Datentreuhand Kompetenz Netzwerk DaTNet

Privacy by Design – Vergleich von Data Stewards und Data Exchanges

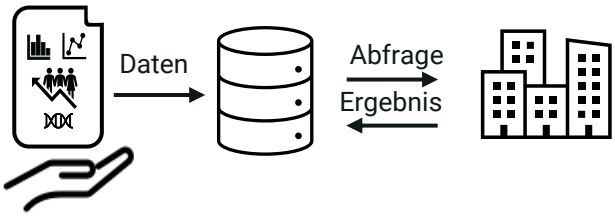
Kategorien: **Architekturen:** **Privacy by Design**

Dr. Lisa Eggerichs (wiss.MA, DaTNet, TU Dresden)

Privacy by Design ist ein architektonisches Prinzip, das darauf abzielt, die Lücke zwischen datenschutzrechtlichen und ethischen Anforderungen an IT-Systeme und der praktischen Umsetzung in der Softwareentwicklung zu schließen (Hoepman 2014). Datenschutzaspekte müssen daher von Anfang an – also bereits in den frühen Phasen der Systementwicklung – berücksichtigt werden. Zur technischen Umsetzung von Privacy by Design formuliert Hoepman (2014) vier grundlegende Strategien. Diese dienen als Bewertungsrahmen, um die Datenschutzkonformität verschiedener Modelle *Data Steward* und *Data Exchange* –zu analysieren.

Data Steward

Abb. Schematische nach Gehring & Tschorsch (2014)



Datenquellen schicken ihre Daten an den Steward, der diese speichert und API-Endpunkte zu Verfügung stellt, über die die Daten abgefragt werden können. Der Data Steward verarbeitet die Anfrage.

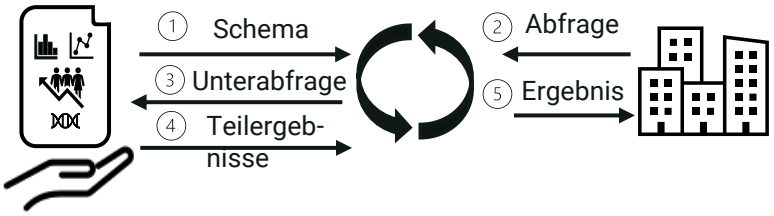
Datenempfänger (Datennutzende) fragen die Daten ab und erhalten diese vom Data Steward.

Data Trustee Models:

Aus einer technischen kann zwischen Data Steward und Data Exchange unterschieden werden.

Data Exchange

Abb. Schematische nach Gehring & Tschorsch (2014)



Die zentrale Einheit empfängt das Schema, das von der Datenquelle bereit gestellt wird (Schritt1).

Data Exchange bieten Schnittstellen an und ermöglicht es Empfängern, Informationen abzufragen und Ergebnisse zu erhalten (Schritt 2-4). Data Exchange speichert keine Daten, sondern generiert nach Erhalt der Anfrage Unterabfragen für jede Datenquelle und stellt Teilergebnisse zusammen, um die vollständige Abfrage zu beantworten (Schritt 3, 4).

Datenorientierten (data-oriented) Strategien nach Hoepman (2014), um personenbezogene Daten zu verarbeiten:
MINIMIZE: Die Menge sollte auf das geringstmöglichtste Maß beschränkt werden.
HIDE: Daten und ihre Beziehungen untereinander sollten verborgen bleiben.
SEPARATE: In getrennten Abteilungen verarbeitet werden
AGGREGATE: Verarbeitung auf der höchsten Aggregationsstufe mit der geringsten Detailtiefe verarbeiten.

Vergleich von Data Stewards und Data Exchange hinsichtlich der datenschutzkonformen Verarbeitung (Gehring & Tschorsch 2014)
Data Exchange ist dem Modell des Data Stewards hinsichtlich der datenschutzkonformen Verarbeitung von personenbezogenen Daten vorzuziehen ist. Die Strategien HIDE, MINiMIZE und AGGREGATE sind mit beiden Modellen umzusetzen. Jedoch bietet das Data Exchange Modell eine deutlich bessere Umsetzung der SEPARATE Strategie, da hier die Daten nicht zentralisiert gespeichert werden, sondern über ein verteiltes Protokoll erfolgen kann.

Literatur

Gehring, Lukas, and Florian Tschorsch. 2015. *PrivTru: A Privacy-by-Design Data Trustee Minimizing Information Leakage*. https://easychair.org/publications/preprint/KCVd.

Hoepman, Jaap-Henk. 2014. "Privacy Design Strategies." In *29th IFIP International Information Security Conference (SEC)*, edited by [Editor if known], 446. Vol. AICT-428. Springer, June 2, 2014.

Gefördert durch: Bundesministerium für Forschung, Technologie und Raumfahrt
Finanziert von der Europäischen Union NextGenerationEU
TECHNISCHE UNIVERSITÄT DARMSTADT
TECHNISCHE UNIVERSITÄT DRESDEN
RWTH AACHEN UNIVERSITY
Universität Marburg