Nutzungsbedingungen

Interoperabilität

Datenminierung

Data Trust/Sicherheit

Technische Bausteine

Datenbankystem

Datenübergabe Schnittstelle

Metadaten und Datenformat

Datenminimierung

Authentifizierung

Autorisierung

Protokollierungs-aspekte

Daten-verschlüsselung

Zertifizierung

offene Daten

kaine

Abstufungen beim Akzeptieren der Nutzungsbedingungen:
- nur Häkchen setzen
- Häkchen setzen mit Angabe der Email-Adresse
- Häkchen mit weitergehender Authentifizierung (Positionen etc.)

offene Daten mit Lizenz

geteilte Rohdaten Daten beim Nutzer (Identitätskontrolle)

Prüfung nur der Vertrauenswürdigkeit des Nutzers:
- es gibt Vorgaben zur Nutzung
- aber überprüft wird nur, ob Nutzer vertrauenswürdig ist bzw. berechtigtes Interesse hat (z.B. Forschermen bei den FDZ oder "berechtigtes Interesse" beim Grundbuchamt)
- Prüfung als Angabe der Rolle bzw. Interesse richtig ist (ggf. nur stichprobenhaft)

geteilte Rohdaten Daten beim Nutzer (Nutzungskontrolle)

Prüfung der Nutzung der Daten bei Nutzer (zumindest Stichproben)
- es gibt Vorgaben zur Nutzung
- überprüft wird außerdem, ob Nutzer vertrauenswürdig ist bzw. berechtigtes Interesse hat
- darüber hinaus wird die Nutzung des Nutzers geprüft (zumindest stichprobenhaft)

geteilte Rohdaten Fernzugriff des Nutzers beim Datengeber

geteilte Rohdaten Fernzugriff des Nutzers beim DIT

ACHTUNG Modell
geteilte Rohdaten mit Vorort-Zugriff nur beim Datengeber
nicht separat mit technischen Bausteinen belegt

Daten bleiben bei Datengeber bzw. Datenverwahrender. Nutzer darf aber über Fernzugriff darauf zugreifen
- es gibt dieselben Vorgaben zur Nutzung (z.B. nur beschränkter Zugriff wie etwa nur auf Metadaten)
- überprüft wird außerdem, ob Nutzer vertrauenswürdig ist bzw. berechtigtes Interesse

geteilte Analysedaten

ACHTUNG Modelle
geteilte Analysergebnisse via Dateninhaber und Intermediär
zusammengefasst

Daten bleiben bei Datengeber. Und nur die Analysergebnisse werden mit dem Nutzer geteilt
- für den Datengeber die sicherste Variante
- aber Datennutzer verträt an Datengeber seine Fragen und damit evtl. Geschäftsgeheimnisse

Technische Bausteine

Standard relationale Datenbank — MySQL, PostgreSQL
Standard NoSQL-Datenbank — MongoDB
Standard Graphendatenbank — Neo4j, GraphDB
Standard Zeitreihendatenbank — InfluxDB, Timescale DB

Datenübergabe Schnittstelle

Domänenstandard Richtlinien und Protokolle — Gesundheit: FHIR; IoT: Web of Things (z.B. WOT/JSON-LD)
Generell Standard der Technik
Datei basierte Übertragung (Daten Portal)
RESTful API (Beschreibung durch OpenAPI bzw. Swagger Specification) — GraphQL (Alternative zu RESTful API)
Solid API (Standardisiert durch Solid Protokoll)
API-Beschränkungen Rate limiting — express-rate-limit
Übertragung der Algorithmen — Standard Methode zur Containerisation — Container Registry

Metadaten und Datenformat

Domänenstandard Richtlinien und Protokolle — Gesundheit: FHIR; Forstwirtschaft: ElanFunDiNa
Standard Daten Format — JSON Daten JSON Schema, Python: Pydantic — XML Daten XML Schema
Standard Metadaten und Katalog — Dublin Core Metadata Initiative, METS, Data Catalog Vocabulary — Vokabular schema.org, Domain Ontologie

Datenminimierung

Standard Pseudonymisierung — python packages, MySQL User-Defined Functions
Standard Anonymisierung — PostgreSQL Anonymizer, python: faker, Microsoft Presidio, ARX, UT Dallas Toolbox — Domänenstandard DICAT, DiscomAnonymis, MS Tools for Health Data Anonymization
Treuhandstelle Tools Uni-Greifswald
Individuell

Authentifizierung

Standard Autorisierungsverfahren Level 2 — Oauth 2.0, WT
Standard - Level 1 Einfache Identitätsüberprüfung — Email Registrierung, Time-based One-Time Password, Ad-hoc Entwicklung
Standard - Level 2 IAM System — SAML, OpenID Connect, LDAP, CAS, ADFS — existierende IAM Software Keycloak, Gluu, Zuverlässige Identity Provider — IAM as a Service

Autorisierung

Standard grundlegende Autorisierung — Oauth 2.0, WT
Individuell Digital Rights Management — z.B. OpenDB OpenPGP, Polkrypt, OpenABE, Adobe LiveCycle Rights
Standard feingranulare Zugriffskontrolle — Sevice Security (RBAC), XACML (ABAC), Open Policy Agent (PBAC)
Standard Wasserzeichen, Fingerprinting — Digital Watermarking watermarks
Standard Maßnahmen des Web-Apps — disable-devtool

Protokollierungs-aspekte

Standard API Logging — Logging Bibliotheken
Standard Integrierte Funktionen — python sanet, Bibliothek
Standard Logging Layer — Rsyslog, Graylog, Zeitlog-log, ODBC
Loggringe der Datennutzenden — Zertifizierter Zeitstempel

Daten-verschlüsselung

Standard verschlüsselte Datenübertragung — TLS/SSL (Datenübertragung, web traffic, email)
SSH (remote access, command execution, and file transfers)
Verschlüsselter Tunnel für Datenübertragung — IPsec (Virtual Private Networks)
Standard Homomorphe Verschlüsselung — Paillier, BGV und CKKS

Zertifizierung

Zertifikat für Verschlüsselung — SSL/TSL
Zertifikat für Zugriffskontrolle — SAML Zertifikat, OAuth 2.0 und OpenID Connect Zertifikate
Standard Datenintegrität — Code Signing-Zertifikat