



BWI

IT für Deutschland

BWI **INDUSTRY DAYS**

Gemeinsam für eine resiliente IT-Zukunft
8. bis 9. August 2023, Berlin

Breakouts 9. August 2023, B Session B4, 14 bis 14:55 Uhr

Der Souveräne Arbeitsplatz als wesentlicher Schritt zur digitalen Souveränität



Dr. Martin Deeg

BWI GmbH

CDO Customer Solutions (CS)

+49222598818520

Martin.Deeg@bwi.de



Andreas Reckert-Lodde

Geschäftsführer des Zentrums für

Digitale Souveränität der Öffentlichen Verwaltung
(ZenDiS)

Andreas.ReckertLodde@zendis.de

Breakouts 9. August 2023 B Session B4 14.00 - 14:55 h

Der Souveräne Arbeitsplatz als wesentlicher Schritt zur digitalen Souveränität

01

Digitale Souveränität der öffentlichen Verwaltung

02

Übersicht zum Zentrum für Digitale Souveränität (ZenDIS)

03

Digitale Souveränität der Bundeswehr

04

Open Source Projekte

05

DEMO

06

Projekt Souveräner Arbeitsplatz Bundeswehr

Welches Betriebssystem nutzen Sie privat?

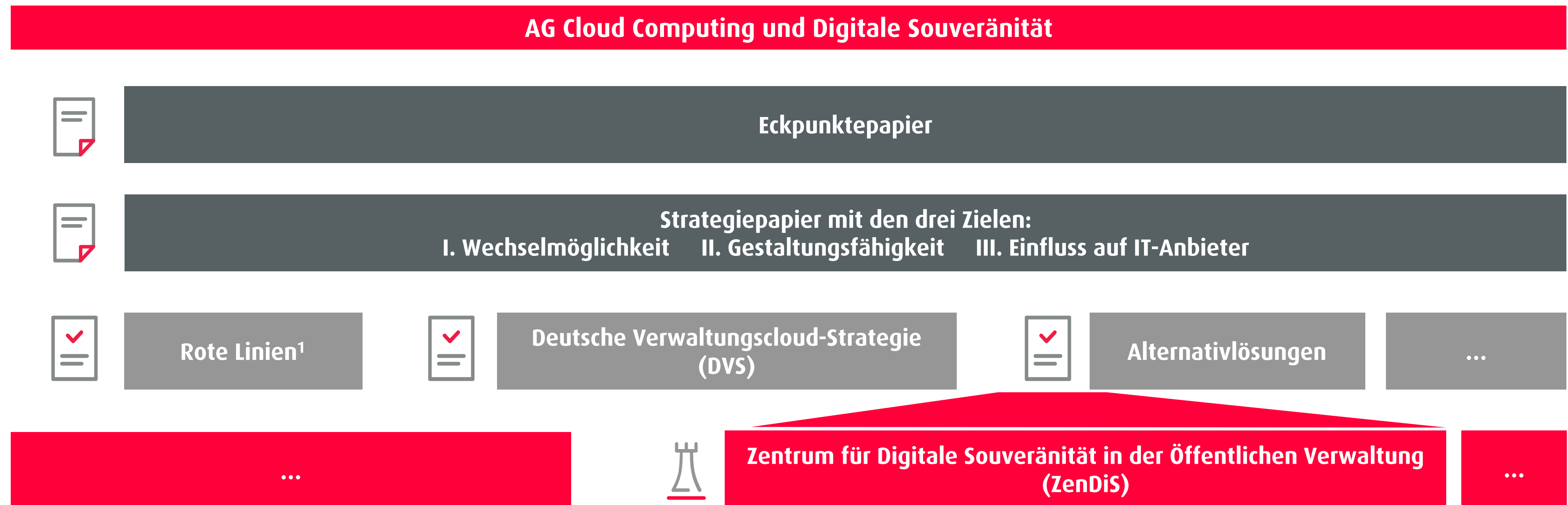
- Android
- Linux
- iOS
- Windows
- sonstige

Fühlen Sie sich dabei digital souverän?

Wie lange würde es dauern, die Daten, die Sie mit diesen Endgeräten verarbeiten, auf einem ganz anderen System wiederherzustellen, falls das Endgerät mitsamt seinem Provider von heute auf morgen nicht mehr verfügbar wäre?

Digitale Souveränität der öffentlichen Verwaltung

Bund, Länder und Kommunen haben beschlossen das Angebot und die Verwendung von **OS-Alternativlösungen** in der ÖV zu stärken



Übersicht zum Zentrum für Digitale Souveränität (ZenDIS)

Dr. Martin Deeg & Andreas Reckert-Lodde - Der Souveräne Arbeitsplatz als wesentlicher Schritt zur digitalen Souveränität - BWI intern - Eine Weitergabe an Auftraggeber ist erlaubt

Ziel des ZenDiS ist es, die Verfügbarkeit von Open Source-Lösungen sicherzustellen sowie deren Einsatz zu forcieren

Mission: Zentrale Koordination zwischen **ÖV** und dem **OS-Ökosystem**, um die **Verfügbarkeit** moderner, leistungsfähiger und skalierbarer **OS-Lösungen sicherzustellen** sowie deren **Einsatz in der gesamten ÖV zu forcieren**



ZenDiS = Zentrum für Digitale Souveränität
 ÖV = Öffentliche Verwaltung
 OS= Open Source

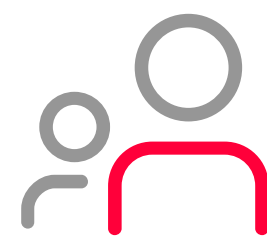
Das Aufgabenspektrum des ZenDiS umfasst eine Vielzahl an Unterstützungsleistungen für die Öffentliche Verwaltung



1) In Abstimmung mit der Deutschen Verwaltungscldoud-Strategie

Digitale Souveränität der Bundeswehr

Warum ist Digitale Souveränität so wichtig?



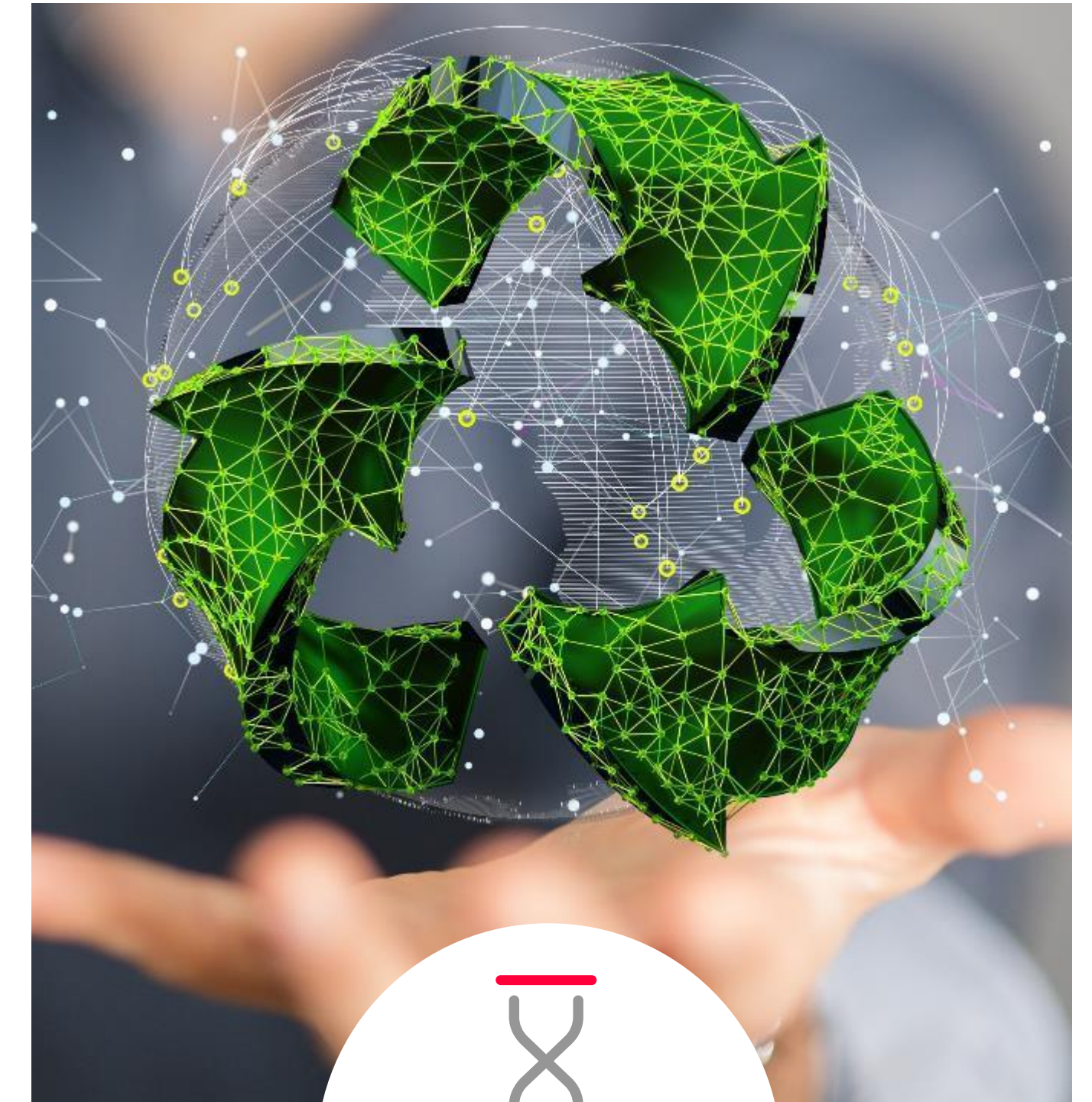
Daten

.. für die Einsatzplanung
verfälscht ..



Anwendungen

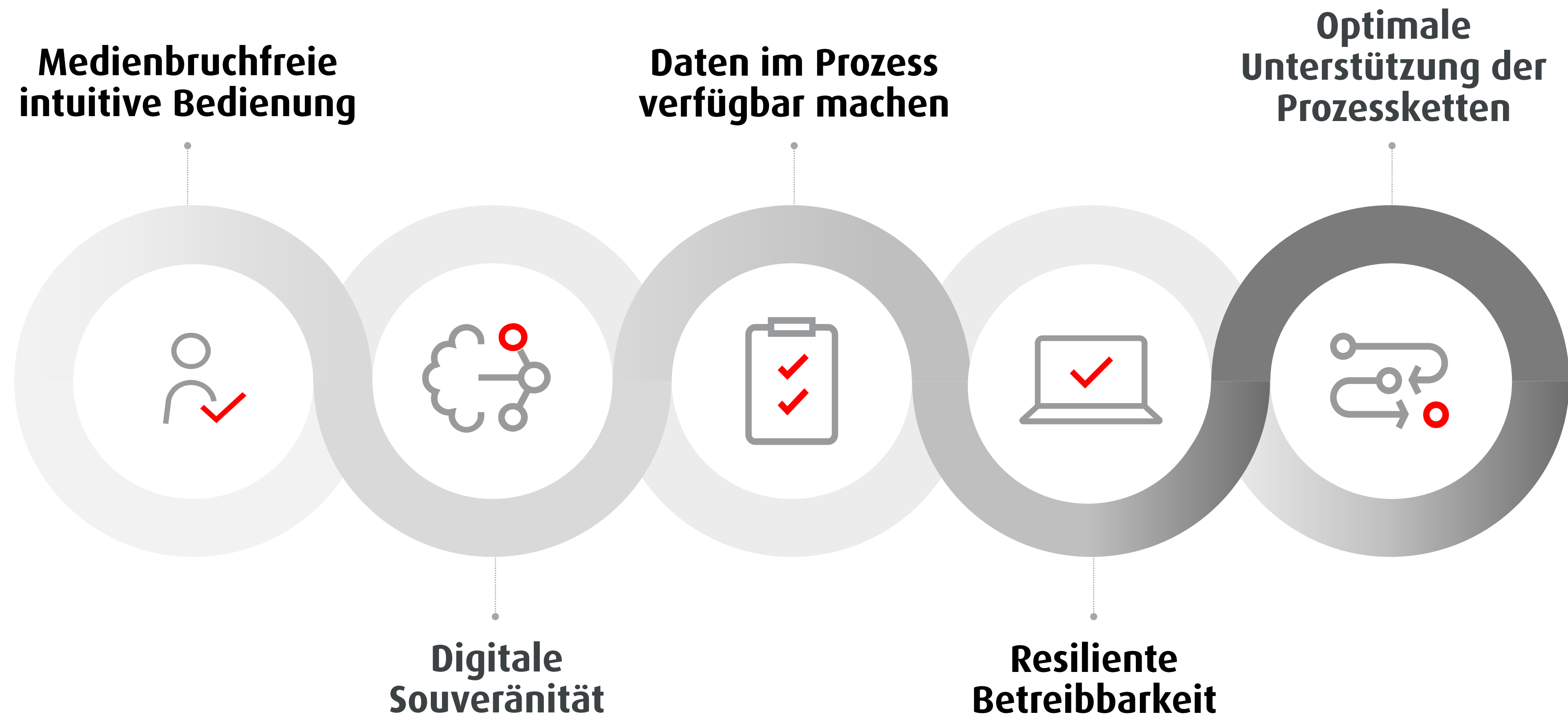
.. im entscheidenden
Moment nicht verfügbar ..



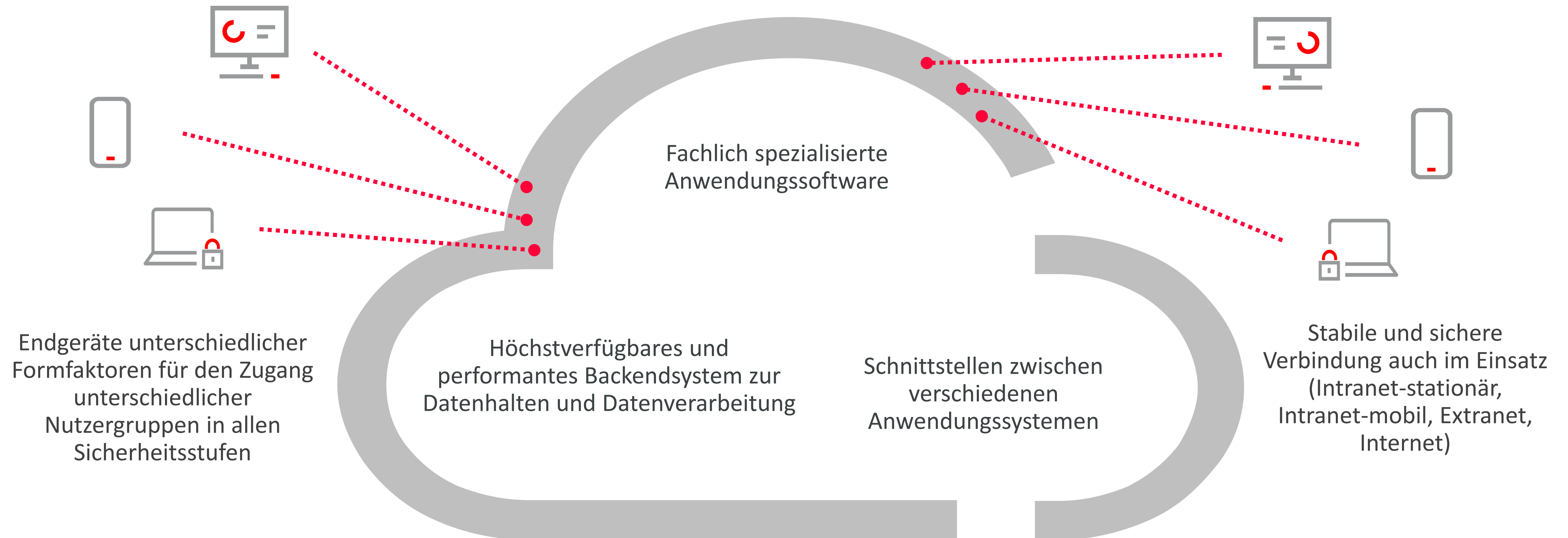
Betreibbarkeit

.. durch eine Preiserhöhung
sehr teuer ..

Digitalisierung ist der Schlüssel zur Wirksamkeit

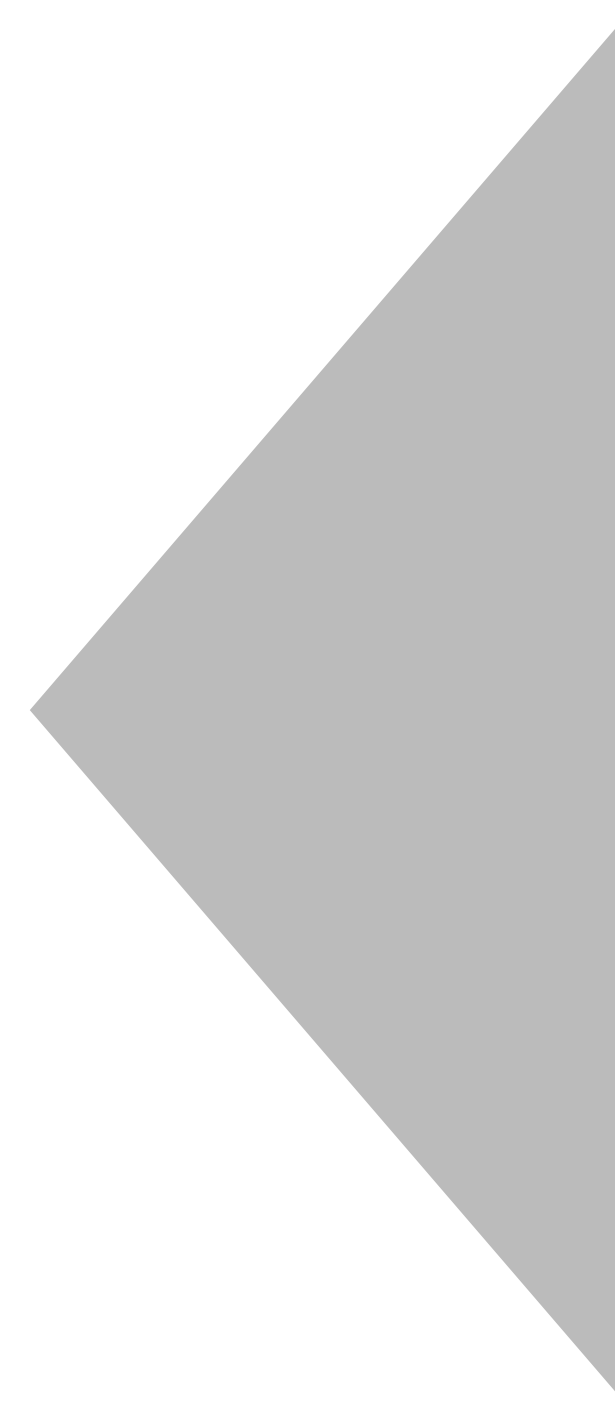


Digitalisierungslösungen fordern alles



.. „die Wahl haben“

- welche Daten werden wofür genutzt
- wo werden die Daten gespeichert
- wie werden die Daten geschützt
- wer hat Zugang zu Daten
- wer hat Zugang zu Anwendungen
- wie wird der Betrieb gestaltet
- wer führt den Betrieb durch
- welche Architektur und Technologie
- welche Produkte werden eingesetzt

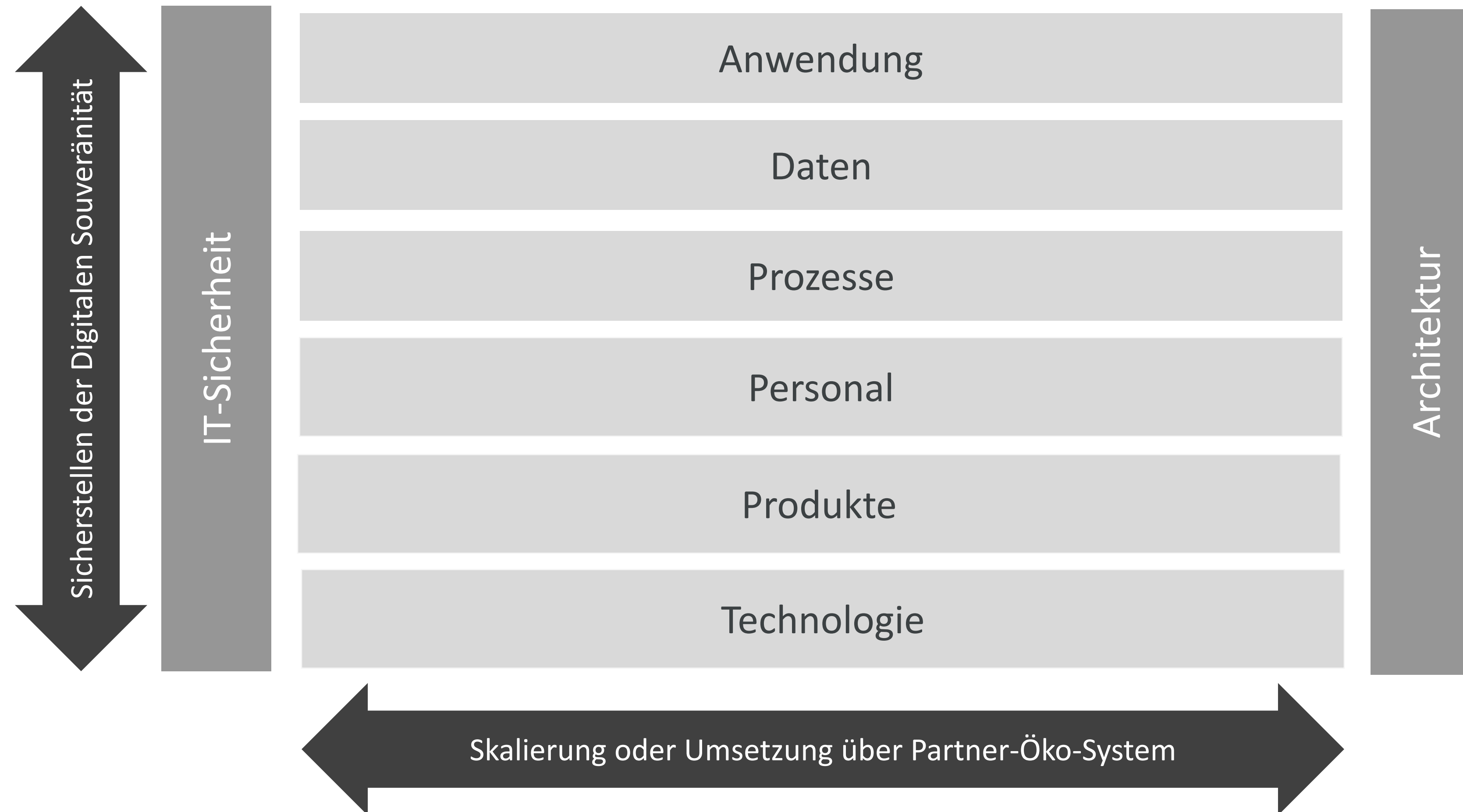


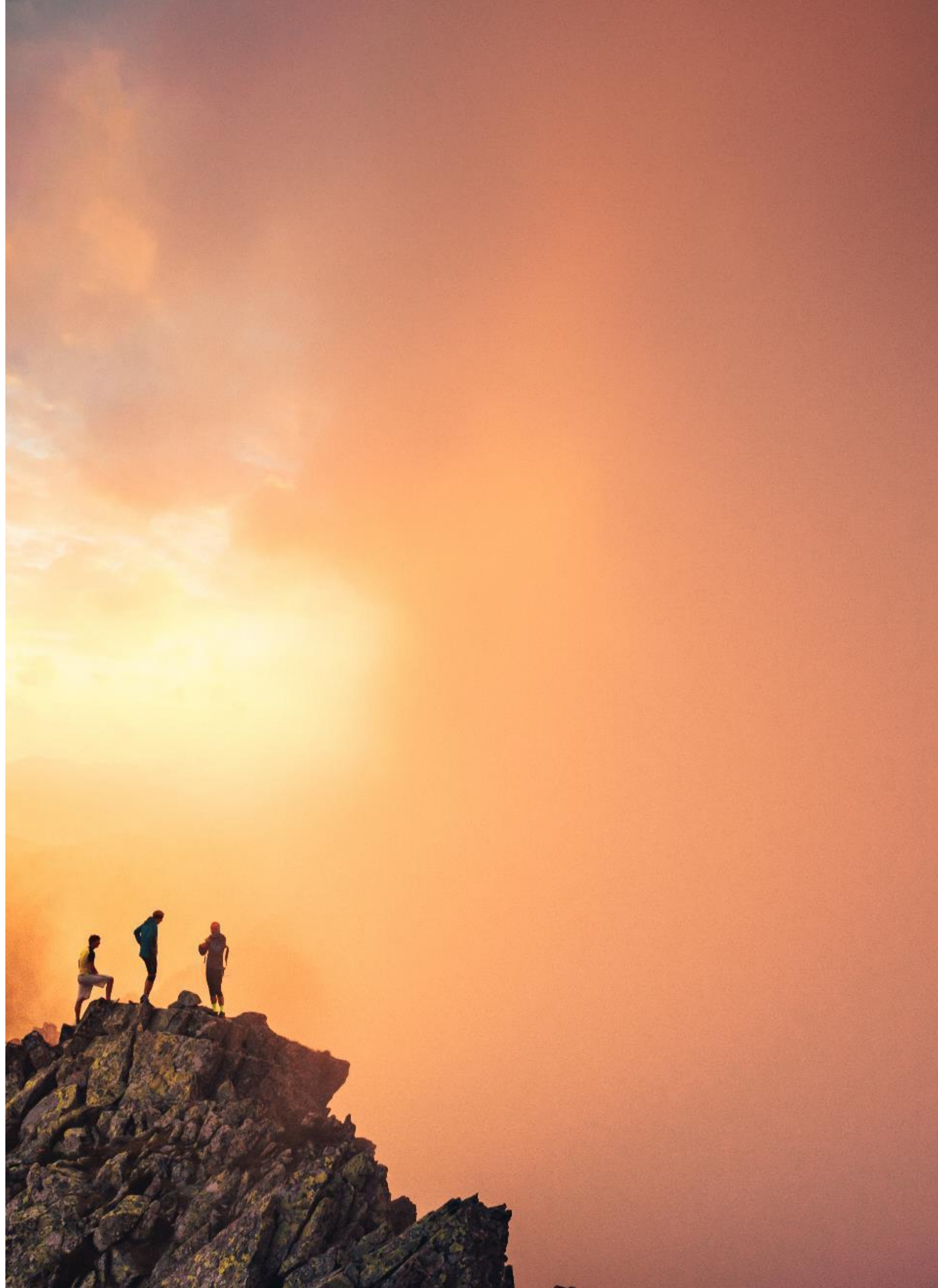
Bewahrung der
Datenverfügbarkeit, -
vertraulichkeit und
-integrität

Sicherstellung der
Handlungsfähigkeit im digitalen
Umfeld

Reduktion von Abhängigkeiten
von einzelnen ITK-
Produktherstellern

Digitale Souveränität für eine resiliente IT-Zukunft braucht starke Partner





Digitale Souveränität

Offene Standards u. Architekturen

Open Source

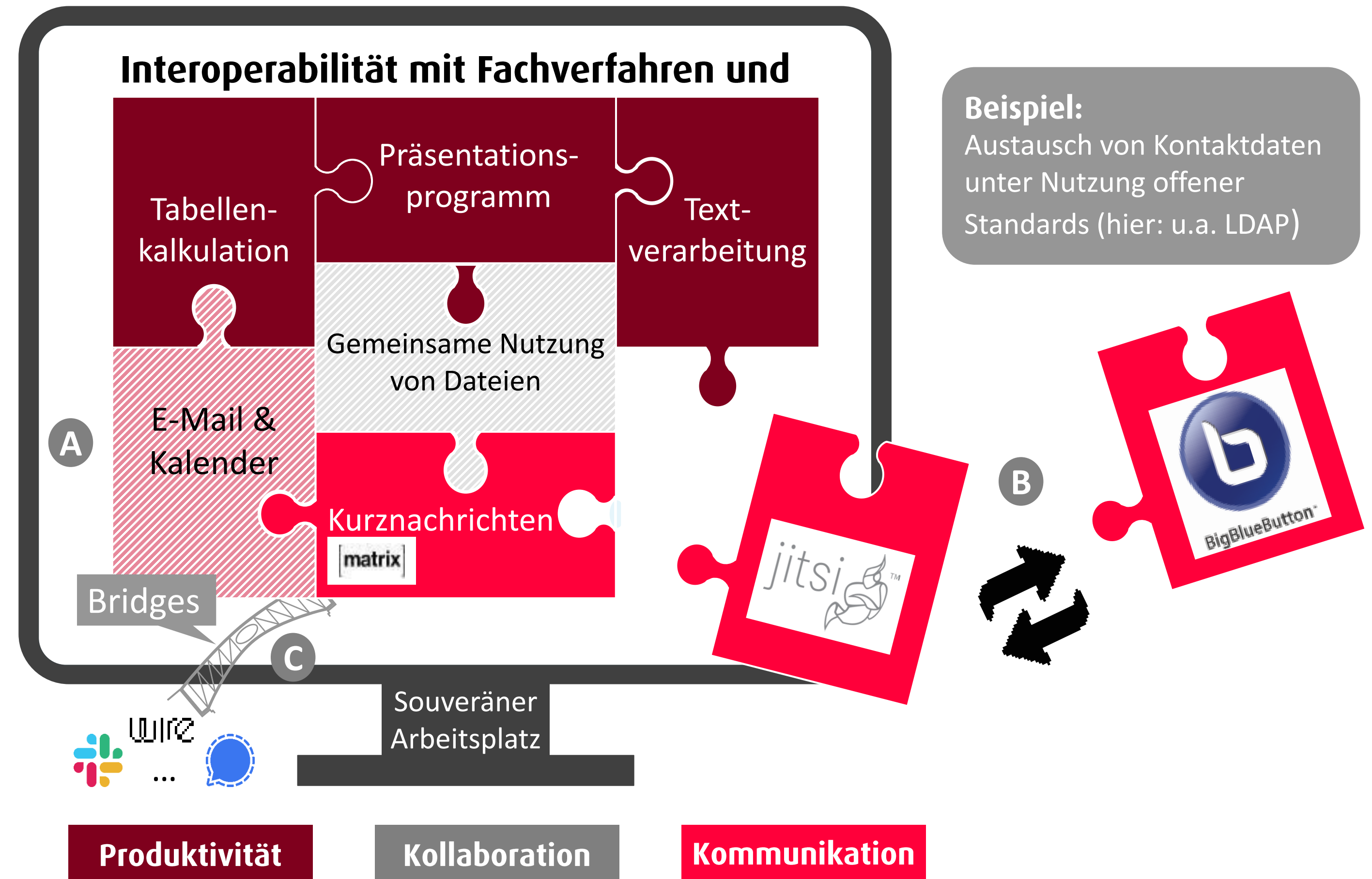
Investitionen

Partnerschaften

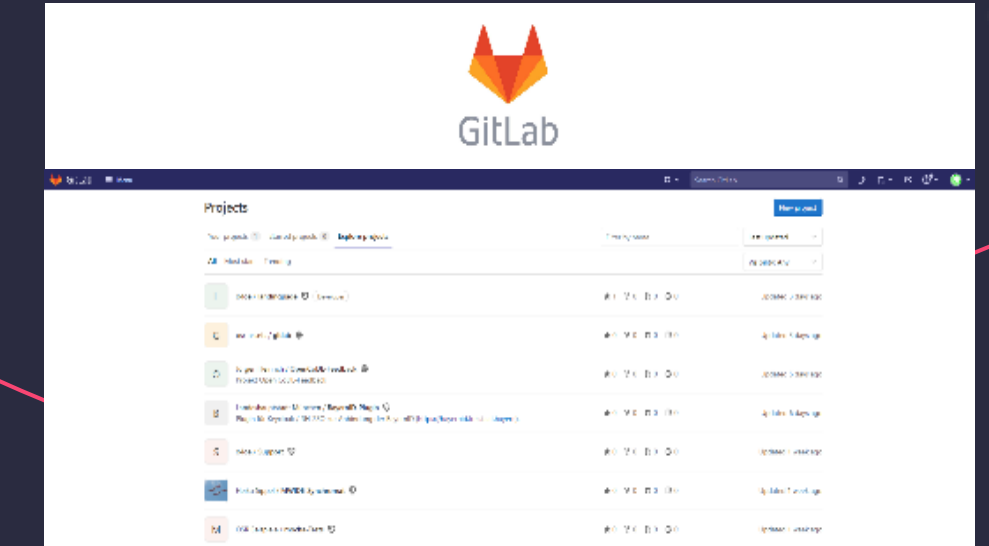
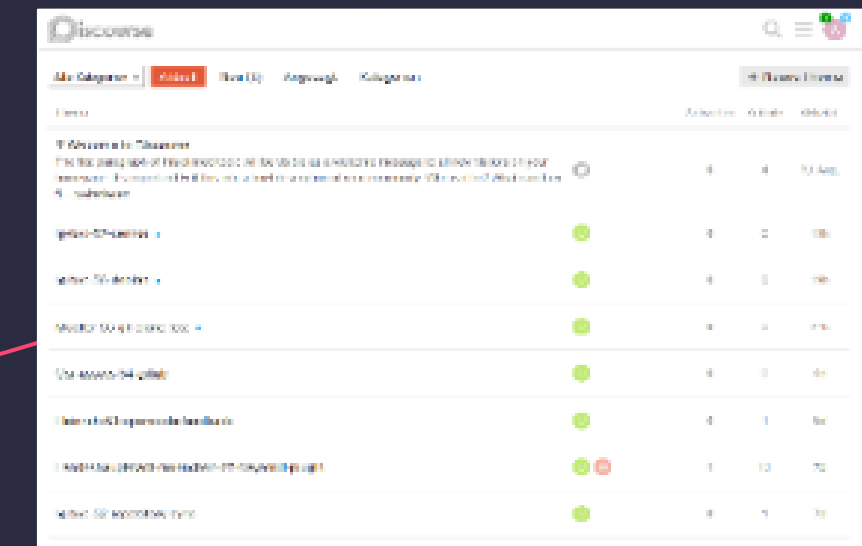
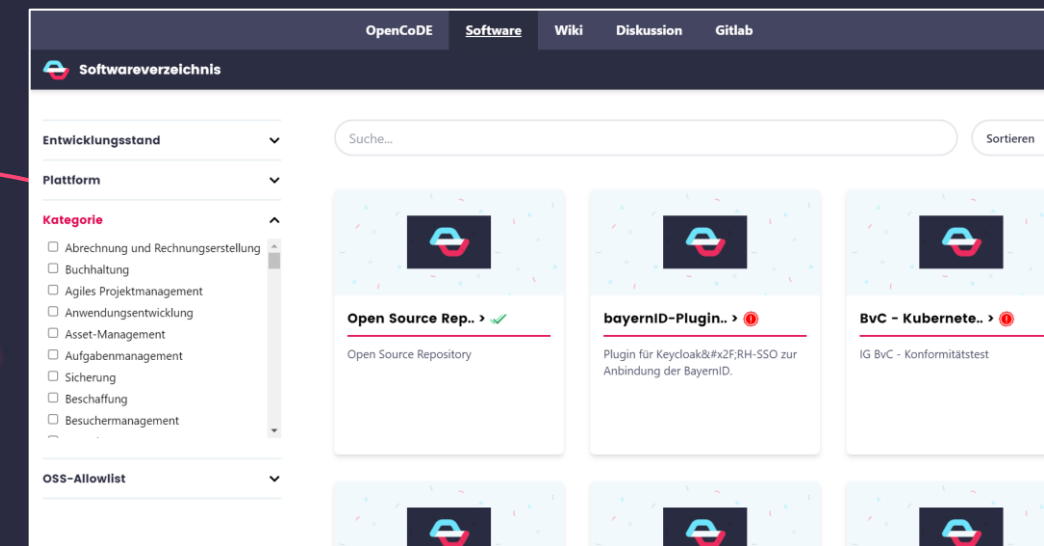
Open-Source Projekte

Ein konsequenter Fokus auf Modularität, Austauschbarkeit und Interoperabilität verhindert dabei neue Abhängigkeiten

- A Modularität**
- Funktionsumfang kann behörden-spezifisch festgelegt werden
 - Nutzung vorhandener Lösungen möglich (z.B. existierender NextCloud Instanz und keine „Pflicht“ zur Nutzung von OpenXchange)
- B Austauschbarkeit**
- Offene Schnittstellen & Standards ermöglichen Austausch von Komponenten & vermeiden Lock-in
 - Integration der Komponenten unter Zuhilfenahme offener Standards
- C Interoperabilität**
- Austausch von Daten mit anderen Lösungen möglich (z.B. Matrix „Bridges“)
 - Anbindung an bestehende Fachanwendungen (wie z.B. E-Akte) durch Schnittstellen und APIs



Open Source Code für die Öffentliche Verwaltung



Informieren

- Informieren über **Ziele, Funktionsweise und Möglichkeiten der Teilnahme**
- Link zu **Lizenzbedingungen, Nutzungsbedingungen und Datenschutzrichtlinie**
- Möglichkeit zur **Registrierung**

OSS wiederverwenden

- **Suche im zentralen Verzeichnis** nach Softwarelösungen der ÖV
- **Wiederverwenden** von Softwarekomponenten
- Veröffentlichen von **eigener Software für höhere Sichtbarkeit**

Diskutieren

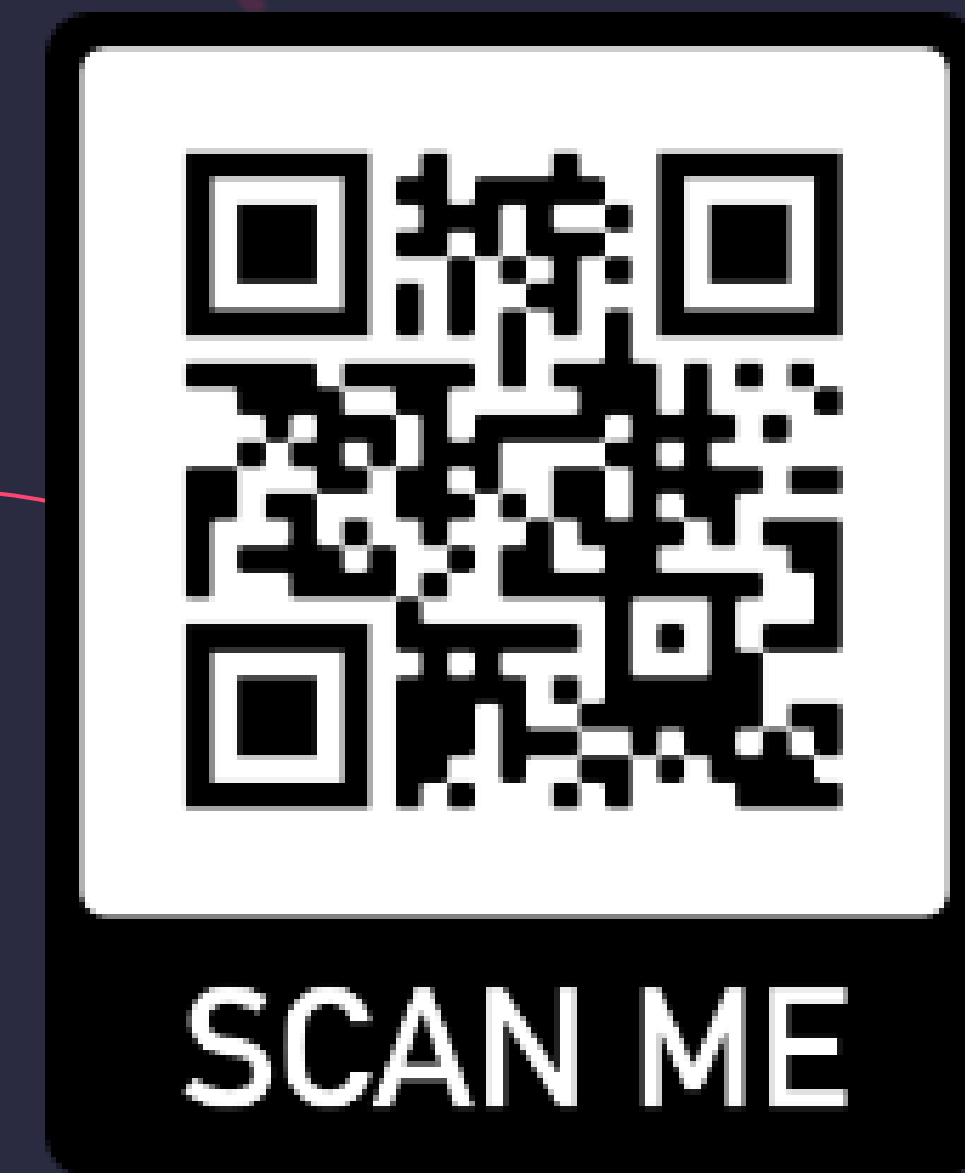
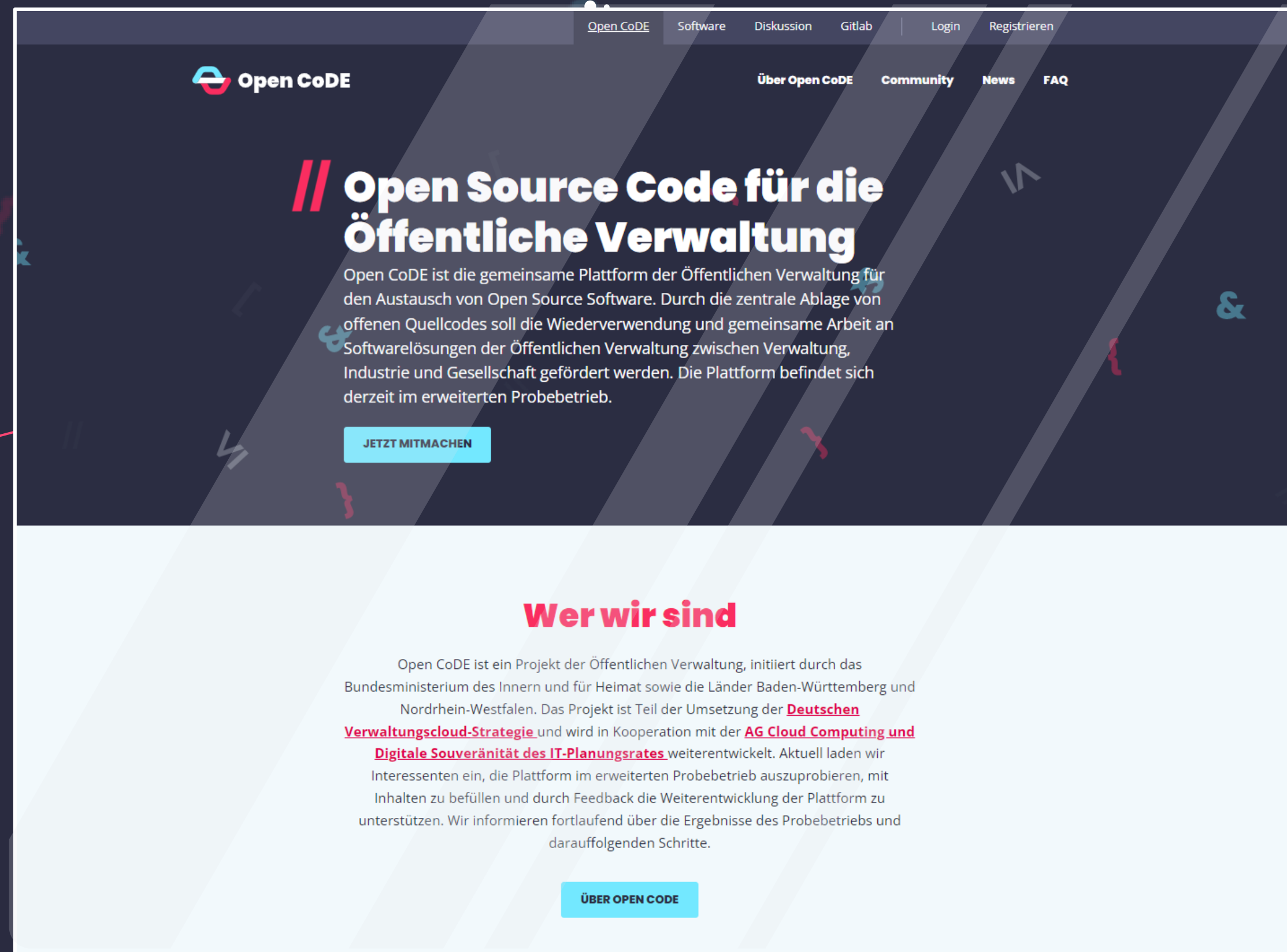
- Beteiligen an der **Diskussion über Softwareprojekte** und allgemeine Themen zu OS in der ÖV
- Starten eines neuen Gespräch über spezifische **Erfahrungen, Herausforderungen und Good Practices**

An Code arbeiten

- **Start eines neuen Softwareprojektes** durch Verwaltungsträger (oder mit deren Zustimmung)
- **Beteiligung an Entwicklung** durch ÖV, Unternehmen oder Privatpersonen; z.B. Beisteuern von Code



Wir laden Sie herzlich ein, die Plattform auszuprobieren und die Weiterentwicklung **durch Feedback zu unterstützen**



DEMO

Souveräner Arbeitsplatz

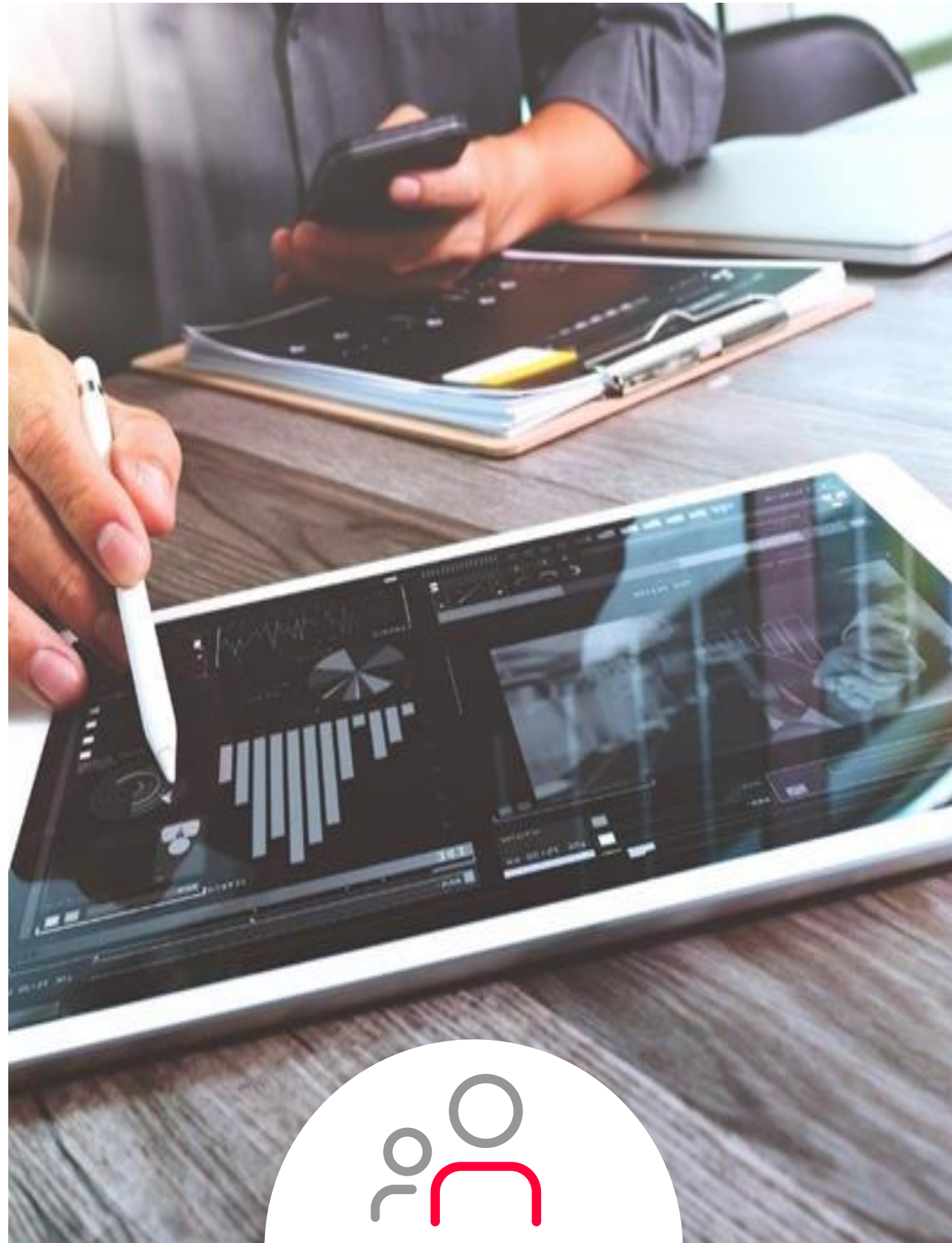


Projekt souveräner Arbeitsplatz Bundeswehr

Proof of Concept

- Office und Collaboration Produkte für einen souveränen Arbeitsplatz für die Bundeswehr
- Leistungsfähigkeit und Nutzerfreundlichkeit
- Skalierbarer und resilienter Betrieb auf Basis offener Standards

PoC - Souveräner Arbeitsplatz Bundeswehr



- Souveräner AP der ÖV über das OpenCoDE Repository des ZenDIS
- Kooperation mit Dataport AöR
- Technische Implementierung erfolgt gemäß Deutscher VerwaltungscLOUD Strategie (DVS) auf der pCloudBw
- Bewertung Eignung für Bw und Machbarkeit
- Vorbereitung des sicheren, skalierbaren, enterprise-tauglichen Betriebs



- Umsetzung von Beschlüssen des IT-Rats



Open Source Suite für den Souveränen Arbeitsplatz Bw

Themenschwerpunkte (1/2)

1



Identity & Access Management der Bw

- Implementierung eines kundeneigenen IAM (IAM Bw)
- Blueprint für z.B. andere Behörden

2



Umsetzung Architekturvorgaben

- Kompatibilität der Applikationen zur DVS und der private Cloud der Bw
- FMN-Interoperabilität

3



Integration des BwMessenger

- Anpassung auf die Bedürfnisse der Bw
- Basis/Blueprint für die Integration des BundesMessenger auch für anderer Behörden

4



Integration einer eigenständigen Open Source Videokonferenz (OSVK)

- Jitsi Meet – Verzahnung und Austausch mit Projekt BMI OSVK Bund

Open Source Suite für den Souveränen Arbeitsplatz Bw

Themenschwerpunkte (2/2)

5



Nutzungs- & Lizenzbedingungen

- Open Source Nutzungsbedingungen für Bw
- Verwaltung Nutzung- und Abrechnung für Bw

6



Offline-/ Verlege-fähigkeit

- Prüfauftrag auf die Bedürfnisse der Bw
- Machbarkeitsanalyse und Lösungsoptionen

7



Proof of Concept Enterprise-fähigkeit

- Laborinstallation techn. Prüfung
- Robustheit
- Belastbarkeit
- Skalierbarkeit

8



Betrieb, Service und Support

- Betriebs- und Sicherheitskonzeption für Provider (hier BWI)
- Release-management & Security-Updates
- OSS Support (OLA/SLA)

Vielen Dank für die Aufmerksamkeit.



Warum nutzen wir so wenig Open Source Software?

Wird ihrer Ansicht nach auf Bundeswehrebene genug für die digitale Souveränität investiert?

In welche Themenfelder sollte Ihrer Meinung nach mehr investiert werden, um die digitale Souveränität zu verbessern?

Nutzt ihre Firma oder Behörde Open Source Software (Skala von 1-10)?