

Analyse, Katalogisierung und Nutzung genetischer Daten aus Sicht des Datenschutzes

Thilo Weichert, Leiter des ULD
TMF-Workshop 19.03.2014, Essen:
Datenbank genomischer Varianten für die klinische Anwendung und die medizinische Forschung

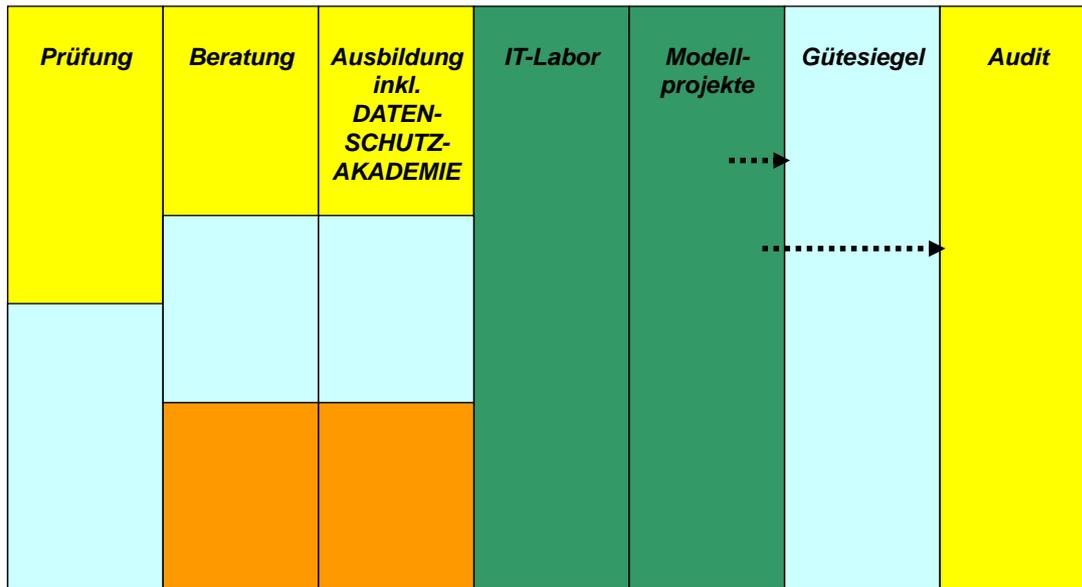


www.datenschutzzentrum.de

Inhalt

- Unabhängiges Landeszentrum für Datenschutz - ULD
- Rechtliche Grundlagen
- Besonderheit genetischer Daten
- Potenzielle Nutzende
- Risiken für die Spender
- Spezielle Probleme
 - Selbstbestimmung
 - Sichere Pseudonymisierung
 - Datensparsamkeit
 - Kontrolle
- Regulierung

Datenschutz und Informationsfreiheit



Primäre Adressaten:
 Öffentl. Verwaltungen
 Unternehmen
 Bürger, Kunden, Patienten
 Wirtschaft, Wissenschaft, Verwaltung

Verfassungsrechtliche Grundlagen

- Schutz von **Leben und körperlicher Unversehrtheit** (Art. 1 II 1 GG, Art. 3 EUGRCh)
 - freie Einwilligung u. vorherige Aufklärung
 - Verbot der eugenischen Selektion
- Allgemeines Persönlichkeitsrecht (Art. 2 I iVm 1 I GG)
 - Grundrecht auf Datenschutz** (Art. 8 EUGRCh)
 - Zweckbindung, Auskunft und Nichtwissen
- **Forschungsfreiheit** (Art. 5 III 1 GG Art. 13 1 EUGRCh)
- Schutz der **Berufsfreiheit** von Arzt und Forschenden (Art. 12 GG, Art. 15 EUGRCh)
- **Diskriminierungsverbot** (Art. 3 III GG, 21 I EUGRCh) auch bzgl. genetischer Merkmale
- Gesundheitsschutz (Art. 35 EUGRCh)

Nationalrechtliche Grundlagen

- Gendiagnostikgesetz (GenDG – 2009)
- Bundesdatenschutzgesetz (BDSG, evtl. LDSG), subsidiär Europäische Datenschutz-Richtlinie, künftig Europäische Datenschutz-Grundverordnung
- Berufsrecht und § 203 StGB
- Medizinrecht (TransplantationsG, TransfusionsG, ArzneimittelG, SGB V, KrebsregisterGe, KrankenhausR)

Besonderheit genetischer Daten

- = unveränderbare genetische Disposition für biologische u. seelische Merkmale (incl. Krankheit, zumeist nur Wahrscheinlichkeit)
- = eindeutiger biologischer Identifikator (faktische Nichtanonymisierbarkeit)
- = Ähnlichkeit zu biologischen Verwandten
- = Aussagekraft f. ethnische Zugehörigkeit mit Diskriminierungsrisiko
- > Besondere Art pers.bez. Daten (Gesundheit, §§ 3 IX, 28 VI-IX BDSG)
- > Schutz durch berufliche Schweigepflicht
- > Schutz durch bereichsspezifische Regelungen (z. B. GenDG)

Potenzielle Nutzende

- Medizinische Diagnostik und Therapie (incl. Register)
- Medizinische und sonstige Forschung (incl. Register)
- Behörden (Polizei, Strafverfolgung, Ausländerb., Ziel insbes. Identifizierung u. Abstammungsklä rung)
- Versicherungen (Risikobewertung zu Krankheit und Lebenserwartung)
- Arbeitgeber (langfristige Produktivität)
- Konsumwirtschaft (Lifestyle-Industrie, Google & Co.)

Risiken für die Spender

- Unfreiwillige Spende, heimliche Auswertung und Nutzung
- Belastung mit unerwünschtem Wissen
- Reidentifizierung und zweckwidrige Nutzung
- Faktische Nichtdurchsetzbarkeit von Betroffenenrechten (Auskunft, Interpretation, Widerspruch, Löschung)

Spezielles Problem: Selbstbestimmung

- Fehlen der Einwilligungsfähigkeit (Kinder, Nichterreichbarkeit, Nichtansprechbarkeit, geistige Behinderung)
- Komplexität der Information (rechtlich, technisch, faktische individuelle Folgen)
- Konkretheit der Information (Art der Daten/Merkmale, Zwecke, verarbeitende Stellen)
- Freiwilligkeit der Entscheidung (ökonom., soziale od. medizinische Abhängigkeit)
- Komplexität der Wahlmöglichkeiten
- Technisch-organisatorische Umsetzung der (selbstbestimmten) Optionen

Spezielles Problem: sichere Pseudonymisierung

Reidentifizierungsrisiken durch

- Identifikationsdaten (Zuordnungstabelle, Entschlüsselung)
- Externes Zusatzwissen (je detaillierter und umfangreicher der Datensatz desto einfacher)
- Verknüpfung mit identifiziertem DNA-Sample

Erstellung separater Pseudonyme für

- Erhebung, - (langfristige) Speicherung, - Herausgabe/Auswertung/Nutzung
- Pseudonym-Trennung zwischen Proben- und Datenmaterial (technisch-organisatorisch-rechtlich)
- Kontrollierte Datentreuhänderschaft/Pseudonymverwaltung

Spezielles Problem: Datensparsamkeit

- Frühestmögliche Anonymisierung/Pseudonymisierung
- Frühestmögliche Löschung
- Weitestgehende Nichtverkettbarkeit

Vielfältige Nutzungszwecke (insbes. Kombi Behandlung, Qualitätssicherung, Forschung) verhindern Datensparsamkeit

> Technisch-organisatorisch-rechtliche Trennung nach Zwecken und Verarbeitern

Spezielles Problem: Datensicherung

Technisch-organisatorische Schutzziele:

- **Vertraulichkeit** (z.B. Verschlüsselung)
- **Integrität**, Authentizität (Backup, digitale Signatur)
- **Verfügbarkeit** (ausfallsichere Stromversorgung, Datenmanagement)
- **Intervenierbarkeit** (Löschen, Sperren, Beauskunften)
- **Unverknüpfbarkeit** (Abschottung)
- **Transparenz**, Revisionsfähigkeit (Protokollierung, Kontrolle der SysAdmin, Dokumentation, Anwenderhandbücher, Information bei Erhebung, Benachrichtigung bei Bearbeitung)
- Zugriffe nach Rollenkonzepten
- Dokumentation und Auswertung der Prozess-Protokolle
- Gewährleistung der zuverlässigen Rechtsnachfolge oder Löschung bei Auflösung

Spezielles Problem: Kontrolle

Gesellschaftliche Kontrolle:

- Transparenz des Verfahrens (Biobankregister, Studienregister, Policies, Verfahrensbeschreibungen, Hinweise und Formulare, Jahresberichte)
- Genehmigung, Zertifizierung/Audit, Begleitung und aufsichtliche Kontrolle durch Ethik-Kommissionen, Datenschutzbeauftragte, wiss. Gremien, Parlamente

Individuelle Kontrolle und Rückmeldung durch Betroffenenrechte (soweit Pseudonym noch identifizierbar)

Regulierung

- Gesetzliche Normierung (z. B. Krebsregistrierung)
- (regulierte) Selbstregulierung (Standard Operation Procedures, Best Practices, Verhaltensregeln/Codes of Conduct, freiwillige Audits)

Quelle: ULD, Datenschutzrechtliches Gutachten – Datentreuhänderschaft in der Biobankforschung – Methoden, Kriterien und Handlungsempfehlungen für die datenschutzrechtliche Auditierung der Datentreuhänderschaft in der Biobank-Forschung, Teilprojekt 2, Schlussbericht, Kiel 30. April 2009

Analyse, Katalogisierung und Nutzung genetischer Daten aus Sicht des Datenschutzes

Dr. Thilo Weichert

Unabhängiges Landeszentrum für Datenschutz Schleswig-
Holstein (ULD)

Holstenstr. 98, D- 24103 Kiel

mail@datenschutzzentrum.de

<https://www.datenschutzzentrum.de>