächliche) Risiken
- aber auch durch Ärzte im Medizinbetrieb
  - die Patienten z.B. in eine *vorgefertigte Schublade* stecken
  - und *keine unbefangene Zweitmeinung* abgeben
  - bei *schlechten Deckungsbeiträgen* abblocken

… im Lichte der Datenschutz-Grundverordnung

Ziel	Einheitliches Datenschutzrecht in der gesamten Europäischen Union (EU) mit unmittelbarer Geltung
Nationales Recht	Sollte weitgehend ersetzt werden, z.B. deutsches BDSG
Umsetzung	Ab 25. Mai 2018 umzusetzen (2 Jahre nach Inkrafttreten) Gleichzeitig tritt neues BDSG in Kraft (Ausgestaltung/Abweichung/Ergänzung, wo erlaubt)
Durchsetzung	Empfindliche Bußgelder (bis 20 Mio. € od. 4 % Umsatz p.a.) Ausgeweitete Haftung

Grundsätze der Verarbeitung personenbez. Daten

Datenschutzgrundsätze nach Art. 5 I DSGVO:

a) **Rechtmäßigkeit** (Vorliegen einer Erlaubnisnorm);
Verarbeitung nach Treu und Glauben;
Transparenz ▸ Art. 12 ff. Informationspflichten, Rechte des Betroffenen.

b) zu festgelegten Zwecken („**Zweckbindung**“)

c) nur soweit für diese Zwecke erforderlich („Datenminimierung“)

d) sachlich richtig

e) nur so lange (zeitlich) erforderlich („Speicherbegrenzung“)

f) mit **angemessenen Schutzmaßnahmen**
(„Integrität und Vertraulichkeit“) ▸ Art. 32, z.B. Pseudonymisierung

⇒ **Grundprinzipen des bisherigen Datenschutzrechts bleiben erhalten.**

Big Data vs. Zweckbindung

Daten aus der medizinischen Behandlung (Gesundheitsdaten)

- Erhebung u. Verwendung zum primärem Zweck der Behandlung
- im Kontext des Vertrauensverhältnisses zwischen Arzt und Patient

Big Data bzw. Sekundärnutzung zu Forschungszwecken

- Daten aus Vielzahl von Behandlungen werden ausgewertet
- zur Generierung u. Überprüfung von Hypothesen durch Forscher
- letztlich zur Erarbeitung neuer, besser Behandlungsstandards

Zweckänderung bedarf i.d.R. der Rechtfertigung

- v.a. bei Gesundheitsdaten, da neuer Kontext ≠ individuelle Behandlung
- Bestimmtheit auch des neuen (Forschungs-)Zwecks

↯ automatisierte Suche nach unbekannten Zusammenhängen

⇒ **Kein Big Data erlaubt?**

Lockerung der Zweckbindung (Art. 5 Abs. 1 lit. b)

- Grds. Erhebung nur für **festgelegte, eindeutige und legitime Zwecke**
- Weiterverarbeitung nicht in einer damit nicht vereinbaren Weise
- **wissenschaftliche Forschung i. R. v. Art. 89 Abs. 1 gilt als vereinbar**

⇒ Erlaubnistatbestand für die Primärnutzung (Behandlung) könnte auch für Sekundärnutzung (Forschung) genügen, wenn die Voraussetzungen des Art. 89 eingehalten werden (i.W. geeignete Garantien wie Pseudonymisierung).

- Ist aber **strittig**, gerade bei Gesundheitsdaten.
- Würde außerdem nur bei Sekundärnutzung helfen, nicht bei primär zu Forschungszwecken erhobenen Daten.

Lockerung der Zweckbindung (Art. 6 Abs. 4)

Prüfung der Vereinbarkeit des sekundären mit dem primären Zweck berücksichtigt darüber hinaus u.a. (Art. 6 Abs. 4 DSGVO)

- jede Verbindung der Zwecke
- Erhebungszusammenhang
- Art. der personenbezogenen Daten,
  insbes. ob besondere Kategorien nach Art. 9 DSGVO verarbeitet werden

⇒ höhere Anforderungen an Vereinbarkeit bei Gesundheitsdaten

- mögliche Folgen der beabsichtigen Weiterverarbeitung
- Vorhandensein geeigneter Garantien wie Pseudonymisierung

⇒ mit Pseudonymisierung liegt eher Vereinbarkeit vor

wenn (primäre) Verarbeitung nicht auf Einwilligung oder Rechtsvorschriften nach Art. 23 Abs. 1 DSGVO (wie nationale Sicherheit) beruht.

Öffnungsklausel für Mitgliedstaaten (Art. 9 Abs. 4)

Für die Verarbeitung von biometrischen, genetischen und **Gesundheitsdaten**:

- Mitgliedstaaten dürfen **abweichende Regeln erlassen oder beibehalten**
- entsprechend der innerstaatlichen Kompetenzverteilung

⇒ für Kliniken v.a. die Bundesländer (LKHG): strenger Erlaubnisvorbehalt

⇒ im Übrigen (niedergelassene Ärzte, sonstige Gesundheitsdienstleiter, Pharmaindustrie) der Bund (BDSG-neu, SGB V, GenDG, …)

Die BRD (der Bund) fordert **zusätzliche Rechtsgrundlage für sekundären Zweck** (§ 23 Abs. 2, § 24 Abs. 2 **BDSG-neu**) bei besonderen Datenkategorien.

Die **Bundesländer** behalten derzeit noch ihre **bisherigen Regeln** bei (LKHG), die **in der Regel in ähnlicher Weise** eine zusätzliche Rechtsgrundlage fordern (mit Ausnahmen z.T. für die interne Eigenforschung in der Klinik).

Nationale Ausgestaltung der Öffnungsklausel

Auf Bundesebene

- Bundesdatenschutzgesetz (**BDSG-neu**): z.B. für Pharmaindustrie
- Sozialgesetzbuch (**SGB V**): Kassen, KVen, z.T. Leistungserbringer in der GKV
- Sonderregeln für bestimmte Patientendaten: **GenDG**, AMG, KFRG
- Schweigepflicht (**§ 203 StGB**): Offenbaren von Patientengeheimnissen

Auf Landesebene

- i.Ü. Gesetzgebungskompetenz bei den Ländern
- v. a. Datenschutz im Krankenhaus – Landeskrankenhausgesetze (**LKHG**)

Öffnungsklauseln für kirchliche Krankenhäuser

- in Landeskrankenhausgesetzen (LKHG) mancher Bundesländer
- dann für die interne Datenverarbeitung ggf. vorhandene kirchliche Regeln

Konsequenzen

- Die Vielzahl von Regelungen in Bund und Ländern, die die Bestimmung der jeweils gültigen Regeln erschweren, **bleiben bestehen**.

Verarbeitung ohne Einwilligung: § 27 BDSG-neu

Verarbeitung besonderer Kategorien personenbezogener Daten ist zulässig,

- für wissenschaftliche Forschungszwecke und statistische Zwecke
- wenn dies für diese Zwecke erforderlich ist und
- wenn die Interessen des Verantwortlichen an der Verarbeitung
- die Interessen der betroffenen Person an einem Ausschluss
- erheblich überwiegen (Abs. 1 S. 1).

⇒ *Keine einfache Interessenabwägung, Gründe & Ergebnis dokumentieren!*

Angemessene technische und organisatorische Schutzmaßnahmen (S. 2)

Betroffenenrechte auf Auskunft etc. z.T. eingeschränkt (Abs. 2)

Besondere Schutzmaßnahmen (Abs. 3)

- Anonymisierung soweit und so bald wie möglich (S. 1)
- In jedem Fall: umgehende Pseudonymisierung (S. 2, 3)

Forschung nach den LKHG (z.T. in Überarbeitung)

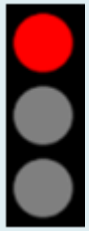
Forschung ohne Einwilligung:

intern zulässig / extern zulässig
zumindest wenn:

- pseudonymisiert
- Vorhabenbezug konkretisiert
- ggf. Interessensabwägung

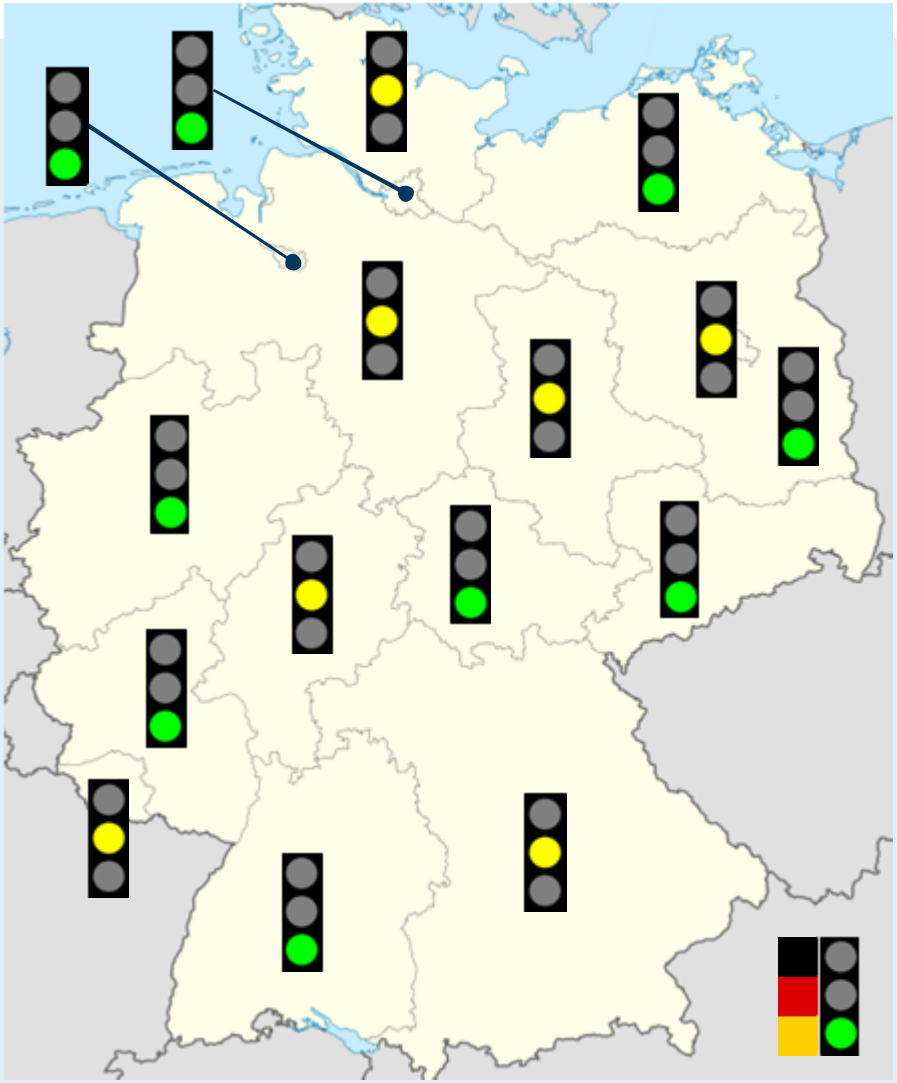
Einschränkungen extern, z.B.:

- Weitergabe nur an bestimmte Personengruppe
- nur Fernzugriff
- Fachabteilungsgrenze



intern und extern
starke Einschränkungen

Forschung nach den LKHG (z.T. in Überarbeitung)



Big Data, Zweckbindung & Einwilligung

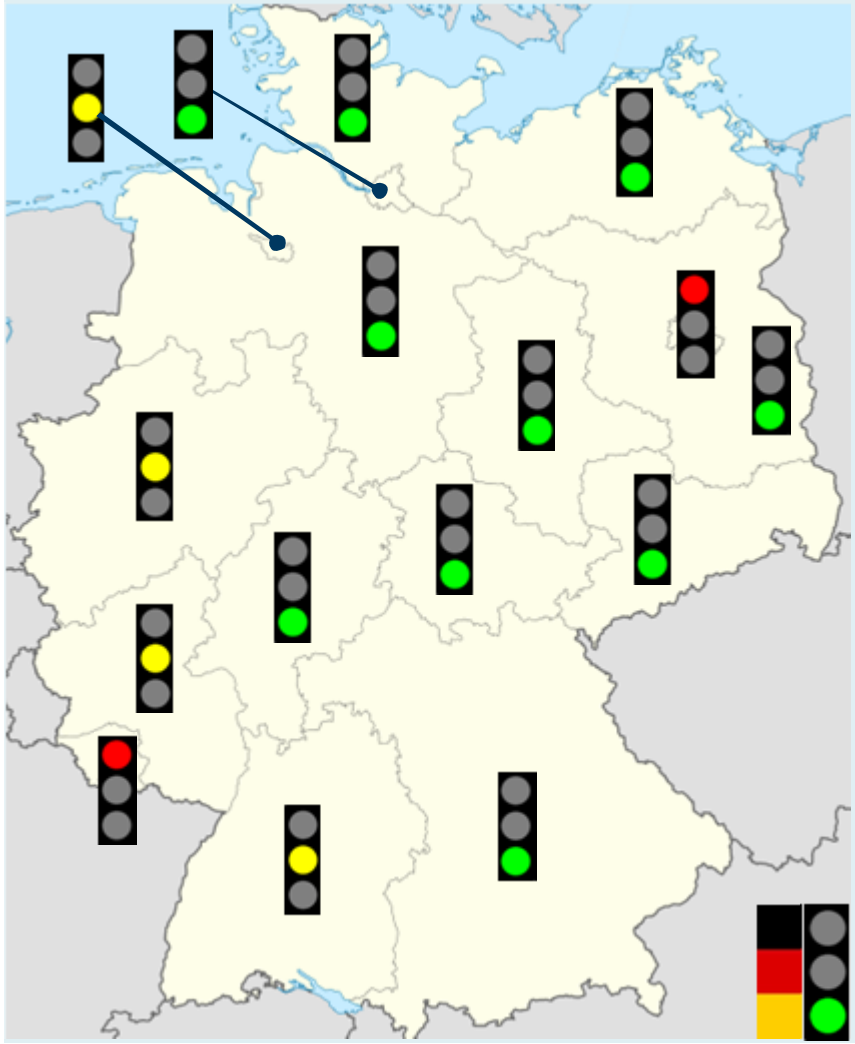
Allgemeine Anforderungen an eine Einwilligung (DSGVO/BDSG)

- Freiwilligkeit: kein Zwang, keine Koppelung an (Notfall-)Behandlung
- Informiertheit: Aufklärung („informed consent")
- Bestimmtheit: keine Generalermächtigungen
- Angemessenheit: bei Formulareinwilligungen (AGB-Kontrolle)
- Widerruflichkeit: mit Wirkung für die Zukunft
  (Ausnahme: klinische Studien nach AMG/Clinical Trials Regulation)

Zusätzlich in einigen Bundesländern

- nicht in allgemeinen Aufnahmebestimmungen (§ 50 LKHG BW)
- im Einzelfall (BW, HB, MV <nicht bei Forschung>, NW, SL):
  Konkretisierung Verarbeitungsbedarf/Datenumfang
- Vorhabensbezug bei Forschungsvorhaben:
  Bremen (schwach), RP (für Privilegierung interne DV), Saarland (streng)
- Pseudonymisierung nur in Verantwortung der Klinik:
  Berlin (§ 25 Abs. 1, 2 LKHG Berlin)

Big Data, Zweckbindung & Einwilligung



Normal
- allgemeine Anforderungen
- ähnlich wie BDSG
- u.a. Bestimmtheit

Mittel
- erhöhte Anforderungen
- „im Einzelfall“
- nur für (mehr oder weniger bestimmtes) „Forschungsvorhaben“

Streng
- Berlin: keine Pseudonymisierung durch unabh. Datentreuhänder
- Saarland: „im Einzelfall“ und Übermittlung nur für „bestimmtes Forschungsvorhaben“

Big Data, Zweckbindung & Einwilligung

Zwei Lösungsmöglichkeiten spezifisch für die Einwilligung in Big Data:

„dynamic consent“

- Erste Einwilligung für Einspeicherung in Datenbank
- Neue Einwilligung, wenn Auswertungs-Vorhaben konkretisiert
- sicherer, jedenfalls wenn in LKHG Einzelfallbezug o.Ä. gefordert

„broad consent“

- Einwilligung des Betroffenen mit Mindestmaß an Bestimmtheit
  - **je weiter die Zwecke**
    (z.B. allgemein Versorgungsforschung im Gesundheitswesen)
  - **desto konkreter die Daten**
    (welche auf Vorrat gesammelt werden)
- Data Access Boards entscheiden über Freigabe für konkrete Projekte

Big Data, Zweckbindung & Einwilligung

„broad consent“

- auf Basis der DSGVO und BDSG-neu **grundsätzlich zulässig**
- Argument aus Erwägungsgrund 33 der DSGVO:

*(33) **Oftmals kann der Zweck** der Verarbeitung personenbezogener Daten für Zwecke **der wissenschaftlichen Forschung zum Zeitpunkt der Erhebung** der personenbezogenen Daten **nicht vollständig angegeben** werden. Daher sollte es **betroffenen Personen erlaubt** sein, ihre **Einwilligung für bestimmte Bereiche wissenschaftlicher Forschung** zu geben, wenn dies unter Einhaltung der anerkannten **ethischen Standards der wissenschaftlichen Forschung** geschieht. Die betroffenen Personen sollten Gelegenheit erhalten, ihre Einwilligung nur für bestimme Forschungsbereiche oder Teile von Forschungsprojekten in dem vom verfolgten Zweck zugelassenen Maße zu erteilen.*

Big Data, Zweckbindung & Einwilligung

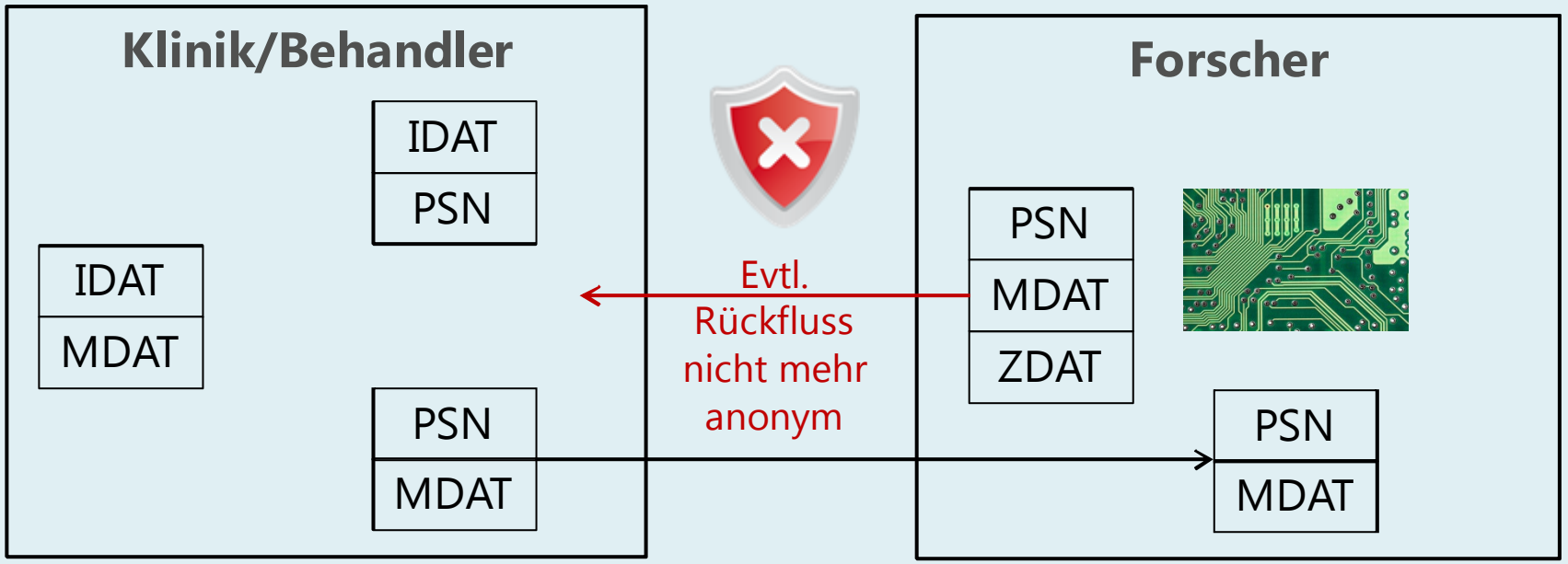
Außerdem: **Gesetzgeber hat das Problem und die Bedeutung von Big Data** insbesondere auch **im medizinischen Bereich erkannt**:

ErwG 157: *„Durch die **Verknüpfung von Informationen** aus Registern können Forscher neue Erkenntnisse von **großem Wert in Bezug auf weit verbreiteten Krankheiten** wie Herz-Kreislauferkrankungen, Krebs und Depression erhalten. Durch die Verwendung von Registern können **bessere Forschungsergebnisse** erzielt werden, da sie auf einen größeren Bevölkerungsanteil gestützt sind."*

- Auch das spricht für die **Zulässigkeit von „broad consent",** um den wohl gewollten Aufbau von Medizindatenbanken zu ermöglichen.

- In **einigen Bundesländern**, wenn und soweit restriktive Regeln in **LKHG** im Rahmen der Öffnungsklausel (Art. 9 IV DSGVO) beibehalten (status quo), aber **nicht gänzlich rechtssicher**.

Big Data & Anonymisierung



IDAT	Patienten-identifizierende Daten
MDAT	Medizinische Daten
PSN	Pseudonym des Patienten

ZDAT	Zusatzdaten Verarbeitungsergebnisse

<u>Relativer Ansatz d. Personenbezuges:</u>
⇒ für Forscher (Klinik-extern) anonym
⇒ keine Datenübermittlung
wenn vertragl. Verbot Identifizierung, …

Big Data & Anonymisierung

Anonymisierung vor Big Data-Aggregation/Sekundärnutzung

- Zuordnung zu bestimmter / bestimmbarer natürlicher Person (Patient)
- nicht mehr möglich (**absolute Anonymisierung**) oder
- nicht mehr mit verhältnismäßigem Aufwand (**faktische/relative Anonymisierung**)
- für anonyme Daten / Anonymisierung (*strittig*) greift kein Erlaubnisvorbehalt

Pseudonymisierung (u.U. mehrfach) vor externer Big Data-Sekundärnutzung

- **Ersetzung** der **Identifikatoren** (Name etc.) durch **Pseudonym**
- um Bestimmung des Betroffenen auszuschließen oder zu erschweren
- Weitergabe Daten ohne die Zuordnung: kein Übermitteln v. Patientendaten
- Annahme: **Relativität des Personenbezuges** (*strittig*) => für Empf. faktisch anonym

Empfehlungen zur Risikovorsorge bzw. vorsorgende Datenschutzpflichten

- Rest-Risiken der Reidentifizierung bei nur faktischer Anonymität
- Maßnahmen der **Datensicherheit**
- **Vereinbarungen** mit Datenempfängern (z.B. „Data Transfer Agreement – DTA“): v.a. Datensicherheit & **Verbot der Reidentifizierung**

Big Data & Anonymisierung

Big Data gefährdet aber die Anonymität:

- Verwendung großer Datenmengen erhöhen das Risiko, dass **Daten durch Verknüpfung „re-identifiziert"** werden können, jedenfalls soweit als Einzelangaben erhalten (Patienten-individuell, wenn auch nicht direkt Patienten-identifizierend) und nicht lediglich Merkmalsausprägungen kumuliert (mit Mittelwert, Standardabweichung)
- Auch ist die **technologische Entwicklung zu berücksichtigen** (z.B. Steigerung Prozessorleistung für Re-Identifizierung durch Mustervergleich); nach ErwG 25 ist immer der zum Zeitpunkt der Verarbeitung technologische Stand maßgeblich => dynamische Betrachtung erforderlich!

⇒ Absolute Sicherheit ist daher auch über eine faktische Anonymisierung kaum zu erhalten. Jedenfalls zusätzliche Sicherheitsvorkehrungen (Zugriffskontrolle)!

Grundlegende Handlungsempfehlungen

1. **Klärung des anwendbaren Rechts**
- Abhängig von Art (Klinik, Pharma) und teils Sitz (Bundesland) des Forschers
- Art der Patientendaten und Zweck der Verarbeitung
- Hilfestellung für Forschung durch Kliniken: http://irene.tmf-ev.de/homeirene

2. **Prüfung der rechtlichen Zulässigkeit**
- Ausreichende Rechtsvorschrift vorhanden oder
- wirksam die Einwilligung des Patienten eingeholt
- oder hinreichende Anonymisierung durchgeführt

3. **Gewährleistung der Datensicherheit**
- technische und organisatorische Maßnahmen
- in jedem Fall Pseudonymisierung und Zugriffskontrolle
- Zugriffskontrolle selbst bei (nur faktischer) Anonymisierung angezeigt

Hilfreich (v.a. TOMs): TMF-Leitfaden, vgl. https://www.tmf-ev.de/Produkte/Mustertexte_DSKonzepte2.aspx

vogel—partner
RECHTSANWÄLTE

Fragen & Diskussion

Vogel & Partner Rechtsanwälte mbB
Technologiepark Karlsruhe
Emmy-Noether-Straße 17
76131 Karlsruhe

www.vogel-partner.eu
us@vogel-partner.eu
Tel. +49 721 782027-0
Fax +49 721 782027-27