Systematisch interaktiv.

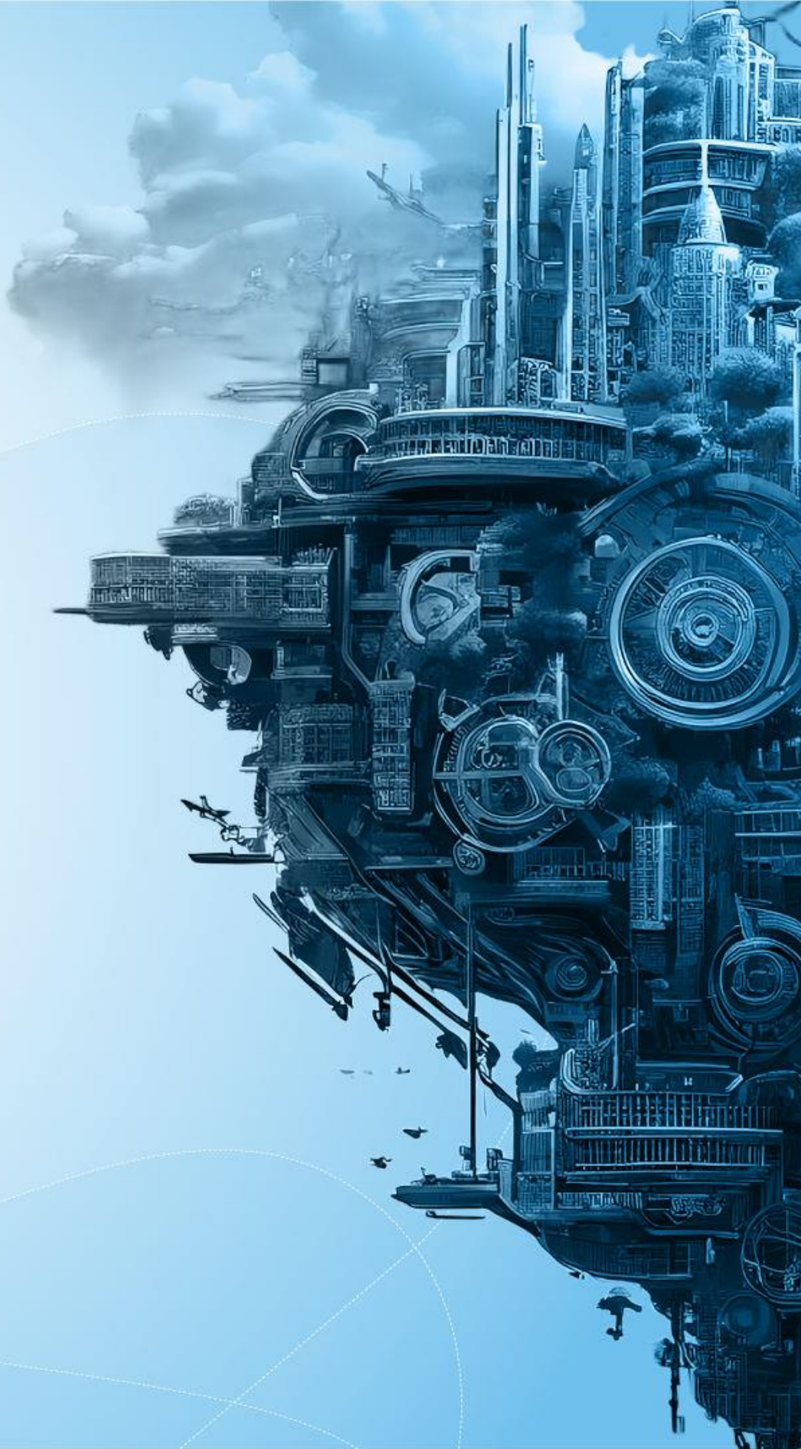
Das Zusammenspiel der Prozesse.

Tobias Kahl

Entwicklungsleiter

Auf Nummer sicher

Unsere Konzepte für
Datenschutz und Datensicherheit



Datenschutz
Informationssicherheit

Datenschutz vs. Datensicherheit

	Datenschutz	Datensicherheit
Zweck	Schutz von personenbezogenen Daten vor missbräuchlicher Verarbeitung	Technische Sicherheit der Daten vor Verlust, Viren, Manipulation etc.
Wodurch	Anwendung von Vorschriften und Gesetzen, sowie technischer und organisatorischer Maßnahmen	Anwendung von technischen und organisatorischen Sicherheitsmaßnahmen
Ziel	Informationelle Selbstbestimmung von Personen (Schutz der Privatsphäre)	Abwendung von Datenverlusten und dem Zugriff unberechtigter Personen
Grundlagen	Datenschutz-Grundverordnung (DSGVO) Bundesdatenschutzgesetz (BDSG)	Technische Möglichkeiten der Datensicherheit

ISO-Zertifizierung bei der ESN

ISO 9001 & ISO 27001

ISO 9001 – Qualitätsmanagementsystem

- Maßnahmen zur kontinuierlichen Verbesserung
- Prozessorientierte Unternehmensabläufe
- Sicherstellung klarer Organisationsabläufe
- Förderung der Transparenz im Unternehmen und gegenüber Kunden
- Steigerung des Kundenvertrauens

seit 2008

ISO 27001 – Informationssicherheits-managementsystem

- **Maßnahmen zur Datensicherheit**
- **Vertraulichkeit betrieblicher und personenbezogener Daten**
- **Starkes Bewusstsein für Cyber-Risiken**
- **Ziel: Zertifiziertes IT-Sicherheitsmanagement zum Schutz unserer und Ihrer Daten.**
  - Wichtiger Meilenstein als Lieferant im Kontext der NIS2-Richtlinie

Work in Progress

Sichere Systemarchitekturen

am Beispiel DNA und ELS

Sichere Systemarchitekturen

- Keine Firewall-Freigaben von niedriger geschützten Netzen (der DMZ) in höher gesicherte Netze (MZ).
  - ReverseProxy mit umgekehrtem Verbindungsaufbau
- Datenhaltung primär im internen Netz
  - Keine Datenhaltung in den DNA-Portalen
  - Mobile Clients mit reduziertem Datenumfang

Sichere Systemarchitekturen

- Neue Authentifizierungsthemen
  - OAuth2 / OIDC
  - Zweifaktor-Authentifizierung
- "Zero-Trust" für (neue) APIs
- Modularisierte Services je Fachdomäne

Anwendungsseitige Maßnahmen

Sonstiges

Anwendungsseitige Maßnahmen

- **Bereitstellung von Modulen zur Umsetzung von Pflichten aus der DSGVO**
- **Verschlüsselung von Config-Parametern**

What’s next?

Womit es weitergeht.

What’s next

- **Etablierung einer zentralen Logverwaltung**
  - inklusive einer Möglichkeit zur einfachen/laufenden Übertragung an den ESN-Support
- **Ausbau des Hostings durch die ESN**
  - Im LIS und bei den DNA-Portalen bereits möglich

Vielen Dank!