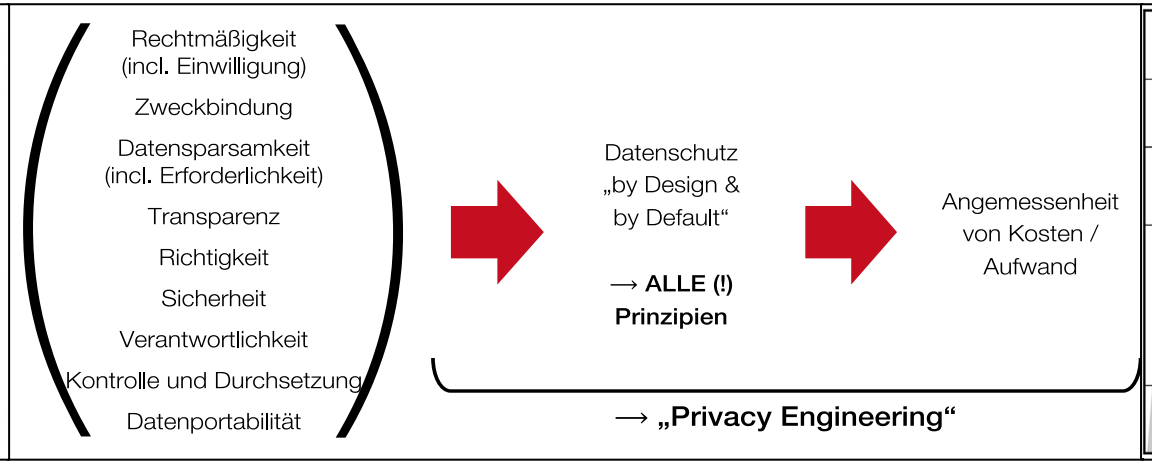
Information Governance
Tutorium 09: Datenschutz 2 – Privacy Engineering



Privacy stages	identifiability	Approach to privacy protection	Linkability of data to personal identifiers	System Characteristics
0	identified	privacy by policy (notice and choice)	linked	• unique identifiers across databases • contact information stored with profile information
1			linkable with reasonable & automatable effort	• no unique identifies across databases • common attributes across databases • contact information stored separately from profile or transaction information
2	pseudonymous	privacy by architecture	not linkable with reasonable effort	• no unique identifiers across databases • no common attributes across databases • random identifiers • contact information stored separately from profile or transaction information • collection of long term person characteristics on a low level of granularity • technically enforced deletion of profile details at regular intervals
3	anonymous		unlinkable	• no collection of contact information • no collection of long term person characteristics • *k*-anonymity with large value of *k*

Recall: Corona-Gästelisten in Restaurants

Name, Vorname

Vollständige Anschrift

Telefonnummer

Zeitraum des Aufenthalts / ggf. Platz- oder Tischnummer

Beispiel: Digitale Corona-Gästelisten in Restaurants

Digitale Corona-Gästeliste (am Beispiel corona-anmeldung.de, ähnlich auch für Luca, CWA-Checkin, ...):

- Restaurant registriert sich bei Anbieter
- Anbieter generiert QR-Code, der auf Restaurant-spezifische Anmeldeseite verweist
- Gäste scannen ausliegenden QR-Code und tragen sich online ein
- Restaurant kann im Bedarfsfall Gästeliste (für bestimmten Zeitraum) abfragen

Wenn Ihr so etwas bauen würdet, was müsstet Ihr aus Datenschutzsicht beachten?

„9 + 1 Prinzipien“

Welche waren das?

Was noch? 9 Prinzipien

Rechtmäßigkeit (incl. Einwilligung)

Zweckbindung

Datensparsamkeit (incl. Erforderlichkeit)

Transparenz

Richtigkeit

Sicherheit (insb. Vertraulichkeit, Integrität, Verfügbarkeit)

Verantwortlichkeit (incl. nachweisbare Rechtskonformität)

Kontrolle und Durchsetzung

Datenportabilität

⟶ Was besagten diese Prinzipien nochmal?

Was noch? 9 Prinzipien

Rechtmäßigkeit (incl. Einwilligung)

Zweckbindung

Datensparsamkeit (incl. Erforderlichkeit)

Transparenz

Richtigkeit

Sicherheit (insb. Vertraulichkeit, Integrität, Verfügbarkeit)

Verantwortlichkeit (incl. nachweisbare Rechtskonformität)

Kontrolle und Durchsetzung

Datenportabilität

→ Wie wirken sich die Prinzipien im Kontext „analoge Corona-Gästelisten“ aus?
→ Wie im Kontext digitaler Gästelisten?

Optional: Datenschutz-Aufgabe

Als Übung ein Mini-Essay schreiben (1 Seite + Quellen) und gegebenenfalls in Sprechstunde besprechen:

Ein Prinzip wählen und auf Basis wiss. Lit. erklären

⟶ Technologischen Ansatz identifizieren, der das Prinzip „by Design“ in konkretes technisches System integriert und auf Basis wiss. Lit. erklären

⟶ Chancen und Grenzen des technischen Ansatzes darstellen / diskutieren

⟶ Möglicher sinnvoller Einsatz in Anwendungsfall aus Eurem Alltag

Optional: Datenschutz-Aufgabe

Prinzip wählen und auf Basis wiss. Lit. erklären
⟶ **Technologischen Ansatz identifizieren und auf Basis wiss. Lit. erklären**
⟶ Potenziale und Grenzen des technischen Ansatzes darstellen / diskutieren
⟶ möglicher sinnvoller Einsatz in Anwendungsfall aus Eurem Alltag

<u>Schlüssel für gute Lösung:</u>

Wissenschaftlichen & tragfähigen technischen Ansatz finden, der für die konkrete praktische Umsetzung eines Datenschutzprinzips genutzt werden kann, nicht einfach „irgendwelche“ technischen Mechanismen

Einige Prinzipien eignen sich zudem besser als andere – klug wählen und ggfs. auch Wahl ändern

Gutes Zeichen ist, wenn technisches wiss. Paper zu einer neuen Technologie sich explizit auf GDPR und Prinzip bezieht:
z.B. Scholar: “<principle> gdpr <term-to-ensure-technicality>“, ggfs. + „2018 und neuer“

Schlechte Beispiele, die in der Vergangenheit niemals gut funktioniert haben

„Semantic Web“ für Datenportabilität:
Löst zentrale Probleme nicht; geht immer dann kaputt, wenn es konkreter werden soll (Schema, Datentypen, ...)

Blockchain-Ansätze für Nachweisbarkeit (im Kontext von Verantwortlichkeit):
Ist jedenfalls dann problematisch, wenn public Blockchains vorgeschlagen werden.
Funktioniert außerdem nicht, wenn z. B. jede Datenoperation einen Eintrag in einer (auch: private) Blockchain bekommen soll – Skalierbarkeit
Außerdem löst es hier kein Problem, das sich nicht auch mit (verketteten) Hashes/Signaturen lösen ließe

Cookie Banner
Nicht geeignet, um es beispielsweise für Transparenz zu benutzen

⟶ Gefundene Paper kritisch hinterfragen – „if it smells fishy, it might be fish“

fin