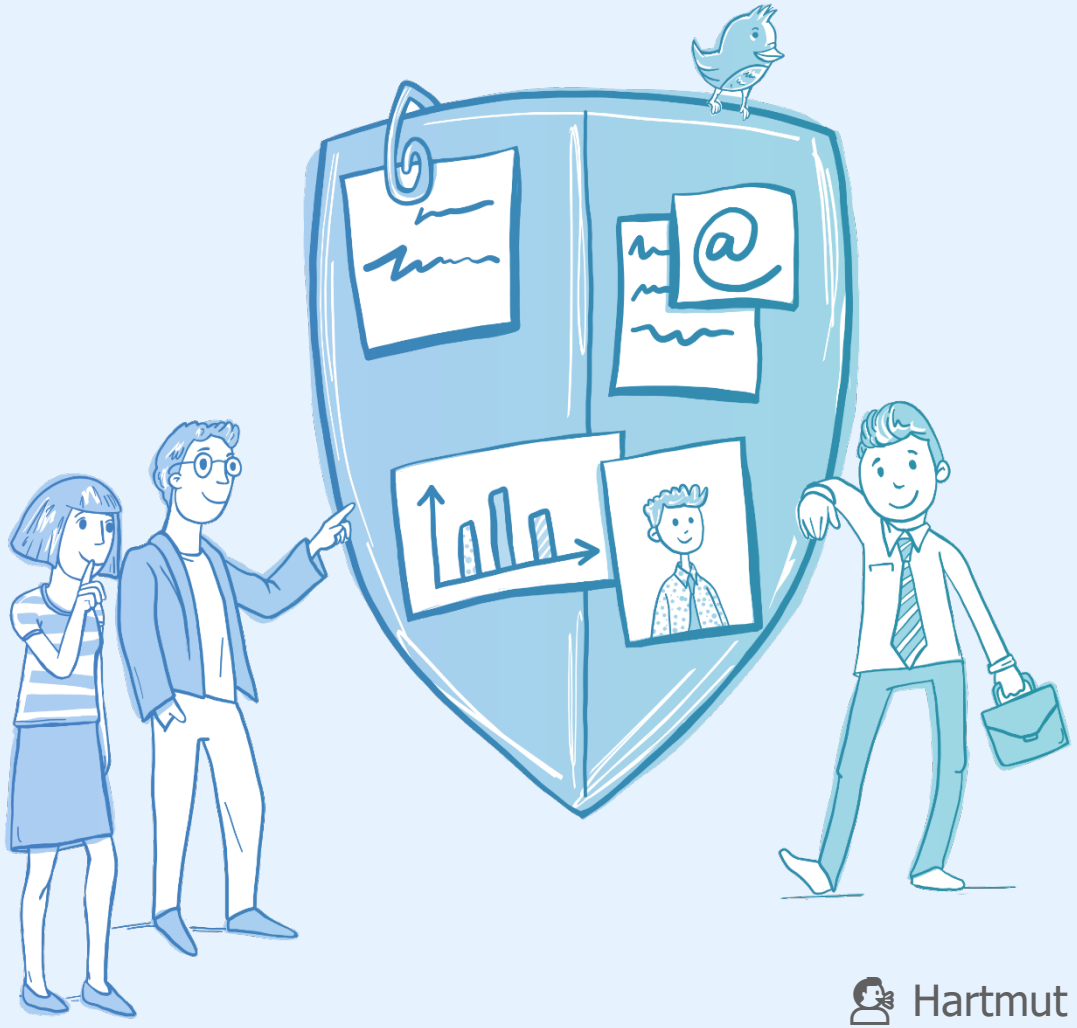


Hartmut Schmitt hartmut.schmitt@hk-bs.de

TrUSD – Transparente und selbstbestimmte Ausgestaltung der Datennutzung im Unternehmen

Abschlussveranstaltung – 31. August 2021

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

TrUSD – Transparente und selbstbestimmte Ausgestaltung der Datennutzung im Unternehmen

- Fördermaßnahme „Privatheit und informationelle Selbstbestimmung in der digitalen Arbeitswelt“
- Förderung mit Mitteln des Bundesministeriums für Bildung und Forschung im Rahmen des Forschungsrahmenprogramms der Bundesregierung zur IT-Sicherheit „Selbstbestimmt und sicher in der digitalen Welt“
- Laufzeit 09/2018 - 08/2021

VDI|VDE|IT

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

Das Projekt TrUSD

HK Business Solutions GmbH	Anwendungspartner / Gesamtprojektleitung
Institut für Technologie und Arbeit	Forschungspartner
Fraunhofer IESE	Forschungspartner
Technische Hochschule Köln	Forschungs- und Anwendungspartner *(bis 05/2020)*
Hochschule Bonn-Rhein-Sieg	Forschungs- und Anwendungspartner *(seit 06/2020)*
Universität des Saarlandes	Forschungspartner

Agenda

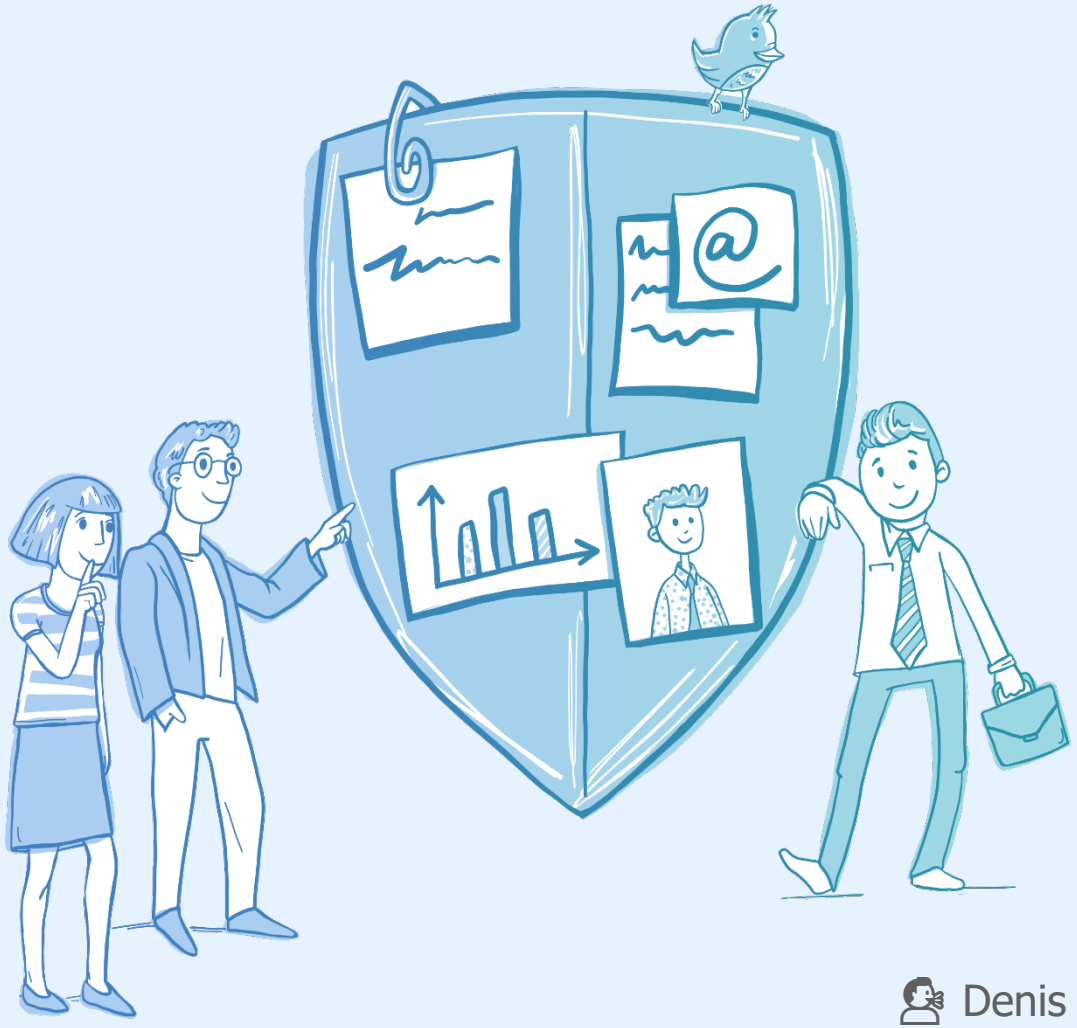
I. Big Picture
Die Ideen hinter dem Projekt »TrUSD«.

II. Umsetzungsbeispiele
So können Privacy-Dashboards in der Praxis gestaltet sein.

III. Werkzeugkasten
So können Sie das Privacy-Dashboard auf Ihr Unternehmen maßschneidern.

IV. Lessons Learned
(Überraschende) Erkenntnisse aus dem Projekt.

V. Diskussionsrunde
Offene Punkte, Ausblick.



Denis Feth denis.feth@iese.fraunhofer.de

Big Picture

Die Ideen hinter dem Projekt »TrUSD«

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Warum besteht Handlungsbedarf beim Thema Beschäftigtendatenschutz?

Motivation

- Unternehmen erfassen immer mehr **personenbezogene Daten** – auch von **Mitarbeitern**
- Dahinter stehen i.d.R. legitime Interessen (und Pflichten) des **Arbeitgebers**

Mitarbeiter:in

Heiratsurkunde
Kreditkartennummer
Reisepassnummer
Krankschreibung
Urlaubszeiten
Qualifikationsdaten
Fotos
Antrag

Verwaltung

- ✓ Reise gebucht
- ✓ Stammdaten aktualisiert
- ✓ Social Media Beitrag gepostet
- ✓ Elternzeitantrag erfasst
- ✓ Abwesenheits-meldung erfasst
- ✓ Personalakte aktualisiert

Motivation

Motivation

Ich möchte über meine Daten bestimmen! Aber wie?

Welche Daten hat mein Arbeitgeber?

Wer darf die Daten verwenden? Wofür?

Was ist unser Projektziel?

TrUSD

Transparente und selbstbestimmte Ausgestaltung der Datennutzung im Unternehmen

Ziele

- Im Einklang mit den **gesetzlichen Regelungen*** …
- **mehr Transparenz** für Arbeitnehmer:innen bei der Verarbeitung personen-bezogener Daten am Arbeitsplatz schaffen und ihnen …
- Möglichkeiten bieten, ihre **Selbstbestimmungsrechte** wahrzunehmen.

* insb. DS-GVO, BDSG-neu

Vorteile

- Insgesamt: **fairer Interessenausgleich und Vertrauen** zwischen Arbeitgebern und Arbeitnehmer:innen
- Arbeitnehmer**:** Ermöglichung der **Datensouveränität**
- Arbeitgeber: **Rechtssicherheit**

Kernergebnisse

- **Modulare Privacy-Dashboards**
  - Umfassender **Anforderungskatalog**
  - Rechtliche **Bewertung**
  - **Umsetzungskonzepte und -beispiele**
  - **Werkzeuge**
  - **…**

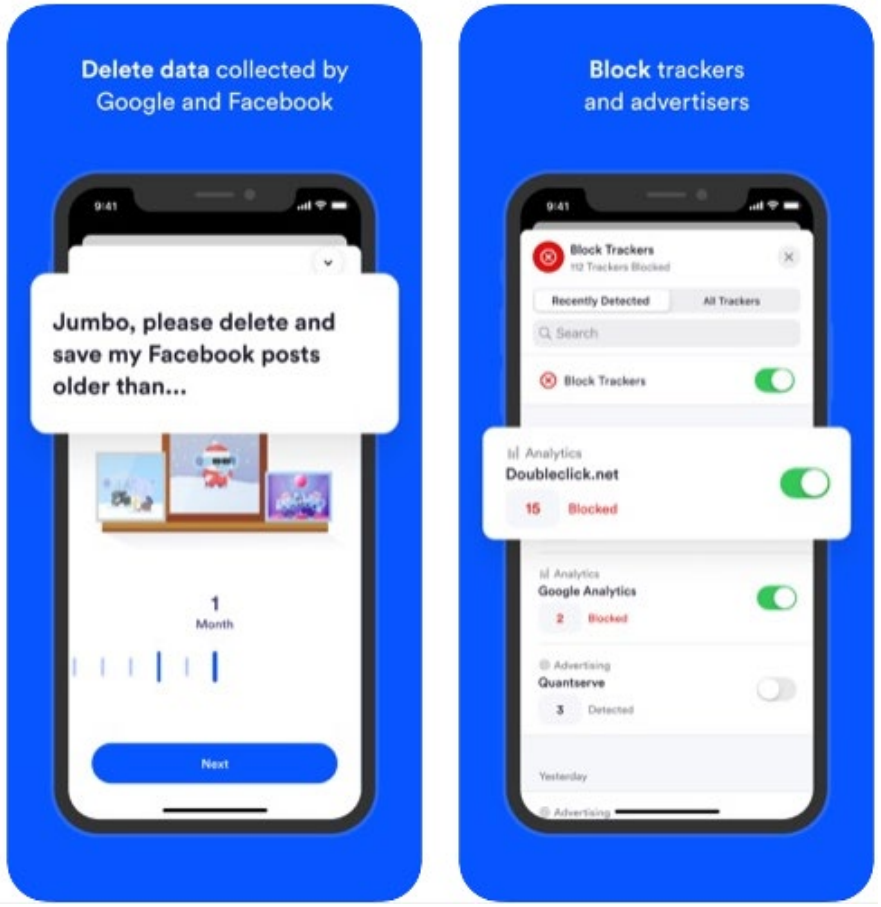
Was sind Privacy-Dashboards?

Was sind Privacy-Dashboards?

Anwendungen, die einen einfachen und zentralen Zugriff auf Funktionen des Datenschutzes und der informationellen Selbstbestimmung ermöglichen

Privacy-Dashboards werden **immer verbreiteter**

- Google Dashboard + Privacy Check
- Microsoft 365
- Social Media platforms
- „Jumbo: Privacy + Security"
- …



Welche Bausteine können Privacy-Dashboards beinhalten?

Information und Auskunft

- Sammlung von Dokumenten und Regelungen
- Datenauskunft
- Übersicht über Berechtigungen
- Verwendungsprotokoll

Durchsetzung in Bestandssystemen

- Zugriffs- und Nutzungskontrolle
- Anonymisierung
- (Semi-)Automatisierte Korrektur und Löschung

Selbstbestimmung

- Datenschutzeinstellungen
- Einwilligungen und Widersprüche
- Datenexport und –übertragung
- Korrektur und Löschung

Kommunikation

- Öffentliche News
- Individuelle Benachrichtigung
- Meldung von Verdachtsfällen

Datenzugriff

- Anfrage von Einwilligungen
- Zugriff auf Daten von Kollegen

Support

- Anleitungen
- Kontakt mit Ansprechpartnern
- Such- und Filterfunktionen

Wie hilft TrUSD bei der Umsetzung und Einführung von Privacy-Dashboards?

Der TrUSD-Werkzeugkasten

Demonstratoren	Wissensdatenbank und Einwilligungsmanagement	Datenkorb	Datennutzungskontrolle	Anonymisierungs-verfahren
Werkzeuge	Selbstbewertungs-instrument	Checklisten für Datenqualität	Navigator für Qualitäts-beziehungen	Glossar
Konzepte	Bausteine & Stufenkonzept	UI- und Interaktionskonzepte	Referenzarchitektur	Einführungskonzepte
Modelle	Qualitätsmodell	Personas	Organisationstypen	Inhaltsontologie
	Anforderungsmodell	Mentale Modelle	Vorgehensmodell	
Anforderungen, Rahmen-bedingungen	Rechtliche Rahmenbedingungen	Bedarfe und Anforderungen verschiedener Stakeholder	Stand der Wissenschaft und Technik	Technische und organisatorische Umsetzbarkeit

Weiterführende Informationen

Was?	Wo?
Allgemeine Informationen zum Projekt	• Webseite: https://www.trusd-projekt.de
Datenschutzrechtliche Grundlagen	• Deliverable 7.1 – Bericht über inhaltliche Anforderungen und Anforderungen an die Datenverarbeitung an das Privacy Dashboard aus Sicht des Datenschutzrechts • Christian K. Bosse, Aljoscha Dietrich, Patricia Kelbert, Hagen Küchler, Hartmut Schmitt, Jan Tolsdorf, Andreas Weßner: Beschäftigtendatenschutz: Rechtliche Anforderungen und technische Lösungskonzepte. In: Erich Schweighofer, Walter Hötzendorfer, Franz Kummer, Ahti Saarenpää (Hrsg.): Tagungsband des 23. Internationalen Rechtsinformatik Symposions IRIS 2020 • Hartmut Schmitt, Christian K. Bosse, Aljoscha Dietrich, Svenja Polst: Wie ich an deine Daten kam oder Dark Patterns und Phishing im Beschäftigtenkontext. In: Erich Schweighofer, Stefan Eder, Philip Hanke, Franz Kummer, Ahti Saarenpää (Hrsg.): Cybergovernance: Tagungsband des 24. Internationalen Rechtsinformatik Symposions IRIS 2021, S. 293–302. Bern: Editions Weblaw.
Rahmenwerk	• Deliverable 2.1 – Rahmenwerk • Hartmut Schmitt & Svenja Polst: Anforderungen und Rahmenwerk für den betrieblichen Datenschutz. In: Softwaretechnik-Trends 40:1, Februar 2020, S. 9-10
Bausteine	• Deliverable 3.1 – Dokumentation der Konzepte zur Erstellung und Einführung von Privacy Dashboards • Florian Dehling, Denis Feth, Svenja Polst, Bianca Steffes und Jan Tolsdorf: „Components and Architecture for the Implementation of Technology-driven Employee Data Protection" in Proceedings of the International Conference on Trust, Privacy and Security Digital Business (TrustBUS 2021)

Agenda

TrUSD

I. Big Picture
Die Ideen hinter dem Projekt »TrUSD«.

II. Umsetzungsbeispiele
So können Privacy-Dashboards in der Praxis gestaltet sein.

III. Werkzeugkasten
So können Sie das Privacy-Dashboard auf Ihr Unternehmen maßschneidern.

IV. Lessons Learned
(Überraschende) Erkenntnisse aus dem Projekt.

V. Diskussionsrunde
Offene Punkte, Ausblick.

Demonstratoren

TrUSD

Kathleen Späth kathleen.spaeth@iese.fraunhofer.de

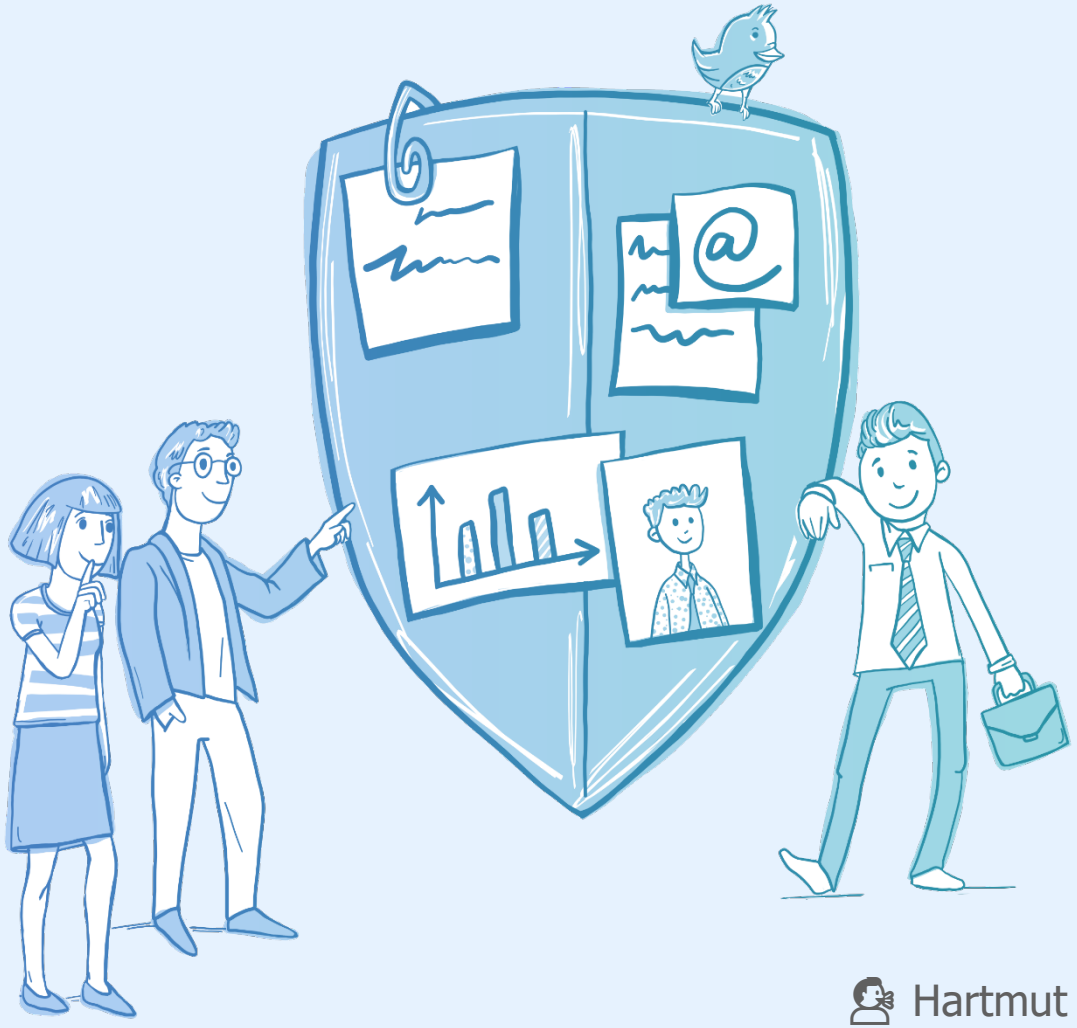
So können Privacy-Dashboards in der Praxis gestaltet sein

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

https://youtu.be/x-bXgRAut-s

Demonstratoren

TrUSD



Hartmut Schmitt hartmut.schmitt@hk-bs.de

Umsetzung eines Privacy-Dashboards bei der HKBS

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Privacy Dashboard – Umsetzung bei der HKBS

- Kontext
  - IT-Firma, Schwerpunkt betriebswirtschaftliche Softwareprodukte
  - Anwenderunternehmen aus Handel und Industrie
- Inhalte
  - allgemeine Informationen zum (Beschäftigten-)Datenschutz
  - unternehmensspezifische Informationen zum Datenschutz
  - Einwilligungsmanagement
  - Erfüllung der Informationspflichten
- Umsetzung als Webapp

Funktionsfähiger Demonstrator

TrUSD

Projekt 1

- allgemeine und unternehmensspezifische Informationen
- im HKBS Look & Feel
- in vorhandene Intranet Anwendung integriert
- reale Umgebung/Produktivbetrieb, partizipatives Vorgehensmodell

Projekt 2

- allgemeingültige Informationen, Beispieldokumente
- neutrales UI-Design
- Stand-alone-Lösung
- genutzt für Interviewstudie

TrUSD - Wissensdatenbank

https://trusd.hk-bs.de:51252/TrusdDashboard/Index

TrUSD

Hallo cevaoffner! Abmelden

Dashboard | Wissensdatenbank | Nutzungsanfragen | Meldungen 1

Was möchten Sie wissen?

Dashboard

Allgemeine News

Verpflichtungserklärung Datenschutz
Erstellt am 30.06.2021 09:42:34 von cevaoffner in **Meldung**

Ankündigung Kontrolle Internet-Traffic
Erstellt am 30.06.2021 09:07:30 von cevaoffner in **Meldung**

Datenschutz-Dashboard
Erstellt am 30.06.2021 09:07:00 von cevaoffner in **Meldung**

Startseite Dashboard

Wissensdatenbank - Letzte Einträge

Verarbeitungszwecke
Erstellt am 15.06.2021 16:50:48 von oholinski in **Wiki-Eintrag**

Verarbeitung personenbezogener Daten
Erstellt am 15.06.2021 16:49:06 von oholinski in **Wiki-Eintrag**

Verantwortlicher
Erstellt am 15.06.2021 16:48:20 von oholinski in **Wiki-Eintrag**

Transparenz
Erstellt am 15.06.2021 16:48:07 von oholinski in **Wiki-Eintrag**

Telearbeit / Home Office
Erstellt am 15.06.2021 16:47:57 von oholinski in **Wiki-Eintrag**

Nachrichten jetzt ✕

Sie haben 1 neue Meldungen bekommen

Nutzungsanfragen - Historie

Neue Nutzungsanfragen

TrUSD - Dashboard

https://trusd.hk-bs.de:51252/Home/Logged_Index

TrUSD

Hallo cevaoffner! Abmelden

Dashboard | Wissensdatenbank | Nutzungsanfragen | Meldungen 1

Was möchten Sie wissen?

- Datenschutz-Wiki
- Betriebsvereinbarungen
- ADV-Verträge
- Audits/Reviews
- Datenschutzschulungen
- Verfahrensverzeichnis
- Technische und organisatorische Maßnahmen
- Dater

Wissens-Datenbank

Letzte Einträge

Verarbeitungszwecke
Erstellt am 15.06.2021 16:50:48 von oholinski in **Wiki-Eintrag**

Verarbeitung personenbezogener Daten
Erstellt am 15.06.2021 16:49:06 von oholinski in **Wiki-Eintrag**

Verantwortlicher
Erstellt am 15.06.2021 16:48:20 von oholinski in **Wiki-Eintrag**

Transparenz
Erstellt am 15.06.2021 16:48:07 von oholinski in **Wiki-Eintrag**

Telearbeit / Home Office
Erstellt am 15.06.2021 16:47:57 von oholinski in **Wiki-Eintrag**

Sage GmbH
Erstellt am 22.06.2021 08:49:23 von brath in **ADV Vertrag**

Datenschutz-Review
Erstellt am 22.06.2021 08:53:34 von brath in **Audit/Review**

IT-Sicherheitsrichtlinie
Erstellt am 30.06.2021 09:34:44 von cevaoffner in **Betriebsvereinbarung**

Verpflichtungserklärung Datenschutz
30.06.2021 09:34:16 von cevaoffner in **Betriebsvereinbarung**

Impfpass
Erstellt am 16.06.2021 10:04:01 von oholinski in **Betriebsvereinbarung**

gen
16.06.2021 10:02:21 von oholinski in **Betriebsvereinbarung**

Reiseprofil
Erstellt am 16.06.2021 10:00:15 von oholinski in **Betriebsvereinbarung**

lanung
Erstellt am 22.06.2021 09:01:16 von brath in **Datenschutz-Folgenabschätzungen**

Interne Schulung
Erstellt am 22.06.2021 08:58:35 von brath in **Datenschutzschulung**

TrUSD - Index

https://trusd.hk-bs.de:51252/TrusdWikiEntries/Index

TrUSD

Hallo cevaoffner! Abmelden

Dashboard | Wissensdatenbank | Nutzungsanfragen | Meldungen 1

Was möchten Sie wissen?

- Datenschutz-Wiki
- Betriebsvereinbarungen
- ADV-Verträge
- Audits/Reviews
- Datenschutzschulungen
- Verfahrensverzeichnis
- Technische und organisatorische Maßnahmen
- Datenschutz-Folgenabschätzungen

Home / Datenschutz-Wiki

Eintrag erstellen

Arbeitsanweisungen

Arbeitsanweisung Allgemeine Regelungen zu Datenschutz und IT-Sicherheit

Erstellt am 15.06.2021 15:46:10 von oholinski

Arbeitsanweisung E-Mail-Nutzung

Erstellt am 15.06.2021 15:46:36 von oholinski

Arbeitsanweisung Firmennetzwerk und Fernzugriff

Erstellt am 15.06.2021 15:51:22 von oholinski

nweisung Internetnutzung

5.06.2021 15:52:46 von oholinski

Arbeitsanweisung Mobile Datenträger

Wiki

TrUSD - Index

https://trusd.hk-bs.de:51252/TrusdProcedureDirectories/Index

TrUSD

Hallo cevaoffner! Abmelden

Dashboard | Wissensdatenbank | Nutzungsanfragen | Meldungen 1

Was möchten Sie wissen?

- Datenschutz-Wiki
- Betriebsvereinbarungen
- ADV-Verträge
- Audits/Reviews
- Datenschutzschulungen
- Verfahrensverzeichnis
- Technische und organisatorische Maßnahmen
- Daten

Verfahrens-verzeichnis

Home / Verfahrensverzeichnis

Eintrag erstellen

Bewerbermanagement

Bewerbermanagement umfasst den Prozess...

Erstellt am 17.06.2021 10:30:57 von vwagnermueller

Compliance

Compliance umfasst alle Prozesse, die die Ei...

am 17.06.2021 11:44:44 von vwagnermueller

trolling

olling umfasst sämtliche Prozesse, die ...

am 17.06.2021 11:10:08 von vwagnermueller

Customer Relationship Management

TrUSD - Index

https://trusd.hk-bs.de:51252/TrusdTermOfTechnicalAndOrganisationalMeasures/Index

TrUSD

Hallo cevaoffner! Abmelden

Dashboard | Wissensdatenbank | Nutzungsanfragen | Meldungen 1

Was möchten Sie wissen?

- Datenschutz-Wiki
- Betriebsvereinbarungen
- ADV-Verträge
- Audits/Reviews
- Datenschutzschulungen
- Verfahrensverzeichnis
- Technische und organisatorische Maßnahmen
- Datenschutz-Folgenabschätzungen

Home / Technische und organisatorische Maßnahmen

Eintrag erstellen

Automatisierte Verarbeitungsprozesse

Bevorzugung von automatisierten Verarbeit...

Erstellt am 17.06.2021 13:30:34 von vwagnermueller

Benachrichtigung bei Datenpannen

Benachrichtigung von Betroffenen bei Date...

Erstellt am 21.06.2021 09:16:55 von vwagnermueller

veckänderung

ei Weit...

nermueller

Berechtigungskonzept

Technische und organisatorische Maßnahmen

TrUSD - Index

https://trusd.hk-bs.de:51252/PermissionForm/Index

TrUSD

Hallo cevaoffner! Abmelden

Dashboard Wissensdatenbank Nutzungsanfragen Meldungen 1

Was möchten Sie wissen?

Einwilligungshistorie

Neue Anfrage

Verwendungszweck	ID	Antworten bis	Datennutzer	Erhalten am	Status	
Foto für Marketing (inkl. Internetseite), Werbung	3	2021-07-21	mboss	14.07.2021	Einwilligung Erteilt	Löschen

Einwilligungen

TrUSD - Create

https://trusd.hk-bs.de:51252/PermissionForm/Create

TrUSD

Hallo cevaoffner! Abmelden

Dashboard Wissensdatenbank Nutzungsanfragen Meldungen 1

Was möchten Sie wissen?

Einwilligung erstellen

Mitarbeitername

Vera Wagner-Müller (Arbeitnehmer)

Verwendungszweck

Kontext

Antworten bis

27.08.2021

Anhänge

Datei hier hinzufügen...

Status

Einwilligungen – neue Anfrage

TrUSD - Index

https://trusd.hk-bs.de:51252/Notification/Index

TrUSD

Hallo cevaoffner! Abmelden

Dashboard | Wissensdatenbank | Nutzungsanfragen | Meldungen 1

Was möchten Sie wissen?

Meldungszentrum

Neue Meldung erstellen

Erstellt	Titel	Datennutzer	Inhalt	
30.06.2021	Verpflichtungserklärung Datenschutz	cevaoffner	In unserer neuen Verpflichtungserklärung ist der Umgang mit personenbezogenen Daten von Kunden, Partnern, Lieferanten und Mitarbeitern geregelt. Diese liegt in der Wissensdatenbank in der Rubrik: Betriebsvereinbarungen. Jeder Mitarbeiter hat diese Erklärung zur Kenntnis zu nehmen und in seinem Arbeitsbereich entsprechend umzusetzen. Ein eigenhändig unterschriebenes Exemplar ist bei der Geschäftsführung abzugeben.	Löschen
30.06.2021	Ankündigung Kontrolle Internet-Traffic	cevaoffner	Das Internet-Datenvolumen ist in den letzten Wochen extrem stark gestiegen. Um auszuschließen, dass dies durch private Internetnutzung verursacht wird, werden wir ab sofort den Traffic stärker kontrollieren und bei Bedarf geeignete Maßnahmen einleiten. Eure Geschäftleitung	Löschen
30.06.2021	Datenschutz-Dashboard	cevaoffner	In unserem Mitarbeiter-Dashboard rund um Datenschutzthemen gibt es jetzt neue Funktionen. Neben der Wissensdatenbank steht hier nun auch ein Meldesystem und ein Einwilligungsmanagement zur Verfügung. Mehr erfahrt Ihr demnächst in einer kleinen Einweisung/Aufbauschulung zum Dashboard.	Löschen

Meldungen

Agenda

TrUSD

I. **Big Picture**
Die Ideen hinter dem Projekt »TrUSD«.

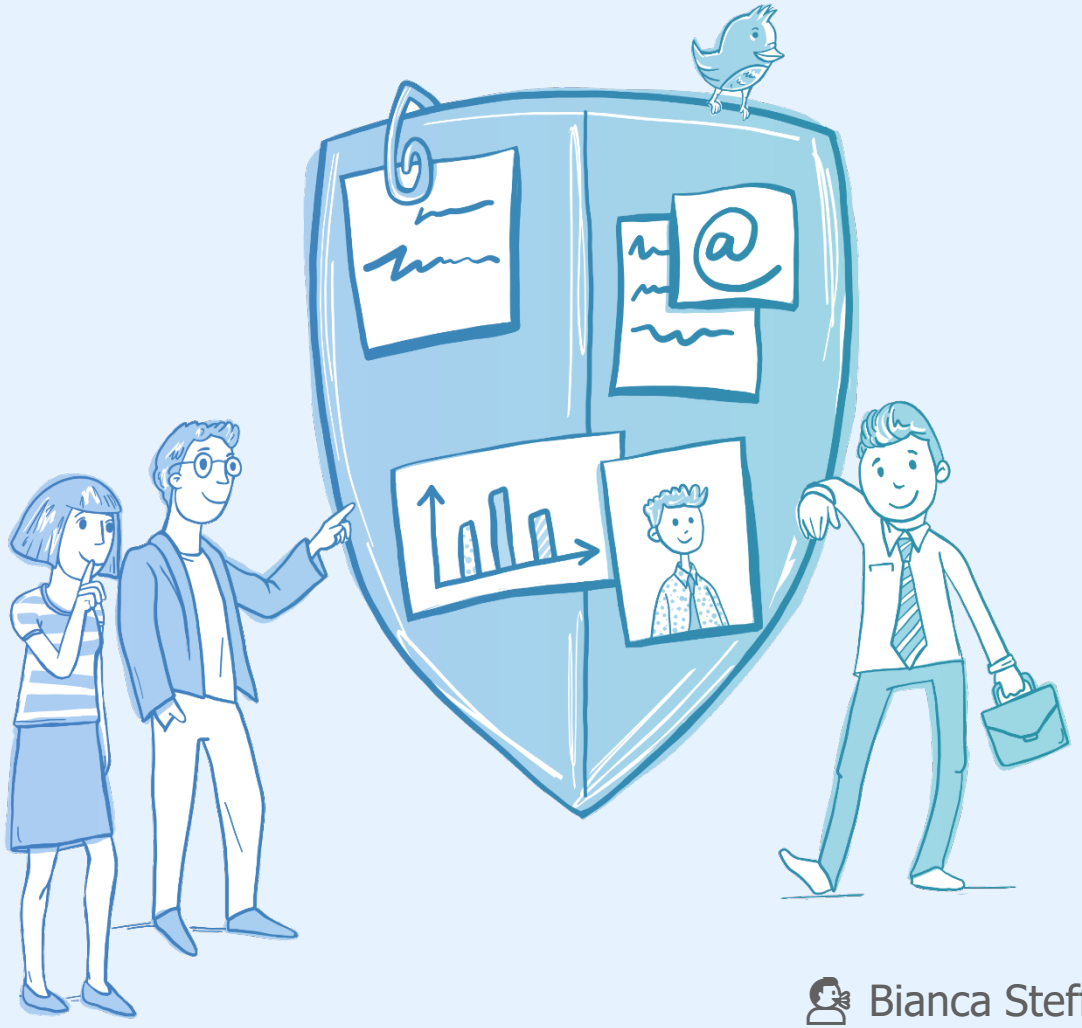
II. **Umsetzungsbeispiele**
So können Privacy-Dashboards in der Praxis gestaltet sein.

III. **Werkzeugkasten**
So können Sie das Privacy-Dashboard auf Ihr Unternehmen maßschneidern.

IV. **Lessons Learned**
(Überraschende) Erkenntnisse aus dem Projekt.

V. **Diskussionsrunde**
Offene Punkte, Ausblick.

Anforderungen, Rahmen-bedingungen



Bianca Steffes bianca.steffes@uni-saarland.de

Datenschutzrechtliche Einordnung

Rechtliche Vorgaben und Leitlinien

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Ziele von TrUSD

TrUSD: Transparente und selbstbestimmte Ausgestaltung der Datennutzung im Unternehmen

- Transparenz
- (Informationelle) Selbstbestimmung
- Technische und organisatorische Maßnahmen

Anforderung an die Datenverarbeitung

§ 26 Abs. 5 BDSG fordert insbesondere das Einhalten der Grundsätze für die Verarbeitung personenbezogener Daten (Art. 5, Abs. 1 DSGVO)

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz (lit. a)
- Zweckbindung (lit. b)
- Datenminimierung (lit. c)
- Richtigkeit (lit. d)
- Speicherbegrenzung (lit. e)
- Integrität und Vertraulichkeit (lit. f)

Transparenz

„Personenbezogene Daten müssen […] in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden“ Art. 5 Abs. 1 lit. a DSGVO

Nur eine Person die weiß, wer, bei welcher Gelegenheit, was, über sie weiß, kann frei und selbstbestimmt planen und entscheiden.

Informationspflichten

Art. 13 DSGVO
Art. 14 DSGVO

Auskunftsrecht

Art. 15 DSGVO

Rechte der betroffenen Person

Art. 16 DSGVO
Art. 17 DSGVO
Art. 18 DSGVO
Art. 21 DSGVO

Informationelle Selbstbestimmung

- Jeder hat das Recht, selbst über die Verwendungen seiner personenbezogenen Daten entscheiden zu können.

- Durch die Transparenz wird eine informierte Selbstbestimmung ermöglicht.

- Das Recht auf informationelle Selbstbestimmung ist nicht im Gesetzestext verankert, sondern formt sich aus Art. 1 Abs. 1, i. V. m. Art. 2 Abs. 1 GG. Zudem sind personenbezogene Daten nach Art. 8 der EU-Grundrechtecharte geschützt.

Zulässigkeit der Nutzung

Nach Art. 88 DSGVO darf der deutsche Gesetzgeber die Zulässigkeit der Datennutzung im Beschäftigungskontext spezifizieren.

<u>§ 26 BDSG: Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses</u>

- Abs. 1: Personenbezogene Daten dürfen u. a. verarbeitet werden, wenn
  - sie für Entscheidung über die Begründung, die Durchführung oder Beendigung eines Beschäftigungsverhältnisses notwendig sind
  - sie für die Ausübung oder Erfüllung von bestimmten rechtlichen Pflichten benötigt werden

Mögliche notwendige Datenverarbeitungen

Beginn

Stammdaten (Name, Adresse, etc.)

Ärztliche Untersuchungen

Eignungstests

Datenerhebung bei Dritten (bspw. früherer Arbeitsgeber / soziale Netzwerke)

…

Dauer

Gesundheitsdaten

Biometrische Daten

Nutzung von Telekommunikations-diensten

Aufzeichnungen aus der Videoüberwachung

…

Ende

Daten der betrieblichen Altersvorsorge

Daten der betrieblichen Statistik

…

Zulässigkeit der Nutzung

Nach Art. 88 DSGVO darf der deutsche Gesetzgeber die Zulässigkeit der Datennutzung im Beschäftigungskontext spezifizieren.

<u>§ 26 BDSG: Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses</u>

- Abs. 2: Personenbezogene Daten dürfen verarbeitet werden, wenn
  - die betroffene Person eine Einwilligung erteilt hat.

Mögliche einwilligungspflichtige Datenverarbeitungen

Daten zur Außendarstellung

(z. Bsp. Fotos in Pressemitteilungen oder Social Media oder der eigenen Webseite)

Daten zur Verbesserung des Kundenkontaktes

(z. Bsp. Weitergabe von Kontaktdaten an den Kunden)

Daten für (unternehmensinterne) Forschungsprojekte

(z. Bsp. Adressdaten für demographische Analysen)

…

Technische und organisatorische Schutzmaßnahmen

Privacy by design

"Unter Berücksichtigung […] der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken […] trifft der Verantwortliche sowohl **zum Zeitpunkt der Festlegung der Mittel** […] geeignete **technische und organisatorische Maßnahmen** […], die dafür **ausgelegt sind**, die **Datenschutzgrundsätze** […] **wirksam umzusetzen** […]." (Art.25, Abs. 1 DSGVO)

Privacy by default

Der Verantwortliche trifft geeignete **technische und organisatorische Maßnahmen**, die sicherstellen, dass **durch Voreinstellung** nur personenbezogene Daten, deren Verarbeitung **für den jeweiligen bestimmten Verarbeitungszweck erforderlich** ist, verarbeitet werden. (Art. 25, Abs. 2 DSGVO)

Weiterführende Informationen

Was?	Wo?
Datenschutzrechtliche Grundlagen	• Deliverable 7.1 – Bericht über inhaltliche Anforderungen und Anforderungen an die Datenverarbeitung an das Privacy Dashboard aus Sicht des Datenschutzrechts • Christian K. Bosse, Aljoscha Dietrich, Patricia Kelbert, Hagen Küchler, Hartmut Schmitt, Jan Tolsdorf, Andreas Weßner: Beschäftigtendatenschutz: Rechtliche Anforderungen und technische Lösungskonzepte. In: Erich Schweighofer, Walter Hötzendorfer, Franz Kummer, Ahti Saarenpää (Hrsg.): Tagungsband des 23. Internationalen Rechtsinformatik Symposions IRIS 2020
Gefahren für den Datenschutz im Beschäftigungsverhältnis	• Hartmut Schmitt, Christian K. Bosse, Aljoscha Dietrich, Svenja Polst: Wie ich an deine Daten kam oder Dark Patterns und Phishing im Beschäftigtenkontext. In: Erich Schweighofer, Stefan Eder, Philip Hanke, Franz Kummer, Ahti Saarenpää (Hrsg.): Cybergovernance: Tagungsband des 24. Internationalen Rechtsinformatik Symposions IRIS 2021, S. 293–302. Bern: Editions Weblaw.
Selbstbewertungsinstrument für den Datenschutz im eigenen Unternehmen	• Link: https://datenschutz-check.ita-befragung.de/

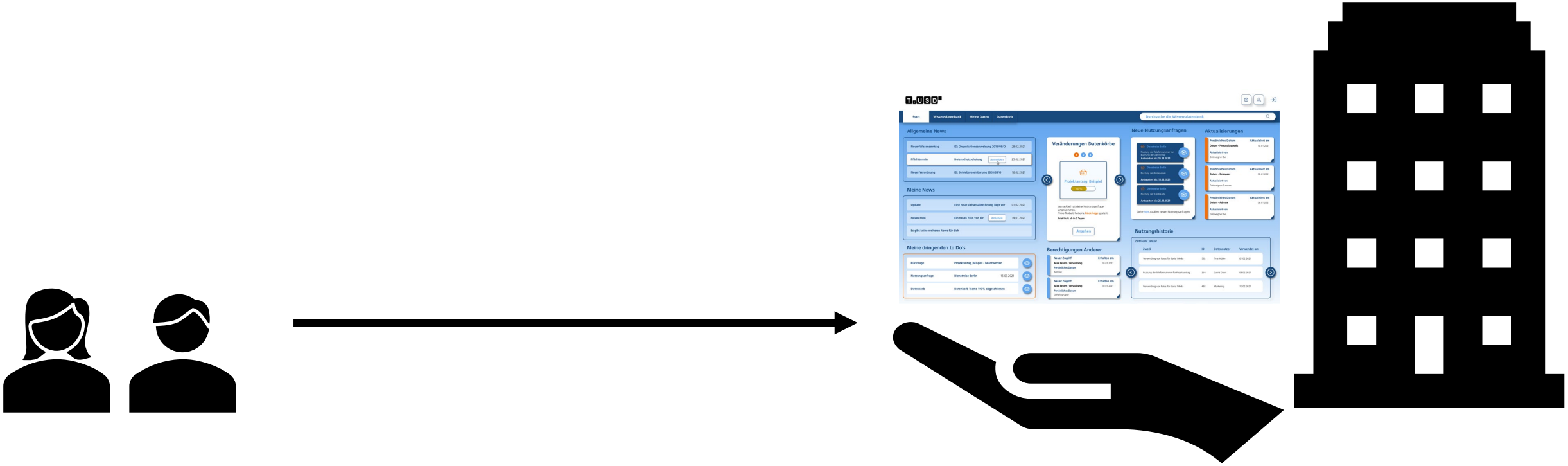
Modelle

Jan Tolsdorf jan.tolsdorf@h-brs.de

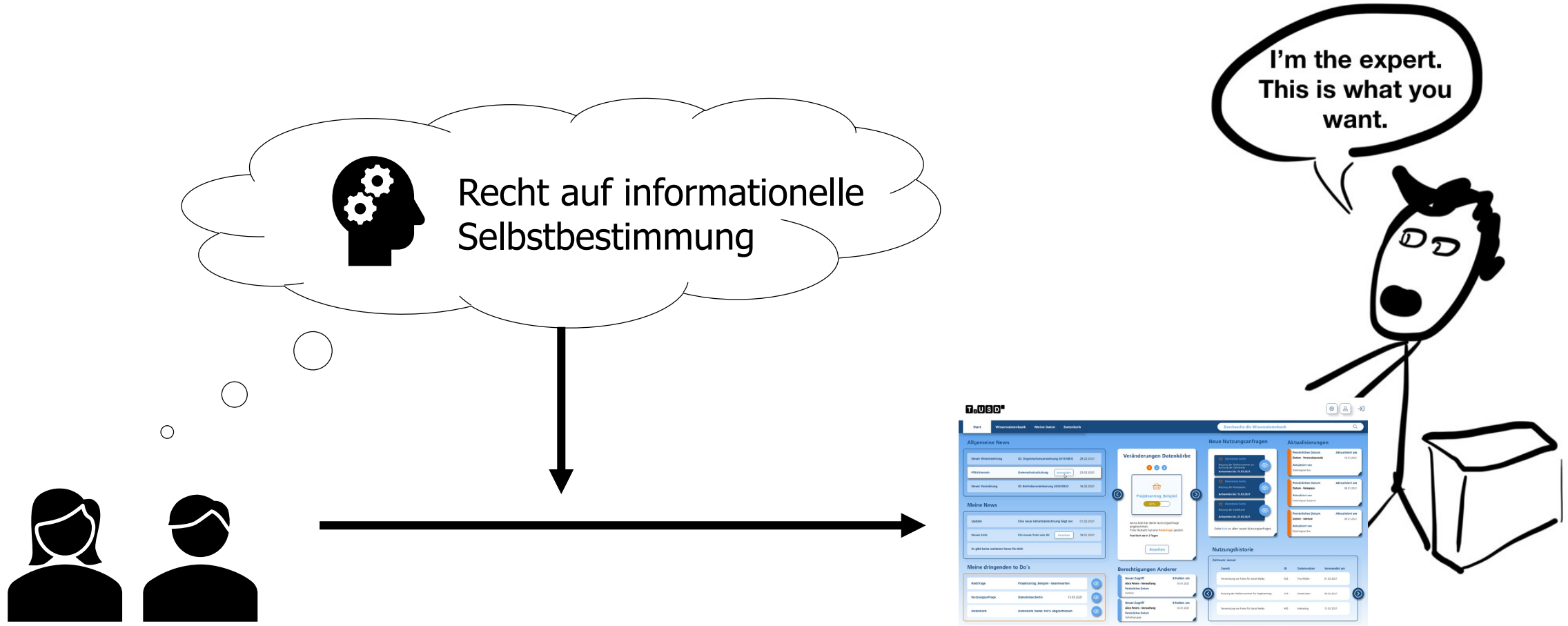
Mentale Modelle des Rechts auf informationelle Selbstbestimmung am Arbeitsplatz

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

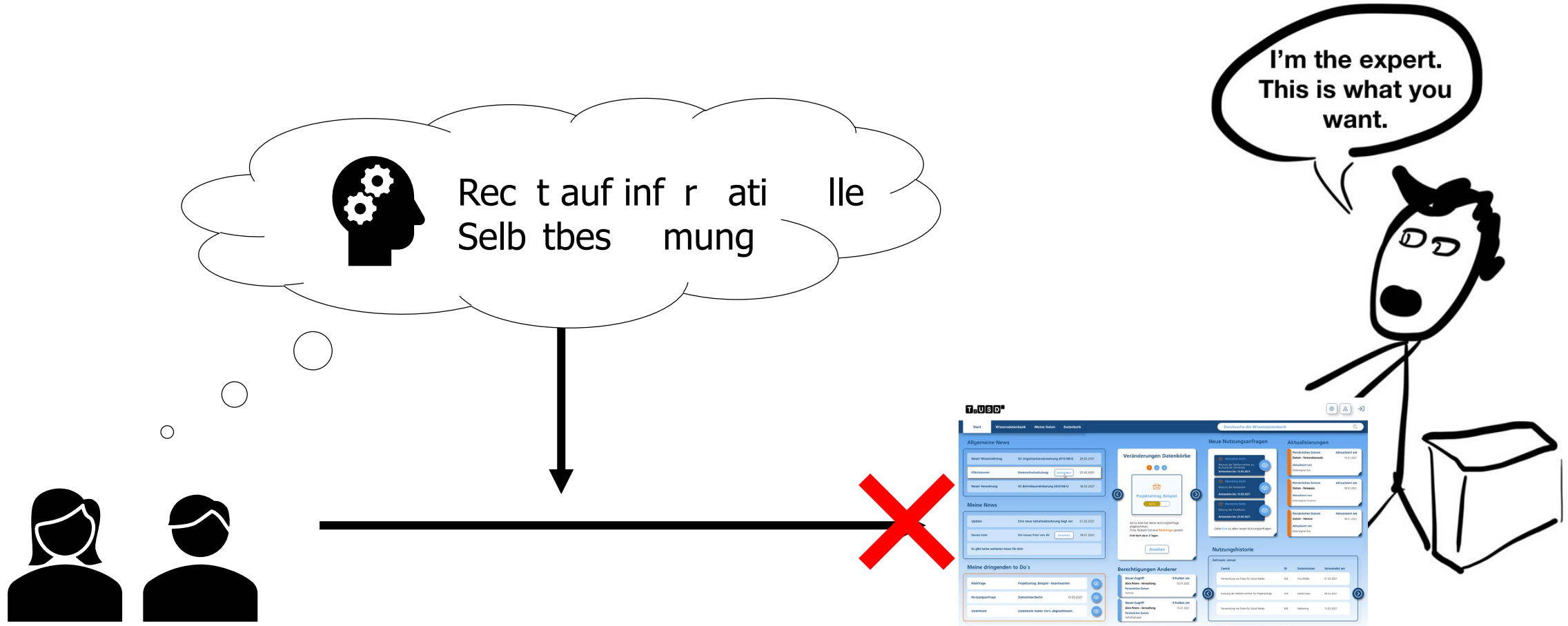
Hintergrund



Hintergrund

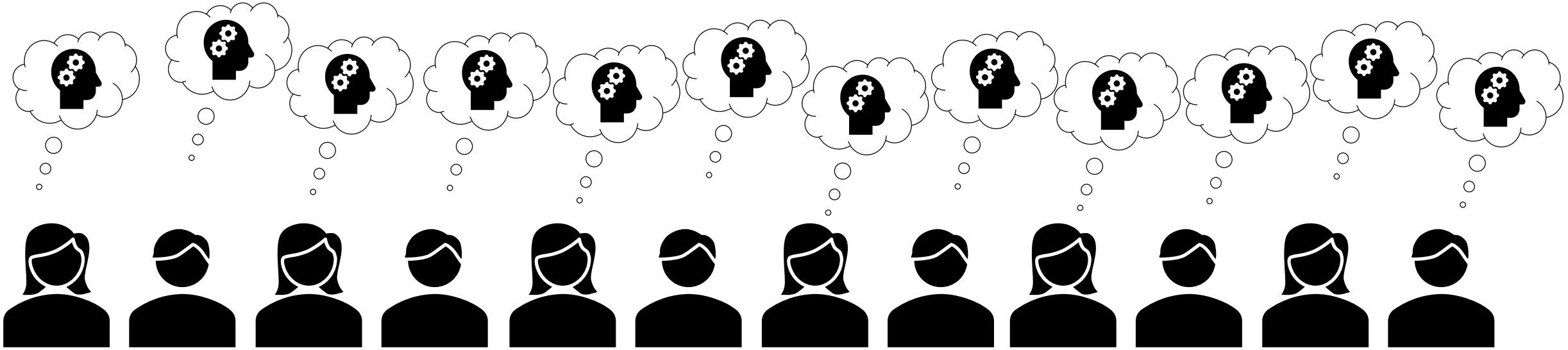


Hintergrund



Hintergrund

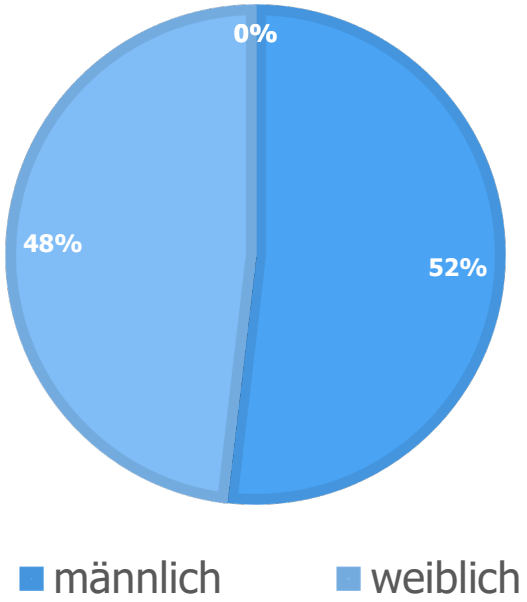
Was sind die mentalen Modelle des Rechts auf informationelle Selbstbestimmung am Arbeitsplatz?



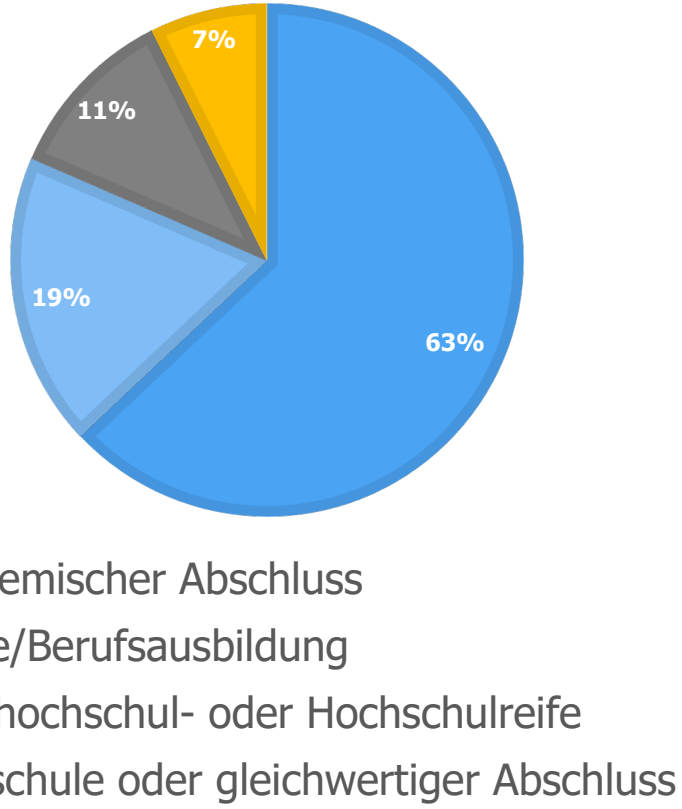
Demographische Angaben

27

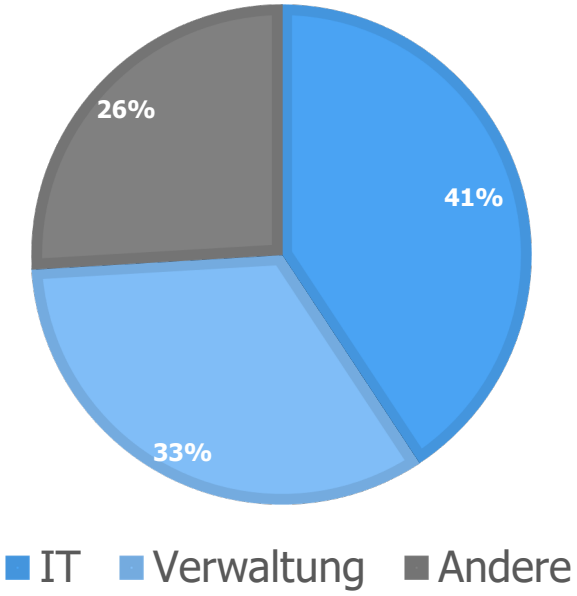
GESCHLECHTERVERHÄLTNIS



BILDUNGSABSCHLÜSSE



BERUFLICHER HINTERGRUND



Verständnis Begriffe

Daten

Informationen

Personenbezogene Daten

Personenbeziehbare Daten

Persönliche Daten

Private Daten

Verständnis Begriffe

Daten

Informationen

Personenbezogene Daten

Personenbeziehbare Daten

Persönliche Daten

Private Daten

- Keine Referenz auf eine Person;
- Sehr relevant für die tägl. Arbeit;

Verständnis Begriffe

Daten

Informationen

Personenbezogene Daten

Personenbeziehbare Daten

Persönliche Daten

Private Daten

- Klare Referenz auf eine Person;
- Eindeutige Identifikation einer Person;
- Eindeutiger indirekter Personenbezug;

Verständnis Begriffe

Daten

Informationen

Personenbezogene Daten

Personenbeziehbare Daten

Persönliche Daten

Private Daten

- Sehr sensibel;
- Schutzbedürftig;
- Keine Relevanz für das Beschäftigtenverhältnis;

Verständnis Begriffe

Daten

Informationen

Personenbezogene Daten

Personenbeziehbare Daten

Persönliche Daten

Private Daten

- Uneindeutig!

  Private Daten ←→ Daten

Mentale Modelle

Modell	Prinzipienreiter	Datenfluss-besorgte Protektionisten	Kontrollsuchende Pragmatiker

Mentale Modelle

Modell	Prinzipienreiter	Datenfluss-besorgte Protektionisten	Kontrollsuchende Pragmatiker
Ziel			
Selbstbestimmung			
Transparenz			
Einschränkungen			

Mentale Modelle

Modell	Prinzipienreiter	Datenfluss-besorgte Protektionisten	Kontrollsuchende Pragmatiker
Ziel	*Unspezifisch*	Schutz der Privatheit vor Externen & Internen	Preisgabe auf notwendige Daten reduzieren
Selbstbestimmung			
Transparenz			
Einschränkungen			

Mentale Modelle

Modell	Prinzipienreiter	Datenfluss-besorgte Protektionisten	Kontrollsuchende Pragmatiker
Ziel	*Unspezifisch*	Schutz der Privatheit vor Externen & Internen	Preisgabe auf notwendige Daten reduzieren
Selbstbestimmung	- Ex-post Kontrolle - Mitbestimmung über Verarbeitung	- Ex-ante Kontrolle - Mitbestimmung Empfänger und Teilen von Daten	- Ex-ante Kontrolle - Bestimmen über Preisgabe - Forderung nach Akzeptanz Dritter
Transparenz			
Einschränkungen			

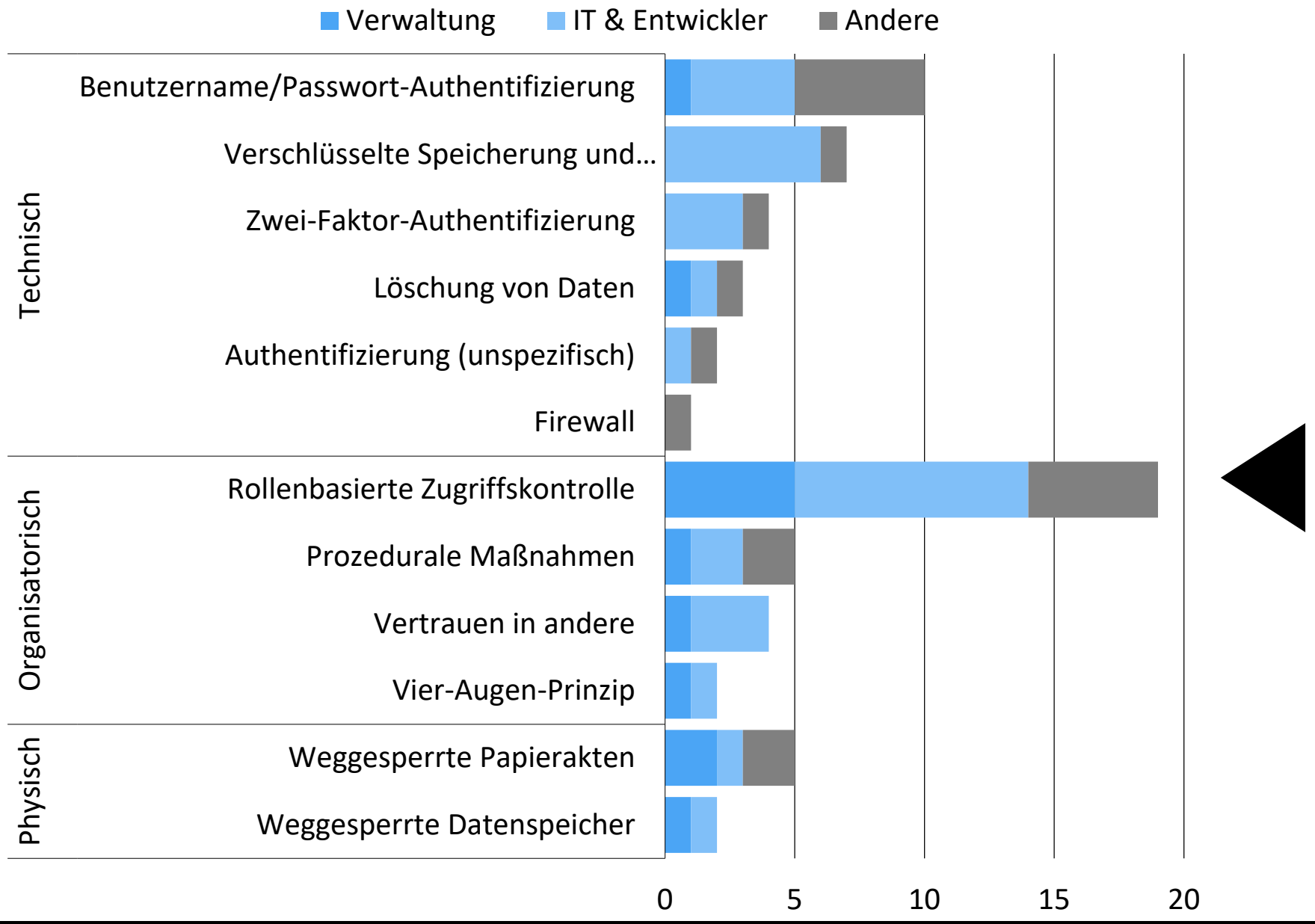
Mentale Modelle

Modell	Prinzipienreiter	Datenfluss-besorgte Protektionisten	Kontrollsuchende Pragmatiker
Ziel	*Unspezifisch*	Schutz der Privatheit vor Externen & Internen	Preisgabe auf notwendige Daten reduzieren
Selbstbestimmung	- Ex-post Kontrolle - Mitbestimmung über Verarbeitung	- Ex-ante Kontrolle - Mitbestimmung Empfänger und Teilen von Daten	- Ex-ante Kontrolle - Bestimmen über Preisgabe - Forderung nach Akzeptanz Dritter
Transparenz	Wertschätzung Transparenz	Ignorieren Transparenz	Ignorieren Transparenz
Einschränkungen			

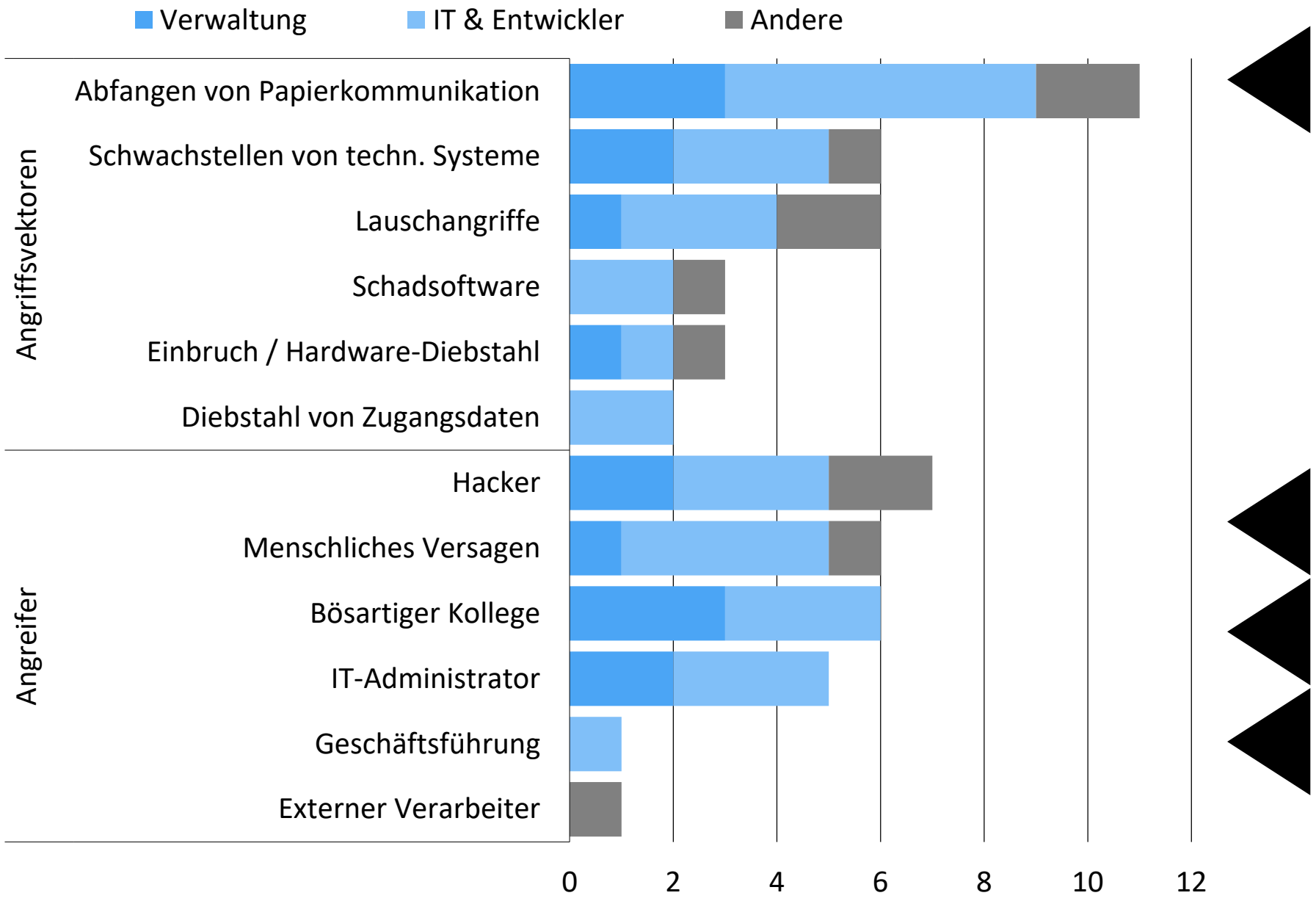
Mentale Modelle

Modell	Prinzipienreiter	Datenfluss-besorgte Protektionisten	Kontrollsuchende Pragmatiker
Ziel	*Unspezifisch*	Schutz der Privatheit vor Externen & Internen	Preisgabe auf notwendige Daten reduzieren
Selbstbestimmung	- Ex-post Kontrolle - Mitbestimmung über Verarbeitung	- Ex-ante Kontrolle - Mitbestimmung Empfänger und Teilen von Daten	- Ex-ante Kontrolle - Bestimmen über Preisgabe - Forderung nach Akzeptanz Dritter
Transparenz	Wertschätzung Transparenz	Ignorieren Transparenz	Ignorieren Transparenz
Einschränkungen	Uneingeschränkte Gültigkeit ISB	ISB eingeschränkt durch Angestellten-dasein	Akzeptanz Einschränkungen / Tausch ISB gegen Beschäftigung

Mentale Modelle – Schutzmechanismen



Mentale Modelle – Angreifermodelle

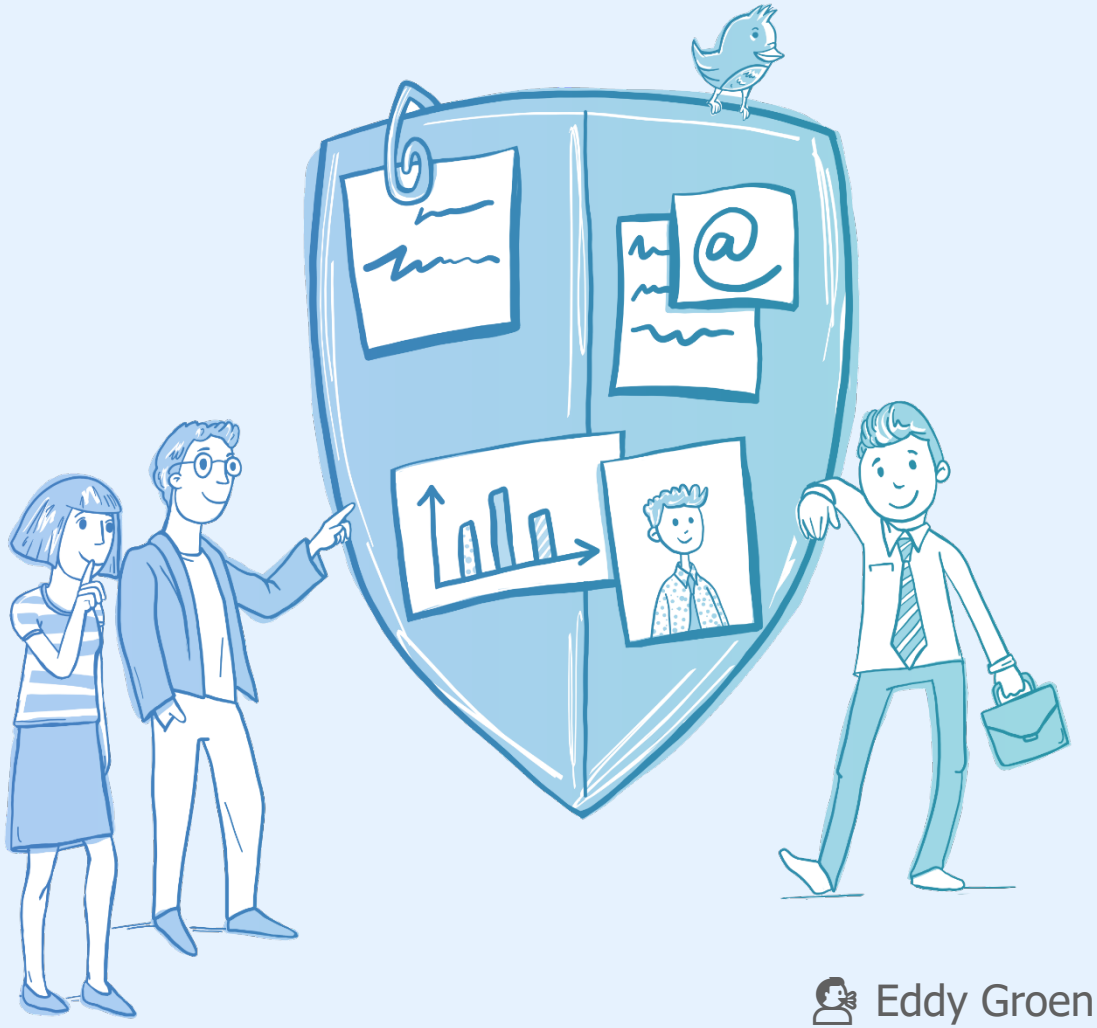


Weiterführende Informationen

Was?	Wo?
Mentale Modelle des Rechts auf informationelle Selbstbestimmung am Arbeitsplatz	• Deliverable 2.2 – Mentale Modelle • J. Tolsdorf, F. Dehling, D. Reinhardt, und L. Lo Iacono, „Exploring Mental Models of Informational Self-Determination of Office Workers in Germany", *Proceedings on Privacy Enhancing Technologies (PoPETs)*, Bd. 2021, Nr. 3, S. 5–27, 2021. • J. Tolsdorf und F. Dehling, „In Our Employer We Trust: Mental Models of Office Workers' Privacy Perceptions", in *Financial Cryptography and Data Security Workshops (FC Workshops)*, 2020, S. 122–136.
Mentale Modelle und Privacy Dashboards	• J. Tolsdorf, F. Dehling, und L. Lo Iacono, „Take Back Control! The Use of Mental Models to Develop Privacy Dashboards", *ITG News*, Bd. 8, Nr. 3, S. 15–20, Okt. 2020.

Anforderungen, Rahmen-bedingungen

TrUSD



Eddy Groen eduard.groen@iese.fraunhofer.de

Entscheidende Kontextfaktoren bei der Entwicklung von Privacy-Dashboards

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Welche Rahmenbedingungen sollen bei der Entwicklung eines Privacy-Dashboards berücksichtigt werden?

Rahmenbedingungen

Qualitätsanforderungen | Empfehlungen | Klärungspunkte

- Anforderungen für das Privacy-Dashboard sind verallgemeinert aufbereitet
  - Verwendbar für die Entwicklung für bzw. durch verschiedene Organisationen
  - Entwurfs- und Entwicklungs**entscheidungen** sind kontextbezogen zu treffen

- Als Hilfestellung beschreiben wir drei Arten von Rahmenbedingungen:
  - Übergreifende **Qualitätsanforderungen** nach ISO 25010 zur Priorisierung
  - Erfahrungsbasierte **Empfehlungen**, die wir als Best Practices mitgeben
  - Identifizierte **Klärungspunkte** für die Definition von Randbedingungen

Rahmenbedingungen

TrUSD

Qualitätsanforderungen | Empfehlungen | Klärungspunkte

Qualitätsmodell

Datenqualität

Produktqualität

- Funktionale Tauglichkeit
- Performanz !
- Kompatibilität !
- Benutzerfreundlichkeit !
  - Erlernbarkeit !
    Bildungsangebote
- Zuverlässigkeit !
- Sicherheit !
- Datenschutz !
- Wartbarkeit !
- Übertragbarkeit

Nutzungsqualität

Prozessqualität

Strukturqualität

- Ausgewählt sind „nur" die Merkmale, für die wesentliche Qualitäten über Anforderungen gewährleistet werden sollen
  - Das betrifft fast alle Qualitätsmerkmale

- Logische Konsequenz der Verarbeitung personenbezogener Daten

Rahmenbedingungen

Qualitätsanforderungen | **Empfehlungen** | Klärungspunkte

Zuständigkeiten zuweisen

Veränderungs-management begleiten

Zertifizieren lassen

Regelmäßige Audits durchführen

ORGANISATION

QUALITÄT

TECHNOLOGIE

INFRASTRUKTUR

Standardisierte Schnittstellen verwenden

Technologie sorgfältig auswählen

Technologieanbieter sorgfältig auswählen

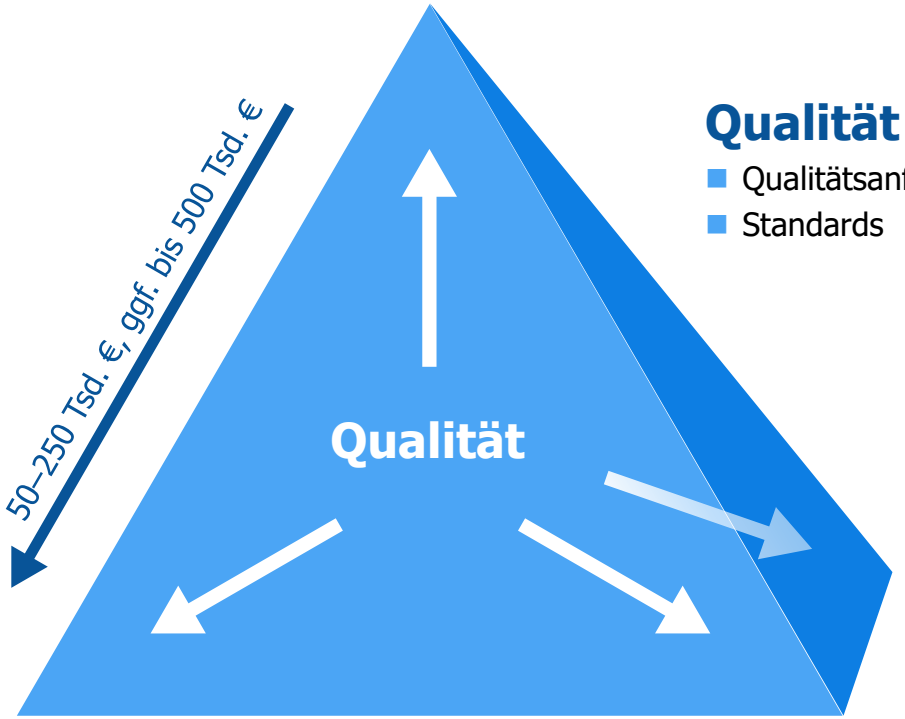
Vereinbarungen mit dem Technologie-anbieter treffen

Rahmenbedingungen

Qualitätsanforderungen | Empfehlungen | **Klärungspunkte**

Umfang

- Funktionsumfang
- Unterstützte Sprachen
- Umfang Datenverarbeitung
- Infrastruktur des PDB



Qualität

- Qualitätsanforderungen
- Standards

Kontext

- Infrastruktur der Organisation (System- und Prozesslandschaft)
- Rechtliche Rahmenbedingungen
- Entwicklungsprozess
- Entwicklungswerkzeuge
- Programmiersprache

Kosten

- Entwicklungsbudget
- Wartungskosten

Zeit

- Entwicklungsdauer

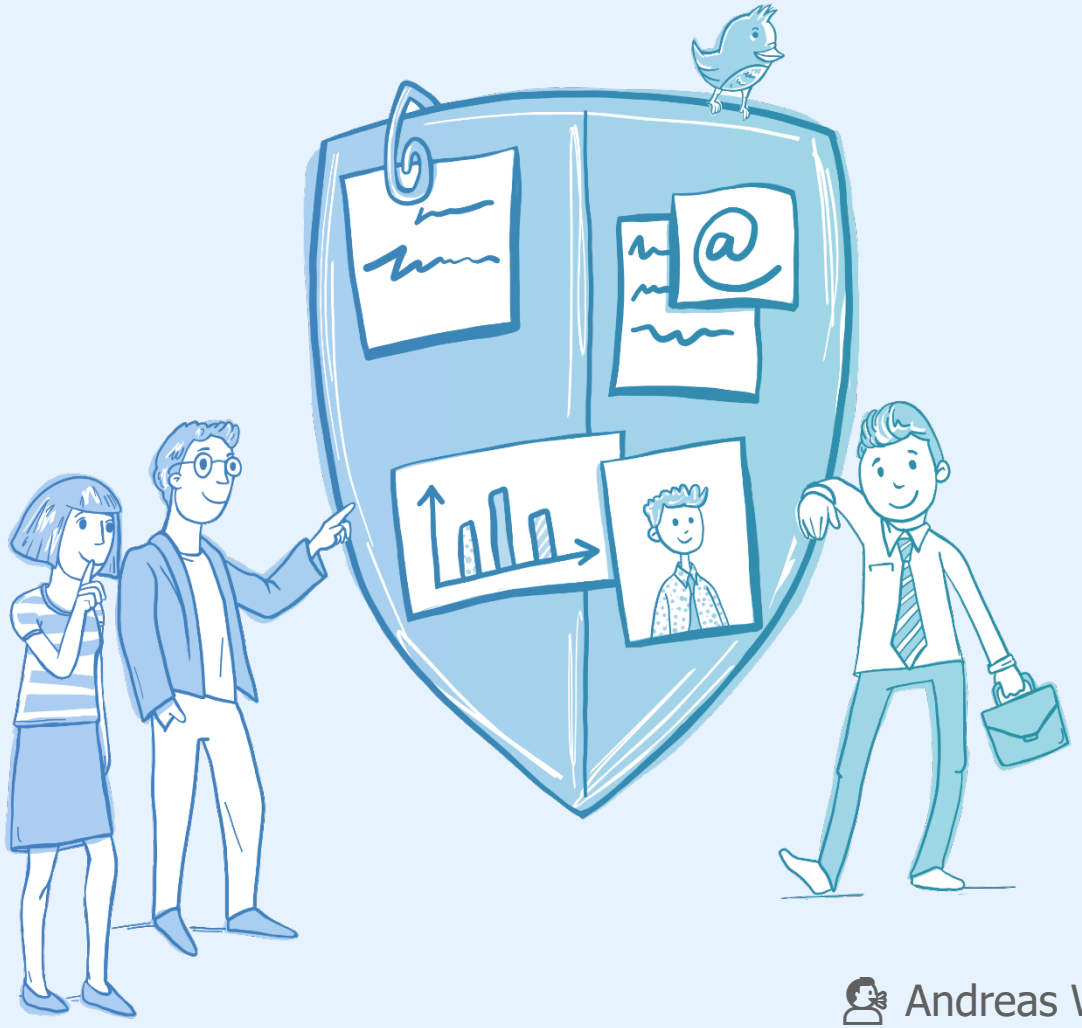
- Diese Entscheidungen sind möglichst frühzeitig festzulegen
  - Eingrenzung der Entwurfsentscheidungen

Fazit

- Ein Privacy-Dashboard dient dem Ziel, **Datenschutz** zu **steigern**
  Selbstbestimmung durch den Dateneigner; eindeutige Einwilligungen für den Datennutzer
  - Weil es letzten Endes Datenschutzverletzungen vorbeugen soll, darf ein Privacy-Dashboard niemals die Ursache einer **Datenschutzverletzung** sein (z. B. durch Fehler bzw. Lücken in der Software)
- Rahmenbedingungen helfen, den **Projektscope** & **Erfolgskriterien** festzulegen
  - Sie schaffen Raum für eine **nachhaltige Qualitätssicherung**
    In der Entwicklung und während des Betriebs

Werkzeuge

TrUSD



Andreas Weßner andreas.wessner@ita-kl.de

Selbstbewertungsinstrument für den Beschäftigtendatenschutz

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Welchen Nutzen hat ein Selbstbewertungsinstrument?

Nutzen und Zielgruppe

- Sensibilisierung bzgl. der organisationalen Herausforderungen bei der Verarbeitung von Beschäftigtendaten
- Analyse und Bewertung des Entwicklungsstandes der Organisation im Kontext der Verarbeitung von Beschäftigtendaten
- Unterstützung beim Erkennen konkreter Handlungsbedarfe bei unzureichender Umsetzung des Beschäftigtendatenschutzes
- Hilfestellung für die Weiterentwicklung des Beschäftigtendatenschutzes in der Organisation
- Zielgruppe: Geschäftsführung, Datenschutzbeauftragte, Arbeitnehmervertretungen

Umsetzung

- Rahmendaten Organisation
- Verarbeitungstätigkeiten
- Grundsätze der Verarbeitung
- Betroffenenrechte
- Technische und organisatorische Maßnahmen
- Meldepflichten und Datenschutzverletzungen
- Leistungsmessung und Überwachung

Online Selbstbewertung

20 Minuten

50 Fragen

Direkte Auswertung

TrUSD

Selbstbewertungsinstrument für den Beschäftigtendatenschutz

Auswertung

Übersicht drucken

Vielen Dank für die Nutzung unseres Online-Checks zur Einschätzung des Beschäftigtendatenschutzes in Unternehmen, der im Rahmen des Forschungsprojekts TrUSD - Transparente und selbstbestimmte Datennutzung in Unternehmen entwickelt wurde. Anhand Ihrer Antworten rund um das Themenfeld Beschäftigtendatenschutz und zu dessen Umsetzung erhalten Sie nachfolgend eine erste Bewertung für Ihr Unternehmen. Insbesondere in einen derart komplexen Themenfeld kann eine Online-Selbstbewertung jedoch nur Anhaltspunkte liefern und keine Rechtsberatung ersetzen.

Ihr Gesamtergebnis:

Einschätzung:
Ihr Unternehmen hat bereits einige Anstrengungen unternommen, um den Anforderungen eines effektiven Beschäftigtendatenschutzes gerecht zu werden. Wir hoffen, Ihnen durch die Anwendung dieses Selbstbewertungsinstruments einige weitere Anhaltspunkte zu geben, um Sie dabei zu unterstützen, den Anforderungen des Beschäftigtendatenschutzes in Ihrem Unternehmen zukünftig noch besser gerecht werden zu können.

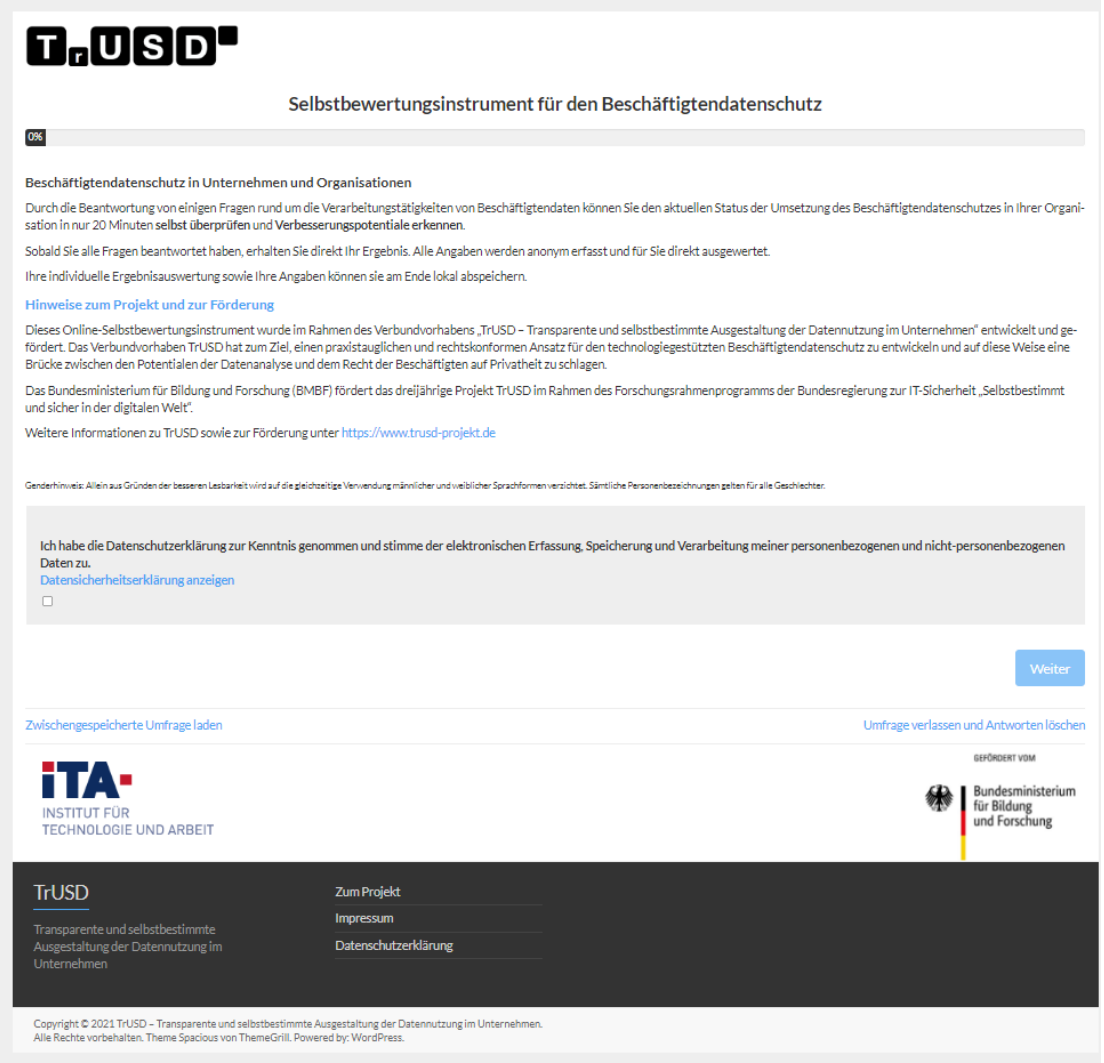
Die **Grundsätze der Verarbeitung von Beschäftigtendaten** sind Ihnen bereits teilweise bekannt, werden in Ihrem Unternehmen aber noch nicht umfassend umgesetzt. Potential besteht darüber hinaus häufig hinsichtlich Art und Umfang des möglichen Nachweises der umfassenden Beachtung dieser Grundsätze, woraus sich auch in Ihrem Unternehmen ggf. noch Optimierungsmöglichkeiten ergeben könnten.

Bei der Wahrnehmung ihrer **Betroffenenrechte** werden die Beschäftigten in Ihrem Unternehmen bereits gut unterstützt. Dieser Unterstützung der Beschäftigten bei der Wahrnehmung der Betroffenenrechte kommt im Beschäftigtendatenschutz eine große Bedeutung zu. Dazu gehören die Information, Sensibilisierung und Qualifizierung der Beschäftigten, die erforderlich ist, damit diese Ihre Rechte überhaupt informiert und selbstbestimmt wahrnehmen können.
Dies gilt umso mehr, wenn es das Ziel des Unternehmens ist, Beschäftigtendaten unter bestimmten Voraussetzungen und mit Zustimmung der Mitarbeiter auch für die Optimierung betrieblicher Prozesse zu nutzen. Das Weiteren ist diese Unterstützung aus arbeitswissenschaftlicher Perspektive entscheidend für um einen fairen Ausgleich der Interessen des Arbeitgebers wie auch der Beschäftigten und nicht zuletzt maßgeblich dafür, wie sich die Kenntnis von der Art und Weise der Verarbeitung ihrer Beschäftigtendaten bei den Beschäftigten auf ihre Arbeitsweisen, ihr Verhalten am Arbeitsplatz oder die Arbeitgeber-/Arbeitnehmerbeziehung insgesamt auswirkt.

In Ihrem Unternehmen wurden zum Teil bereits **technische und organisatorische Maßnahmen (TOM)** ergriffen, um die Schutzziele der DSGVO zu erreichen, den Umfang der verarbeiteten Beschäftigtendaten zu reduzieren und diese zu schützen.
In diesem Zusammenhang geht es aus arbeitswissenschaftlicher Perspektive nicht zuletzt auch darum, ein realistisches Bild von den Schutz-, Selbstbestimmungs- und Transparenzbedarfen der Beschäftigten in der Organisation zu erhalten, um auch den spezifischen Anforderungen der Beschäftigten in Ihrem Unternehmen gerecht zu werden.

Ergänzende Hinweise:
- Bei allen Themen rund um den Beschäftigtendatenschutz - ebenso wie bei allen anderen die Beschäftigten betreffenden Themen - ist es aus arbeitswissenschaftlicher Sicht sehr empfehlenswert und rechtlich zum Teil sogar unbedingt erforderlich, den **Betriebsrat** möglichst frühzeitig und umfassend einzubeziehen.

Link



TrUSD

Selbstbewertungsinstrument für den Beschäftigtendatenschutz

0%

Beschäftigtendatenschutz in Unternehmen und Organisationen

Durch die Beantwortung von einigen Fragen rund um die Verarbeitungstätigkeiten von Beschäftigtendaten können Sie den aktuellen Status der Umsetzung des Beschäftigtendatenschutzes in Ihrer Organisation in nur 20 Minuten **selbst überprüfen** und **Verbesserungspotentiale erkennen**.

Sobald Sie alle Fragen beantwortet haben, erhalten Sie direkt Ihr Ergebnis. Alle Angaben werden anonym erfasst und für Sie direkt ausgewertet.

Ihre individuelle Ergebnisauswertung sowie Ihre Angaben können sie am Ende lokal abspeichern.

Hinweise zum Projekt und zur Förderung

Dieses Online-Selbstbewertungsinstrument wurde im Rahmen des Verbundvorhabens „TrUSD – Transparente und selbstbestimmte Ausgestaltung der Datennutzung im Unternehmen" entwickelt und gefördert. Das Verbundvorhaben TrUSD hat zum Ziel, einen praxistauglichen und rechtskonformen Ansatz für den technologiegestützten Beschäftigtendatenschutz zu entwickeln und auf diese Weise eine Brücke zwischen den Potentialen der Datenanalyse und dem Recht der Beschäftigten auf Privatheit zu schlagen.

Das Bundesministerium für Bildung und Forschung (BMBF) fördert das dreijährige Projekt TrUSD im Rahmen des Forschungsrahmenprogramms der Bundesregierung zur IT-Sicherheit „Selbstbestimmt und sicher in der digitalen Welt".

Weitere Informationen zu TrUSD sowie zur Förderung unter https://www.trusd-projekt.de

Genderhinweis: Allein aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche Personenbezeichnungen gelten für alle Geschlechter.

Ich habe die Datenschutzerklärung zur Kenntnis genommen und stimme der elektronischen Erfassung, Speicherung und Verarbeitung meiner personenbezogenen und nicht-personenbezogenen Daten zu.
Datensicherheitserklärung anzeigen

Weiter

Zwischengespeicherte Umfrage laden

Umfrage verlassen und Antworten löschen

iTA INSTITUT FÜR TECHNOLOGIE UND ARBEIT

GEFÖRDERT VOM Bundesministerium für Bildung und Forschung

TrUSD

Transparente und selbstbestimmte Ausgestaltung der Datennutzung im Unternehmen

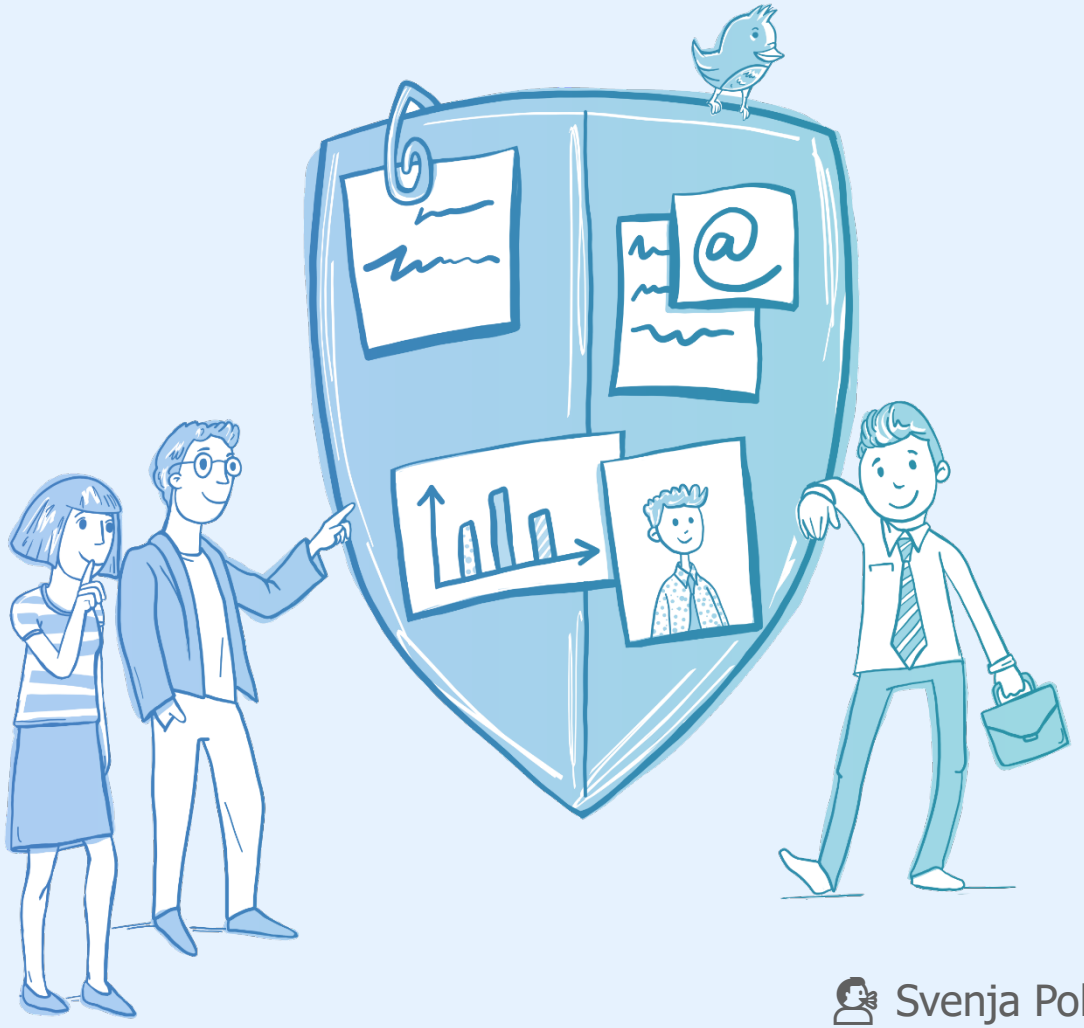
Zum Projekt
Impressum
Datenschutzerklärung

Copyright © 2021 TrUSD – Transparente und selbstbestimmte Ausgestaltung der Datennutzung im Unternehmen.
Alle Rechte vorbehalten. Theme Spacious von ThemeGrill. Powered by: WordPress.

https://datenschutz-check.ita-befragung.de

Anforderungen, Rahmen-bedingungen

TrUSD



Svenja Polst svenja.polst@iese.fraunhofer.de

Erstellen eines unternehmensspezifischen Anforderungskatalogs

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Wieso sieht das Privacy-Dashboard so aus?

Der Werkzeugkasten als Grundlage

TrUSD-Werkzeugkasten

Demonstratoren	Wissensdatenbank und Einwilligungsmanagement	Datenkorb	Datennutzungskontrolle	
Werkzeuge	Selbstbewertungs-instrument	Checklisten für Datenqualität	Navigator für Qualitäts-beziehungen	Glossar
Konzepte	Bausteine & Stufenkonzept	UI- und Interaktionskonzepte	Referenzarchitektur	Einführungskonzepte
Modelle	Qualitätsmodell	Personas	Organisationstypen	Inhaltsontologie
	Anforderungsmodell	Mentale Modelle	Vorgehensmodell	
Anforderungen, Rahmen-bedingungen	Rechtliche Rahmenbedingungen	Bedarfe und Anforderungen verschiedener Stakeholder	Stand der Wissenschaft und Technik	Technische und organisatorische Umsetzbarkeit

Der Werkzeugkasten als Grundlage

TrUSD-Werkzeugkasten

Demonstratoren	Wissensdatenbank und Einwilligungsmanagement	Datenkorb	Datennutzungskontrolle	
Werkzeuge	Selbstbewertungs-instrument	Checklisten für Datenqualität	Navigator für Qualitäts-beziehungen	Glossar
Konzepte	Bausteine & Stufenkonzept	UI- und Interaktionskonzepte	Referenzarchitektur	Einführungskonzepte
Modelle	Qualitätsmodell	Personas	Organisationstypen	Inhaltsontologie
	Anforderungsmodell	Mentale Modelle	Vorgehensmodell	
Anforderungen, Rahmen-bedingungen	Rechtliche Rahmenbedingungen	Bedarfe und Anforderungen verschiedener Stakeholder	Stand der Wissenschaft und Technik	Technische und organisatorische Umsetzbarkeit

Der Werkzeugkasten als Grundlage

Anforderungen, Rahmen-bedingungen

Rechtliche Rahmenbedingungen

Bedarfe und Anforderungen verschiedener Stakeholder

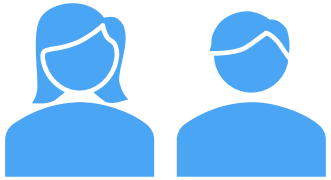
Stand der Wissenschaft und Technik

Technische und organisatorische Umsetzbarkeit

Der Werkzeugkasten als Grundlage

Bedarfe und Anforderungen verschiedener Stakeholder

Stakeholder festlegen



Arbeitnehmer

Betroffene

Verwaltungsmitarbeitende

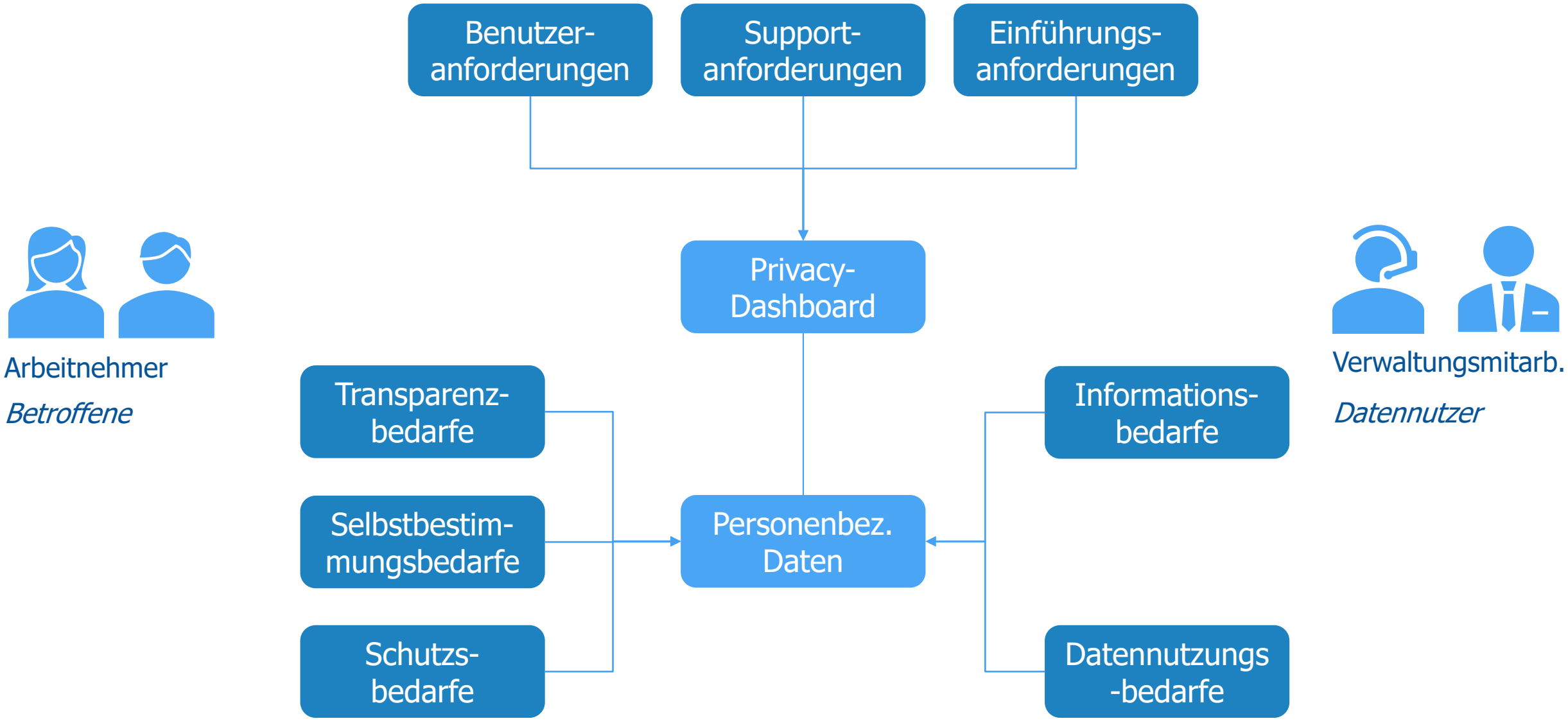
Datennutzer

Stakeholder befragen

Workshops

Interviews

Übersicht der Bedarfe



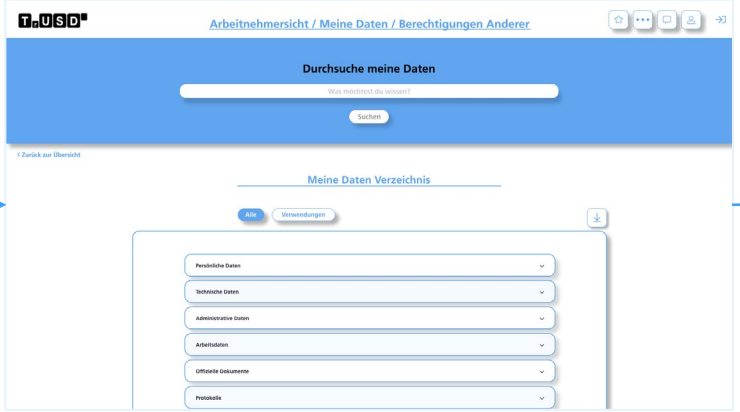
Vom Bedarf zum Privacy-Dashboard

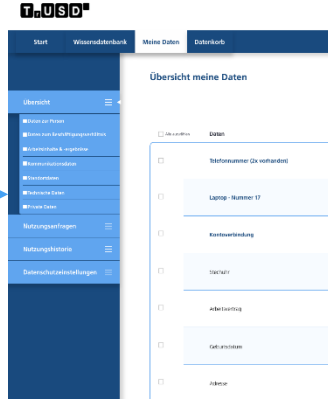
Transparenz-Bedarf:

Als Arbeitnehmer möchte ich einen Überblick über alle von mir in der Organisation existierende Daten erhalten

Systemanforderung:

Das PDB muss dem Dashboardnutzer die Möglichkeit geben Übersichten von Daten barrierefrei abzurufen. […]





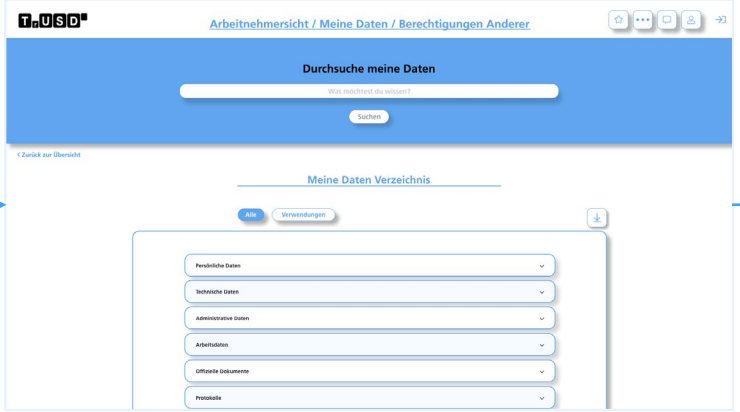
Vom Bedarf zum Privacy-Dashboard

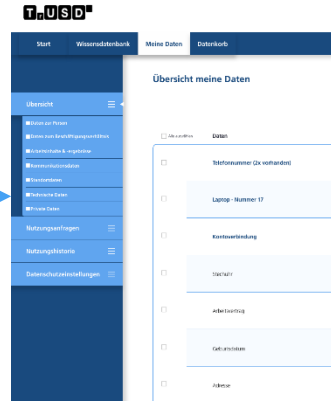
Transparenz-Bedarf:

Als Arbeitnehmer möchte ich einen Überblick über alle von mir in der Organisation existierende Daten erhalten

Systemanforderung:

Das PDB muss dem Dashboardnutzer die Möglichkeit geben Übersichten von Daten barrierefrei abzurufen. […]

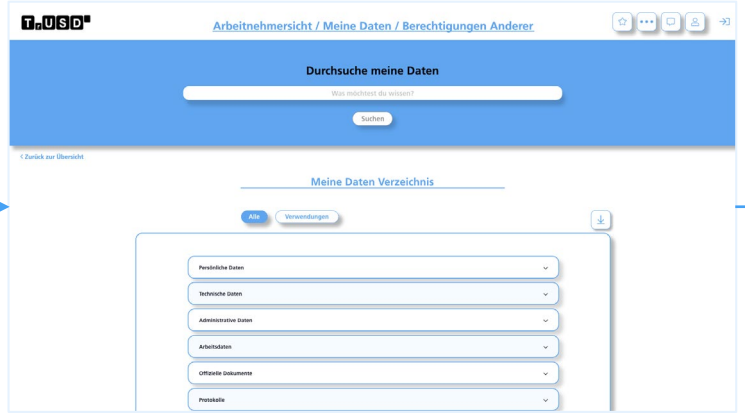


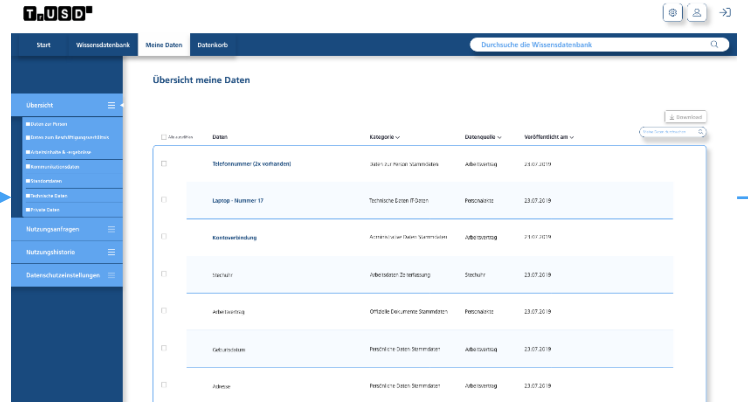


Validierung

Fokusgruppen

Vom Bedarf zum Privacy-Dashboard





Privacy-Dashboard

Anforderungsdokument maßschneidern

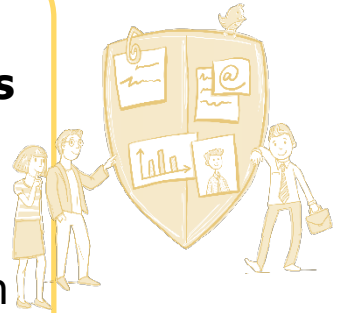
Anforderungs-dokument:

Bedarfe und Anforderungen verschiedener Stakeholder

Prioritäten & Ergänzungen

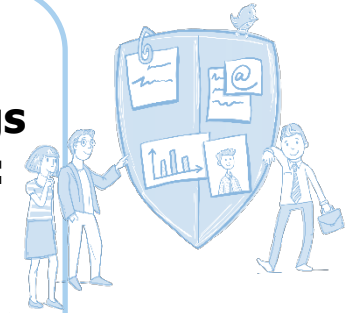
Anforderungs-dokument:

Bedarfe und Anforderungen verschiedener Stakeholder



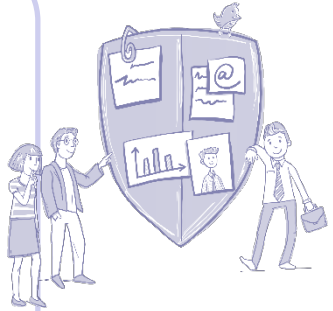
Anforderungs-dokument:

Bedarfe und Anforderungen verschiedener Stakeholder



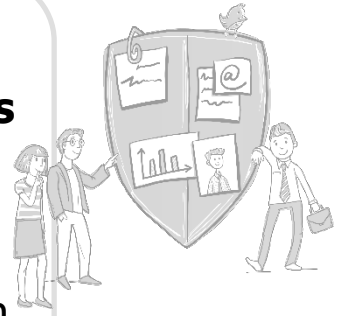
Anforderungs-dokument:

Bedarfe und Anforderungen verschiedener Stakeholder



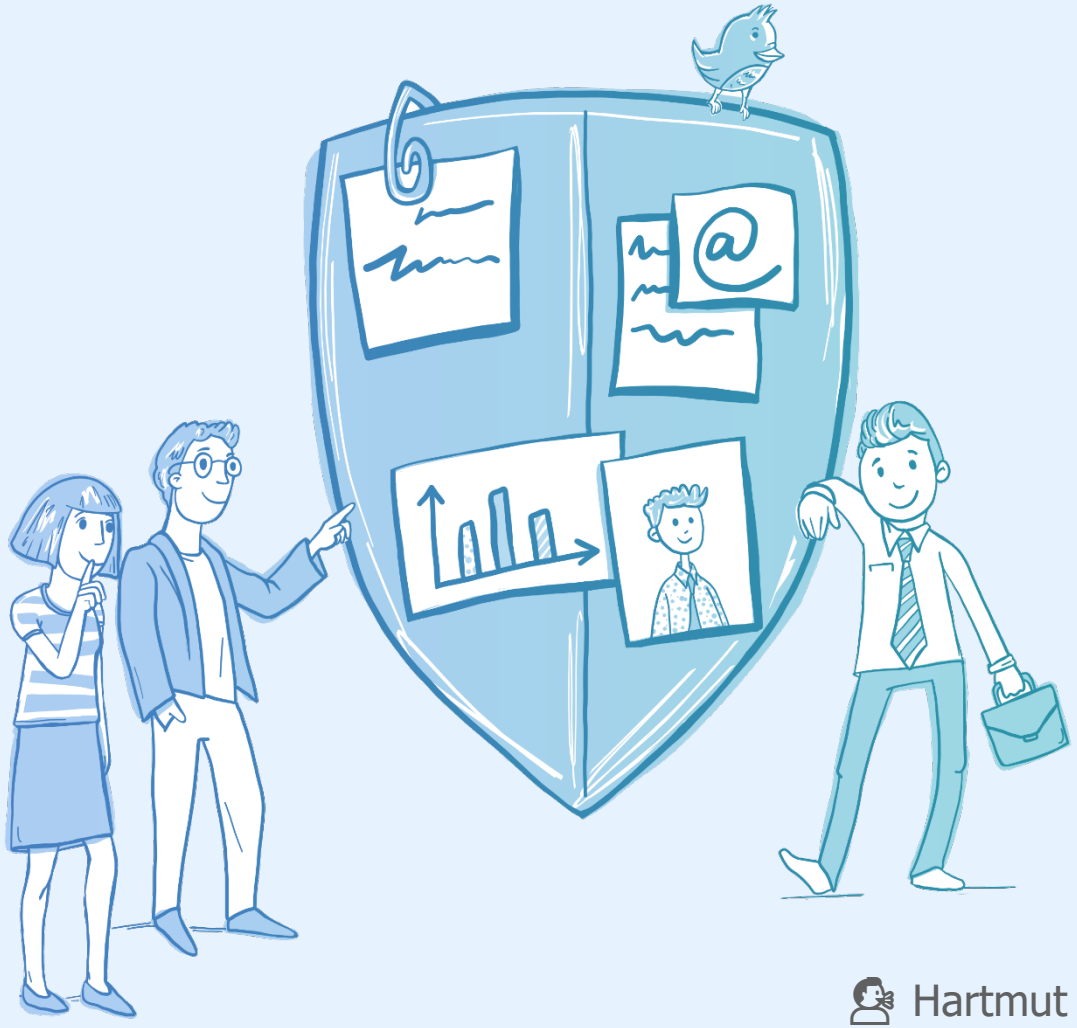
Anforderungs-dokument:

Bedarfe und Anforderungen verschiedener Stakeholder



Was?	Wo?
Anforderungskatalog inkl. Erhebungsworkshopskonzept	• Wird auf Projekt-Webseite veröffentlicht: https://www.trusd-projekt.de/
Wissenschaftliche Publikationen & Fachbeiträge	• Bosse, C. K.; Dietrich, A.; Kelbert, P.; Küchler, H.; Schmitt, H.; Tolsdorf, J.; Weßner, A. **Beschäftigtendatenschutz: Rechtliche Anforderungen und Technische Lösungskonzepte.** In Tagungsband des 23. Internationalen Rechtsinformatik Symposions IRIS 2020; Schweighofer, F. K., Saarenpää, A., Hötzendorfer, W., Eds.; Editions Weblaw: Salzburg, AT, 2020; pp 1–8. • Polst, S.; Kelbert, P.; Feth, D. **Company Privacy Dashboards: Employee Needs and Requirements.** In 1st International Conference on Human-Computer Interaction for Cyberse-curity, Privacy and Trust (HCI-CPT); Moallem, A., Ed.; Orlando, FL, USA, 2019; pp 429–440. https://doi.org/10.1007/978-3-030-22351-9_29. • Schmitt, H.; Polst, S. **Anforderungen und Rahmenwerk für den betrieblichen Datenschutz**. Softwaretechnik-Trends 2020, 40 (1), 9–10. • Karras, O.; Polst, S.; Späth, K. **Using Vision Videos in a Virtual Focus Group: Experiences and Recommendations**. arXiv:2011.00965 [cs] 2020.
Blogbeiträge	• https://www.iese.fraunhofer.de/blog/benutzerfreundliche-datenschutzeinstellungen-1/ • https://www.iese.fraunhofer.de/blog/benutzerfreundliche-datenschutzeinstellungen-2/ • https://www.iese.fraunhofer.de/blog/benutzerfreundliche-datenschutzeinstellungen-3/

Modelle

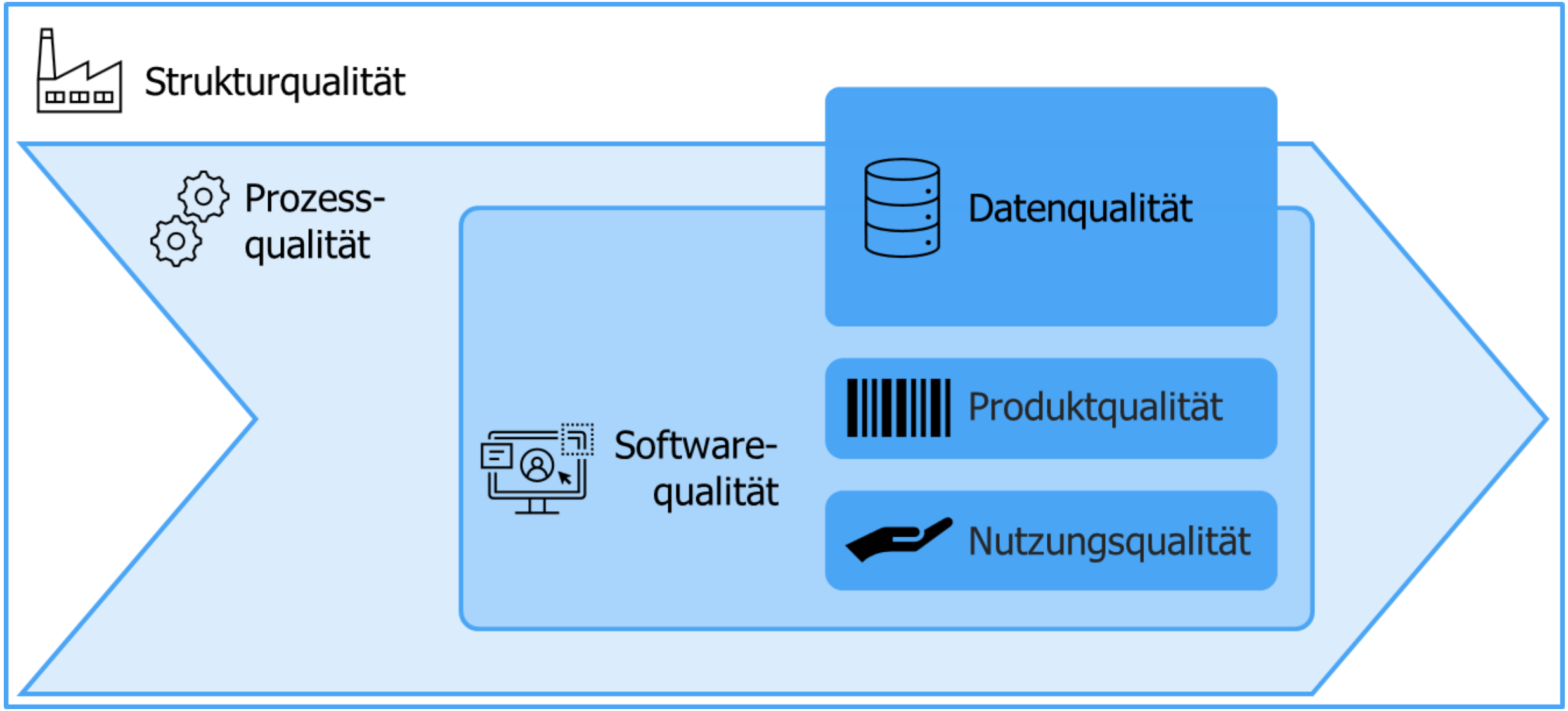


Hartmut Schmitt hartmut.schmitt@hk-bs.de

Qualitätsmodell

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Übersicht Qualitätsmodell



Beispiel „Transparenz“

Qualitätsmodell

Datenqualität
Produktqualität
Nutzungsqualität
Prozessqualität
Strukturqualität

Beispiel „Transparenz“

Qualitätsmodell

Datenqualität

Produktqualität

- Funktionale Tauglichkeit
- Performanz
- Kompatibilität
- Benutzerfreundlichkeit
- Zuverlässigkeit
- Sicherheit
- Datenschutz
- Wartbarkeit
- Übertragbarkeit

Nutzungsqualität

Prozessqualität

Strukturqualität

Quelle: ISO 25010 (Product quality)

einzelne Teilmerkmale und Definitionen ergänzt

Beispiel „Transparenz“

Qualitätsmodell

Datenqualität

Produktqualität

- Funktionale Tauglichkeit
- Performanz
- Kompatibilität
- Benutzerfreundlichkeit
- Zuverlässigkeit
- Sicherheit
- **Datenschutz**
  - Datenminimierung
  - Integrität
  - Intervenierbarkeit
  - Vertraulichkeit
  - Verfügbarkeit
  - Transparenz
  - Nichtverkettung

Standard-Datenschutzmodell

Beispiel „Transparenz“

Qualitätsmodell

Datenqualität

Produktqualität

- Funktionale Tauglichk
- Performanz
- Kompatibilität
- Benutzerfreundlichke
- Zuverlässigkeit
- Sicherheit
- **Datenschutz**
  - Datenminimierur
  - Integrität
  - Intervenierbarkeit
  - Vertraulichkeit
  - Verfügbarkeit
  - **Transparenz**
  - Nichtverkettung

Grad, in dem in einem unterschiedlichen Maße sowohl **Betroffene** als auch **Betreiber** eines Produkts oder Systems sowie zuständige Kontrollinstanzen **erkennen** können, **welche personenbezogenen Daten für welchen Zweck** in einem Verfahren **erhoben und verarbeitet** werden, welche Systeme und Prozesse dafür genutzt werden, wohin die Daten zu welchem Zweck fließen und wer die **rechtliche Verantwortung** für die personenbezogenen Daten und Systeme in den verschiedenen Phasen einer Datenverarbeitung besitzt.

Beispiel „Transparenz“

Bedarfe

und

Anforderungen

Qualit

Datenqu

Produk

- Funkti
- Perfor
- Komp
- Benut
- Zuver
- Sicher
- **Date**
  - D
  - I
  - I
  - V
  - V
  - **T**
  - N

ca. 30 relevante Transparenzbedarfe

- Datenverwendung (in welchen Prozessen?)
- Zugriffe (wer? wann?)
- Verwendungszweck
- Datenweitergabe
- Aufbewahrung (Ort, Frist)
- …

ca. 20 relevante Benutzeranforderungen

- Zugriff auf Auswertungsergebnisse
- Benachrichtigung bei Ereignissen
- Kontext bzw. Mehrwert bei Einwilligungsanfrage
- Erinnerungsfunktion zur Überprüfung der Einstellungen
- …

ca. 10 Systemanforderungen

Beispiel „Transparenz“

Bedarfe

und

Anforderungen

e Maßnahmen

15 typische Maßnahmen zur Gewährleistung der Transparenz

- Dokumentation der Verarbeitungsprozesse
- Dokumentation von Einwilligungen und Widersprüchen
- Konzeptuelle Berücksichtigung der Auskunftsrechte
- Protokollierung von schreibenden und lesenden Zugriffen
- …

- Verfügbarkeit
- **Transparenz**
- Nichtverkettung

Beispiel „Transparenz“

Bedarfe

und

Anforderungen

e Maßnahmen

Sicherheit?

15 typische Maßnahmen zur Gewährleistung der Transparenz

- Dokumentation der Verarbeitungsprozesse
- Dokumentation von Einwilligungen und Widersprüchen
- Konzeptuelle Berücksichtigung der Auskunftsrechte
- Protokollierung von schreibenden und lesenden Zugriffen
- …

- Verfügbarkeit
- **Transparenz**
- Nichtverkettung

Beispiel „Transparenz“

Bedarfe

und

Anforderungen

e Maßnahmen

15 typische Maßnahmen zur Gewährleistung der Transparenz

- Dokumentation der Verarbeitungsprozesse
- Dokumentation von Einwilligungen und Widersprüchen
- Konzeptuelle Berücksichtigung der Auskunftsrechte
- Protokollierung von schreibenden und lesenden Zugriffen
- …

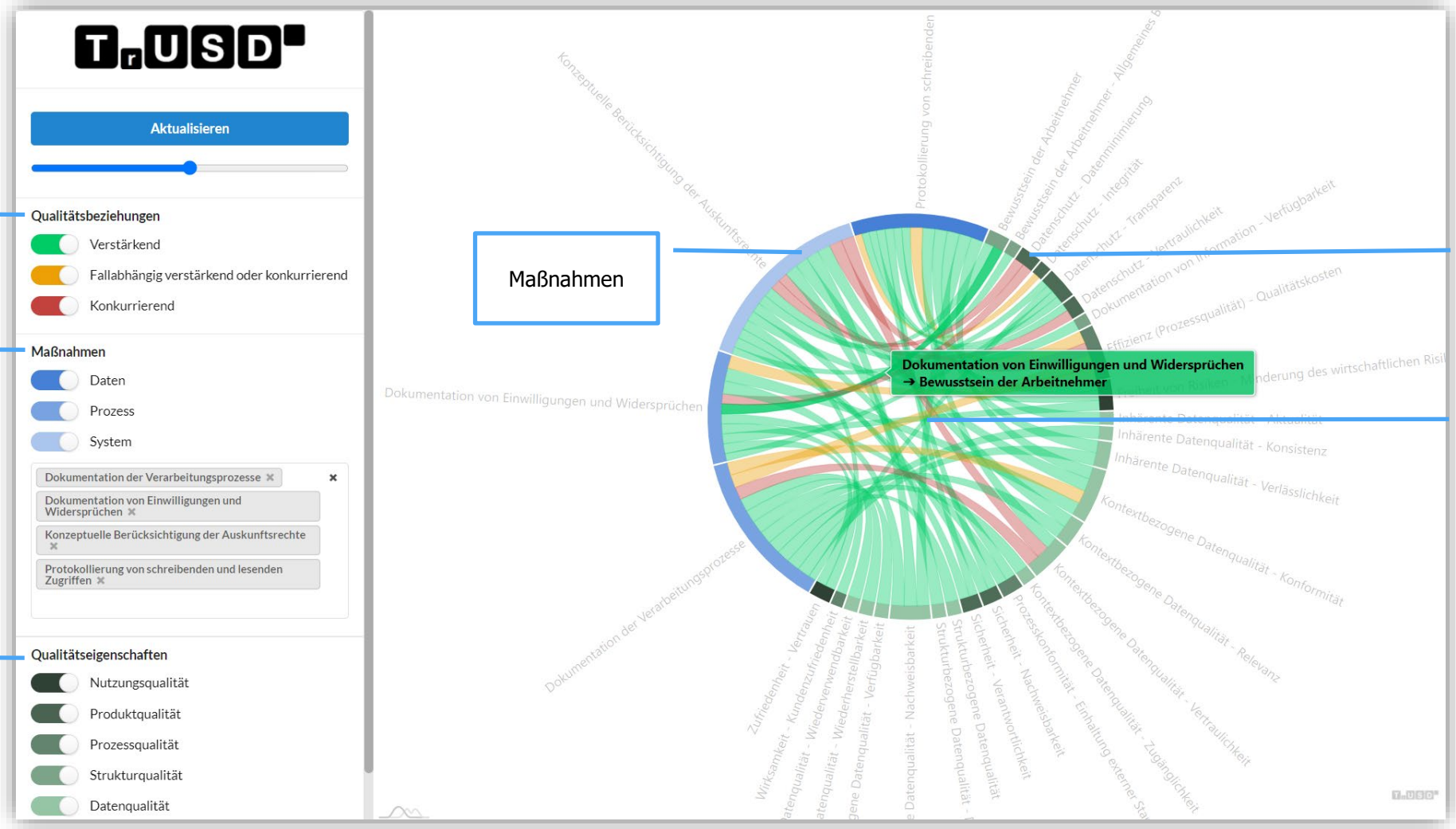
Maßnahmen, die ggf. die Transparenz beeinträchtigen

- Einschränkung von Leserechten
- …

- Verfügbarkeit
- **Transparenz**
- Nichtverkettung

Navigator für Qualitätsbeziehungen

1.132 Beziehungen (787 positiv, 238 negativ, 107 fallabhängig)



Filter: Beziehungen

Filter: Maßnahmen

Filter: Qualitäten

Maßnahmen

Qualitäts-eigenschaften

Qualitätsbeziehungen

Beispiel „Transparenz“

Bedarfe

und

Anforderung

d

he Maßnahmen

oge

- Verfügbarkeit
- **Transparenz**
- Nichtverkettung

Kriterien für Transparenz

- Ist die Transparenz der Datenverarbeitung gegenüber Anwendern und Betroffenen gewährleistet?
- Sind die Kategorien der verarbeiteten Daten nachvollziehbar dokumentiert?
- Wird das zugrundeliegende Konzept der Datenverarbeitung ausreichend erläutert?
- Sind die gemachten Angaben für alle Zielgruppen verständlich?
- ...

Beispiel „Transparenz“

Erfolgskriterium
„Transparenz Datenerhebung und -verarbeitung“

„Ich bin mit der Einführung des Privacy Dashboards zufrieden, wenn es mehr Transparenz beim Umgang mit personenbezogenen Daten schafft (z. B. welche Daten von mir werden wo und aus welchem Grund / zu welchem Zweck erhoben und verarbeitet?), da dann eine konsequente und transparente Umsetzung der DSGVO gewährleistet ist und zudem ein stärkeres Bewusstsein für das Thema Datenschutz entsteht."

Bedarfe und Anforderun

- Intervenierbarkeit
- Vertraulichkeit
- Verfügbarkeit
- **Transparenz**
- Nichtverkettung

Erfolgskriterien

nd che Maßnahmen

loge

Weiterführende Informationen

Was?	Wo?
Qualitätsmodell	• Deliverable 2.4 TrUSD-Qualitätsmodell • Hartmut Schmitt & Eduard C. Groen: Qualitätsmodell zur Förderung des Beschäftigtendatenschutzes. In: DuD Datenschutz und Datensicherheit, Ausgabe 1/2021. Wiesbaden: Springer Gabler. • Denis Feth & Hartmut Schmitt: Requirement and Quality Models for Privacy Dashboards. In: 2020 IEEE 7th International Workshop on Evolving Security & Privacy Requirements Engineering (ESPRE)
Qualitätsbeziehungen	• Anhang zu Deliverable 2.4 TrUSD-Qualitätsmodell (Dokumentation der Qualitätsbeziehungen)

Konzepte

Jan Tolsdorf jan.tolsdorf@h-brs.de

Rahmenarchitektur

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Anforderungen

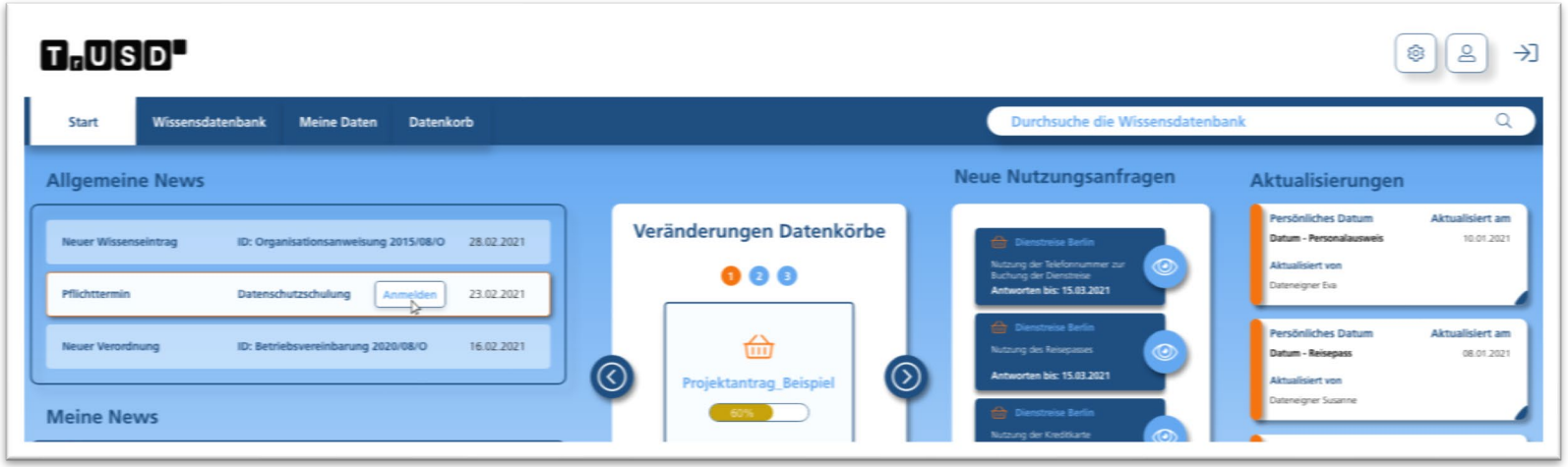
Benutzeranforderungen

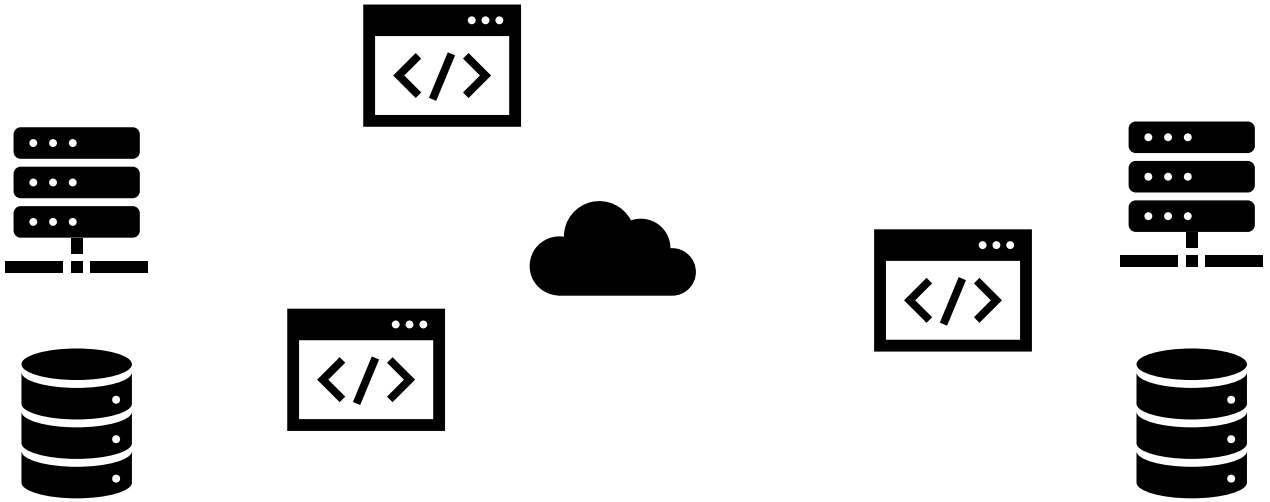
Gesetzl. Rahmenbedingungen

Kontext

Aktuelle IT-Infrastruktur

Aktuelle IT-Standards





Unterteilung nach Fachlichkeit

Anforderungen

- Benutzeranforderungen
- Gesetzl. Rahmenbedingungen
- Kontext

Domänen

- Transparenz
- Selbstbestimmung
- Durchsetzung und Daten
- Nebenaufgaben

Unterteilung nach Fachlichkeit

Transparenz

Selbstbestimmung

Durchsetzung und Daten

Nebenaufgaben

Unterteilung nach Fachlichkeit

Transparenz	Selbstbestimmung	Durchsetzung und Daten	Nebenaufgaben

Umfangreiche Dokumentation und Aufbereitung von Informationen zur Verarbeitung pers. Daten.

- Dokumente und Regularien;
- Strukturiertes (Daten-/Prozess-) Modell;
- Informationen zu zulässigen und erfolgten Verarbeitungen pers. Daten.

Unterteilung nach Fachlichkeit

Transparenz	**Selbstbestimmung**	Durchsetzung und Daten	Nebenaufgaben

Interaktionsmöglichkeiten für die Einflussnahme auf aktuelle und zukünftige Verarbeitungen pers. Daten.

- Einwilligung;
- Löschung;
- Widerspruch;
- Weiterführende Privatheitseinstellungen.

Unterteilung nach Fachlichkeit

Transparenz	Selbstbestimmung	**Durchsetzung und Daten**	Nebenaufgaben

Technische Integration in Dritt- und Bestandssysteme.

- Durchsetzung von Regeln durch PETs;
- Durchsetzung von Transparenz;
- Zugriff auf Daten.

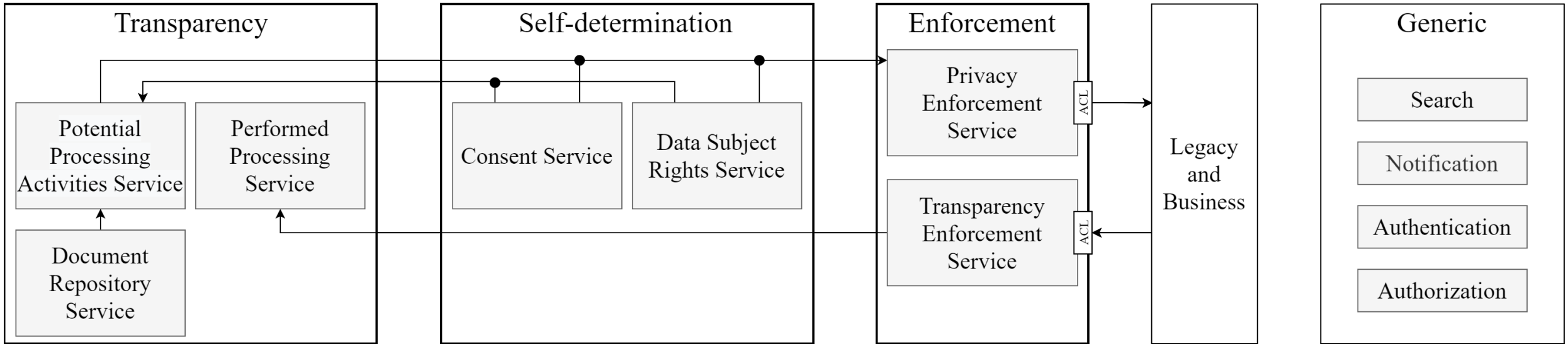
Unterteilung nach Fachlichkeit

Transparenz | Selbstbestimmung | Durchsetzung und Daten | Nebenaufgaben

Unspezifische und generische Aufgaben.

- Authentifizierung;
- Autorisierung;
- Benachrichtigungen.

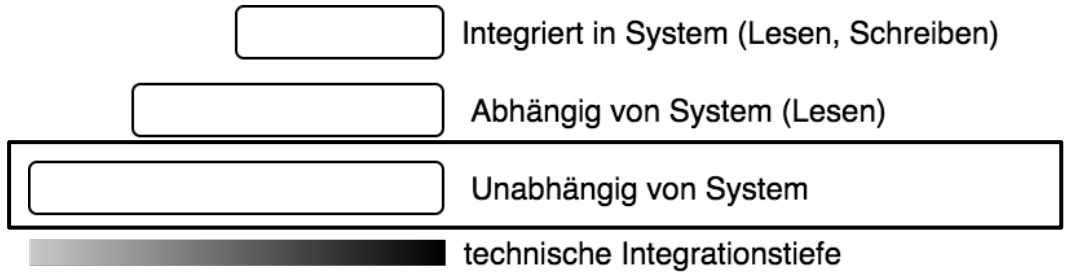
Dienste und Abhängigkeiten

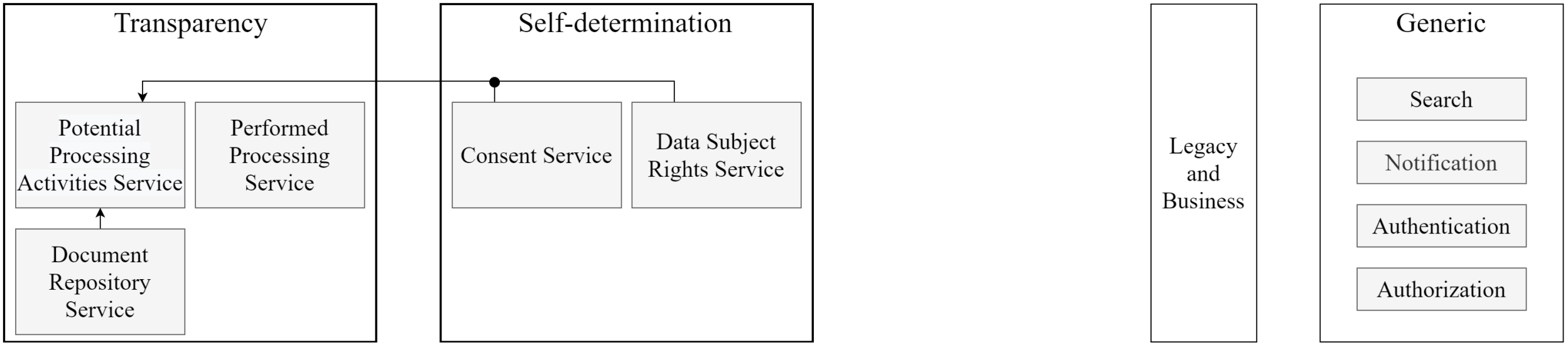


F. Dehling, D. Feth, S. Polst, B. Steffes, und J. Tolsdorf, „Components and Architecture for the Implementation of Technology-driven Employee Data Protection", in *Trust, Privacy and Security in Digital Business*, Linz, Austria, 2021.

Dienste und Abhängigkeiten

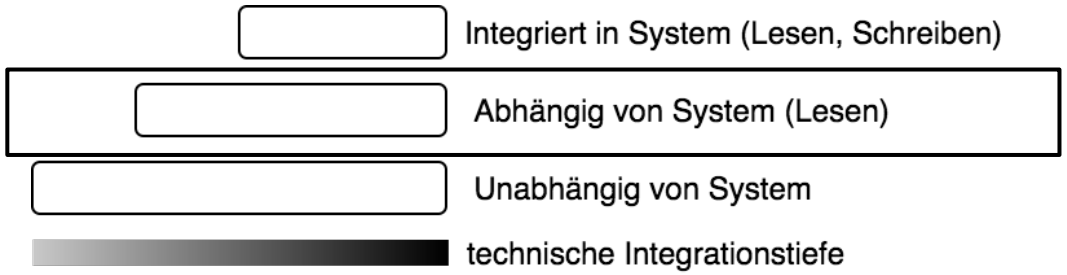
- Integrationstiefe: Unabhängig.

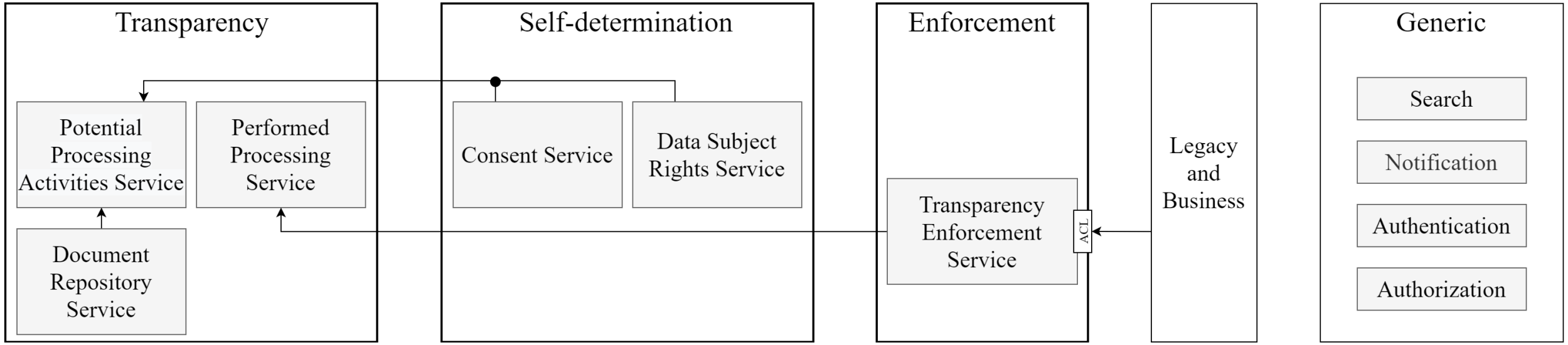




Dienste und Abhängigkeiten

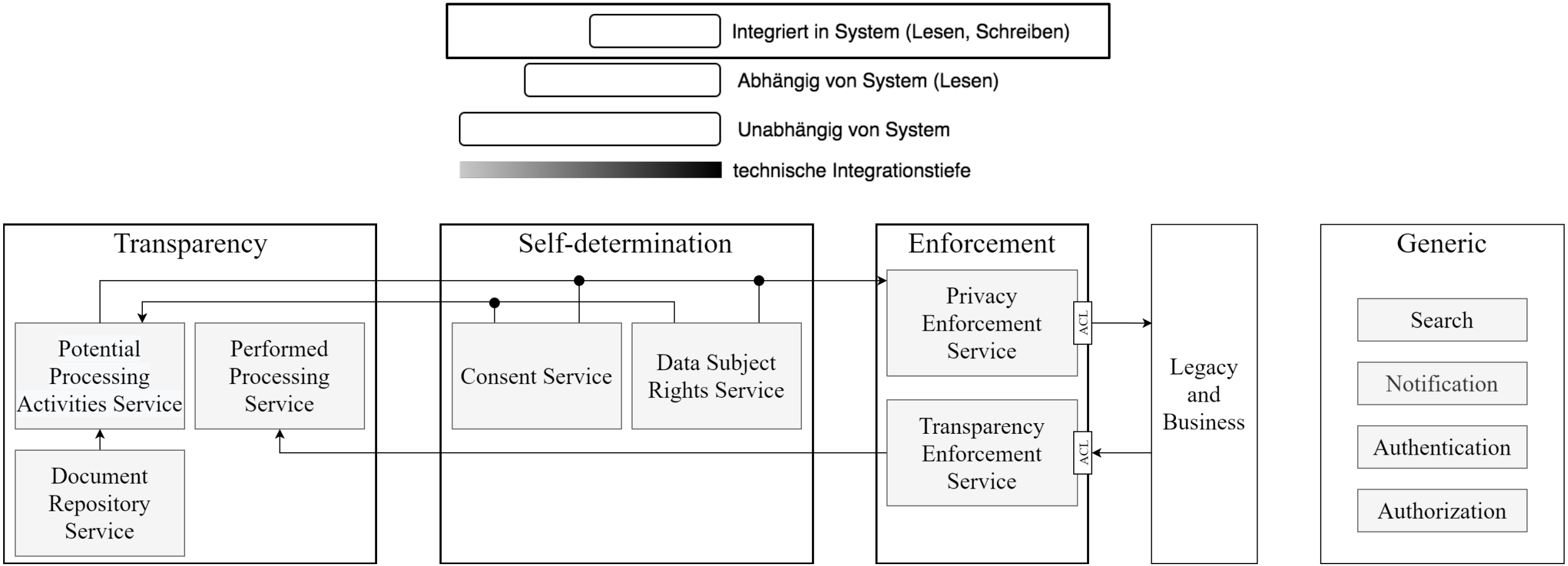
- Integrationstiefe: Abhängig.





Dienste und Abhängigkeiten

- Integrationstiefe: Integriert.

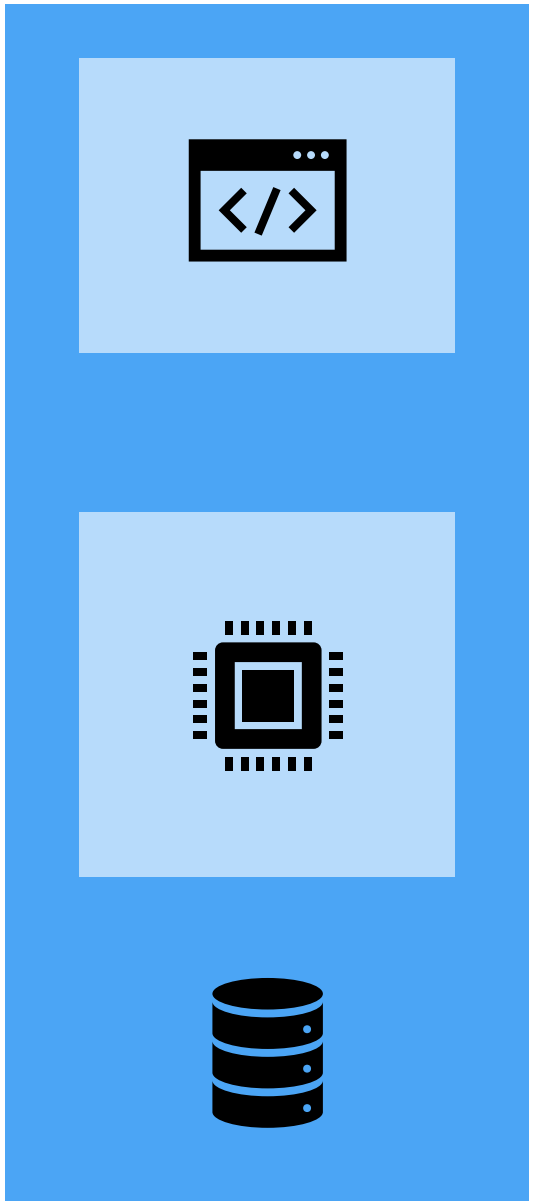


Umsetzung

Aktuelle IT-Infrastruktur

Aktuelle IT-Standards

- Dienste orientierte Architektur auf Basis von Web-Technologien
  - Micro-Frontend Architektur



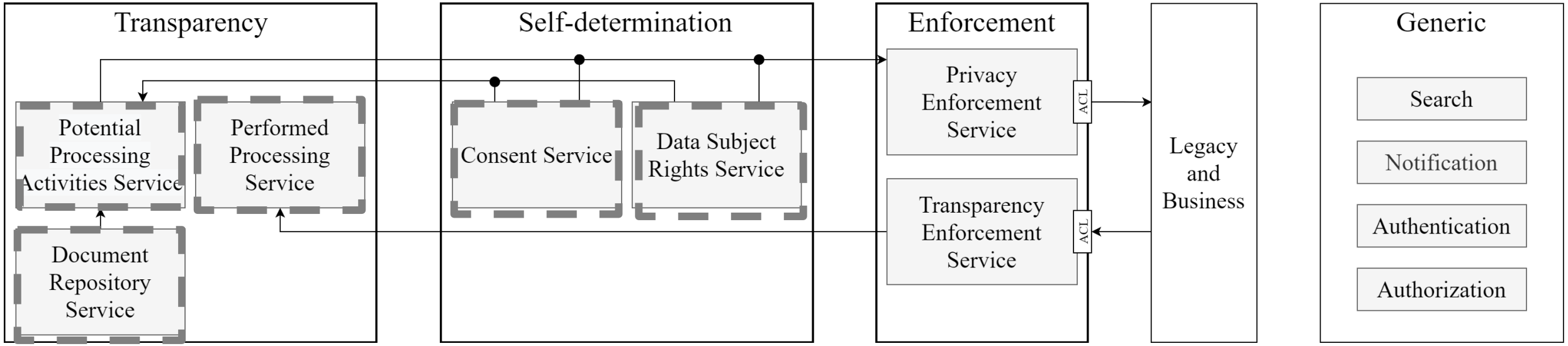
Web Components

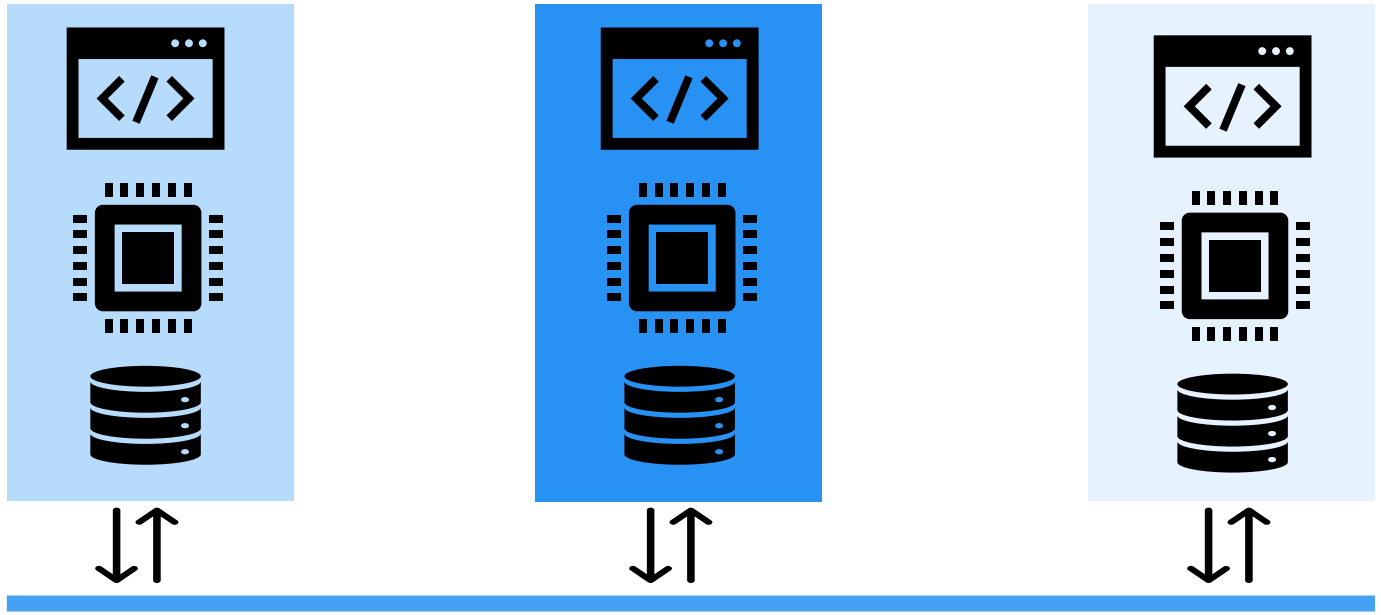
stencil

node.js

mongoDB

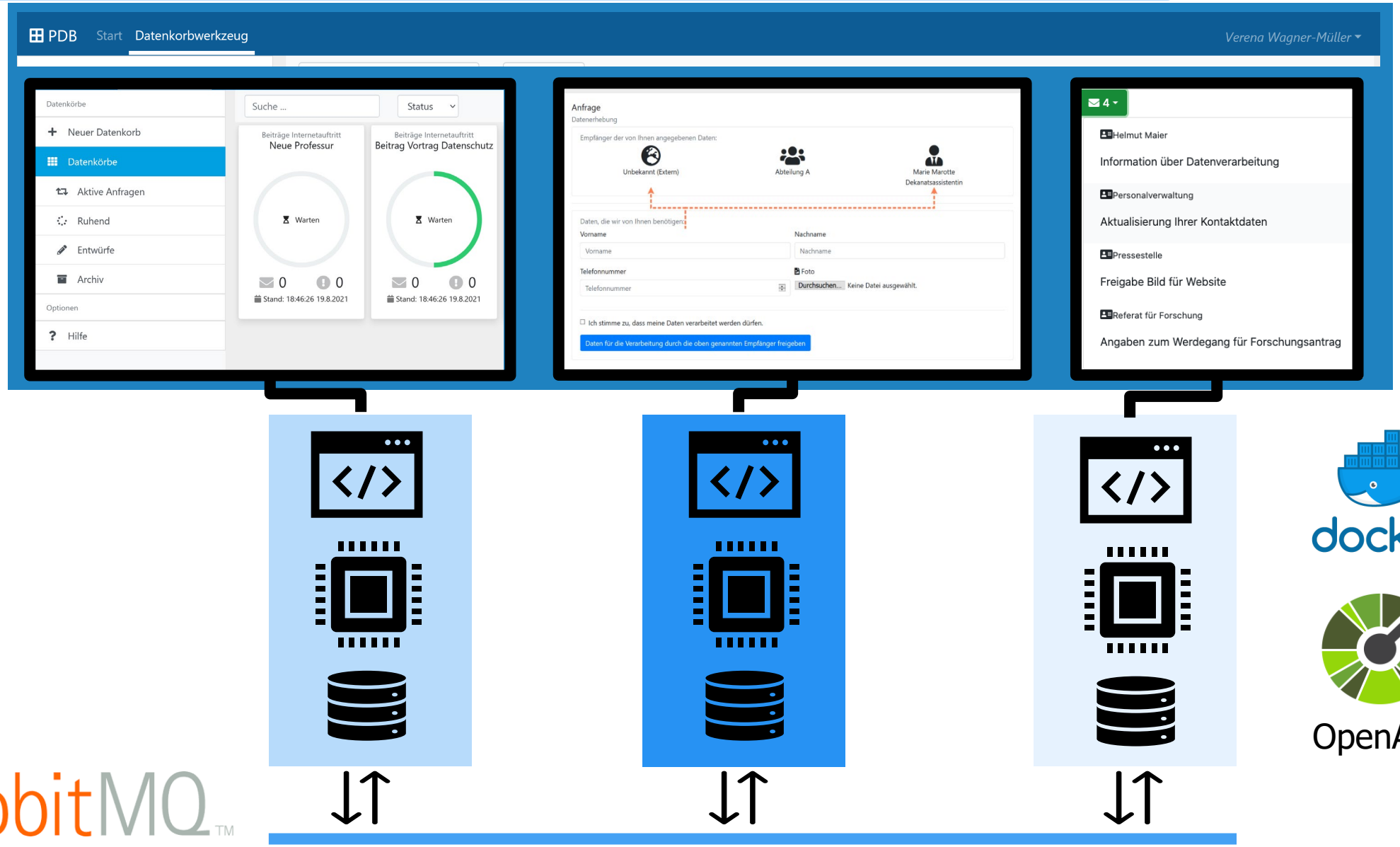
Umsetzung





OpenAPI

Umsetzung



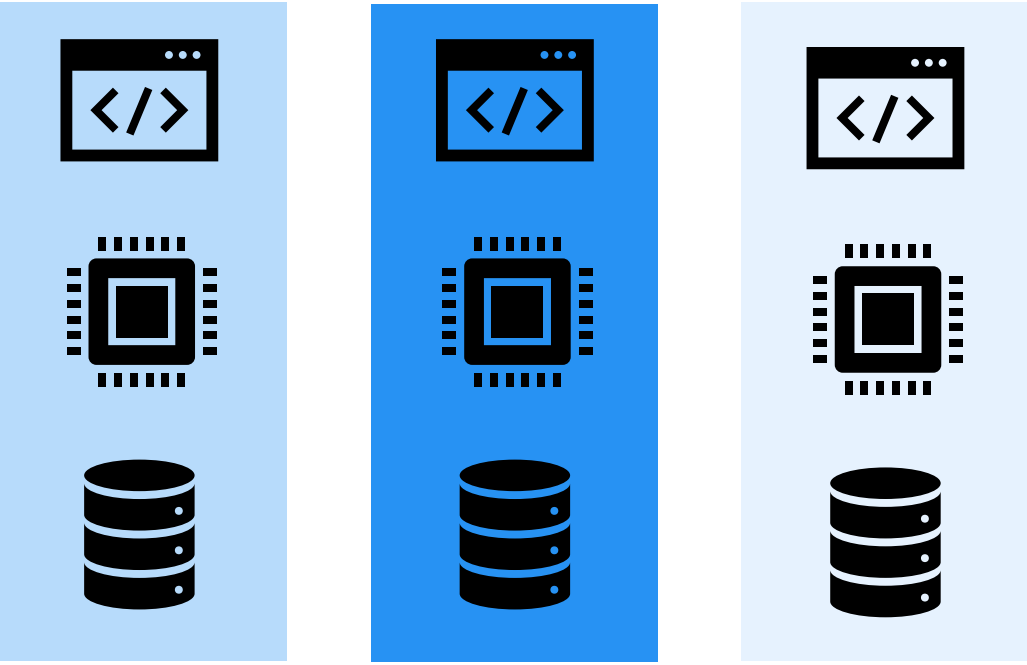
docker

OpenAPI

RabbitMQ™

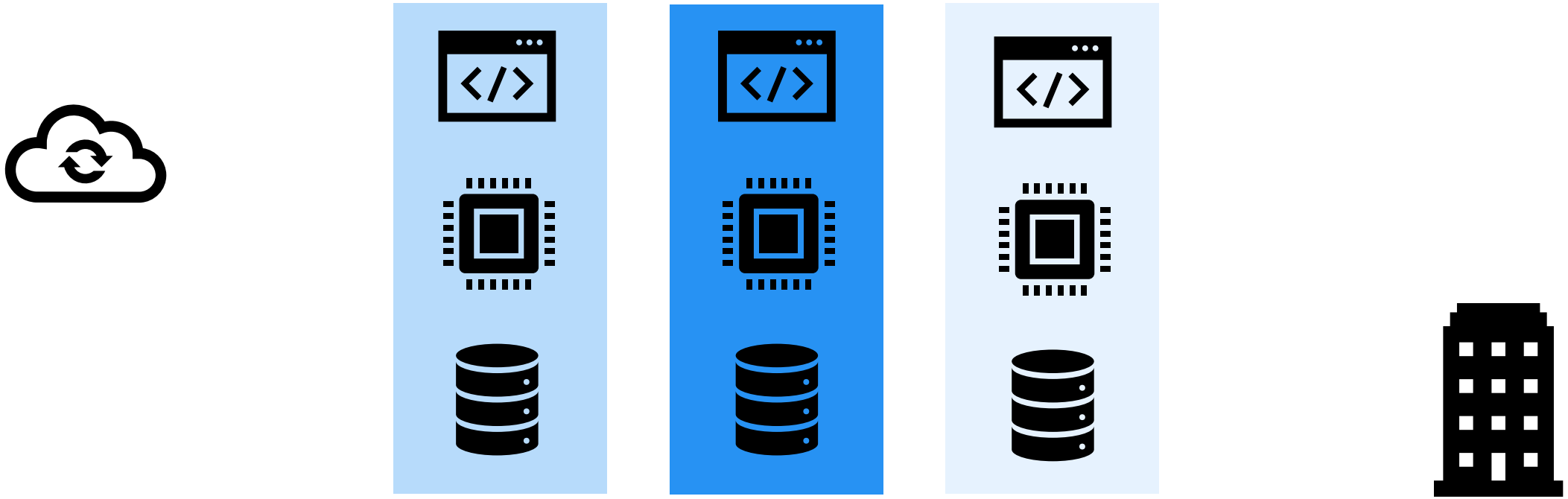
Umsetzung

- Horizontale Skalierung
  → garantiert hohe Verfügbarkeit des PDBs



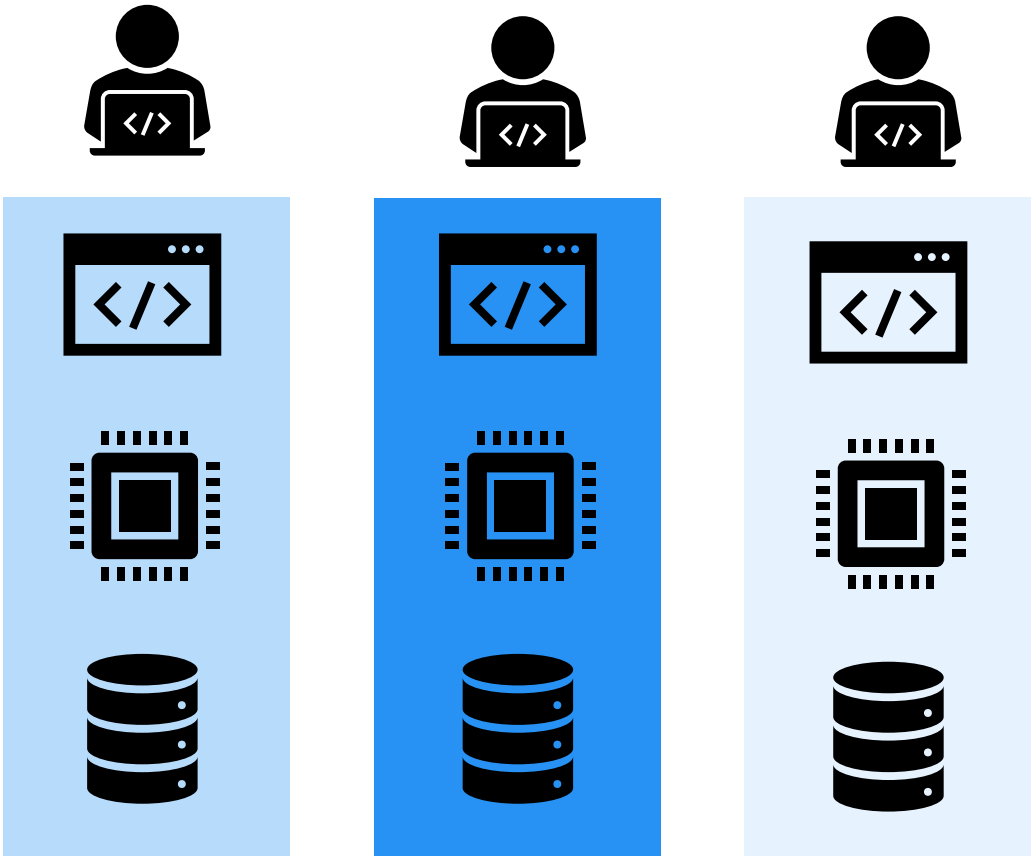
Umsetzung

- Infrastructure as a Service (IaaS) & Software as a Service (SaaS)
  → Reduziert technische Hürde zur Einführung des PDBs



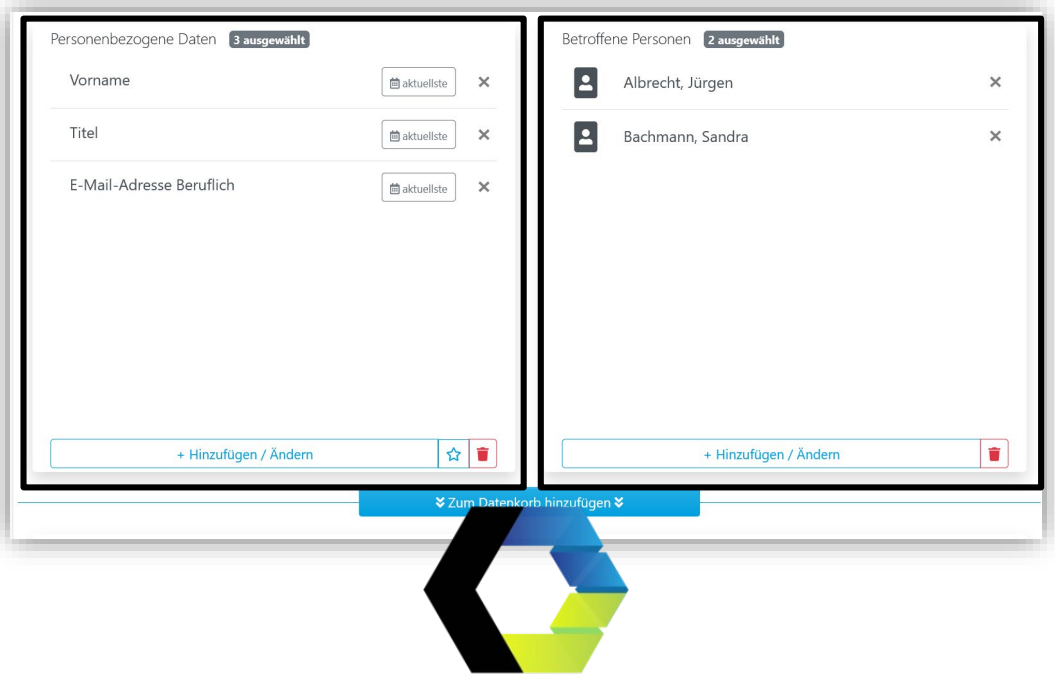
Umsetzung

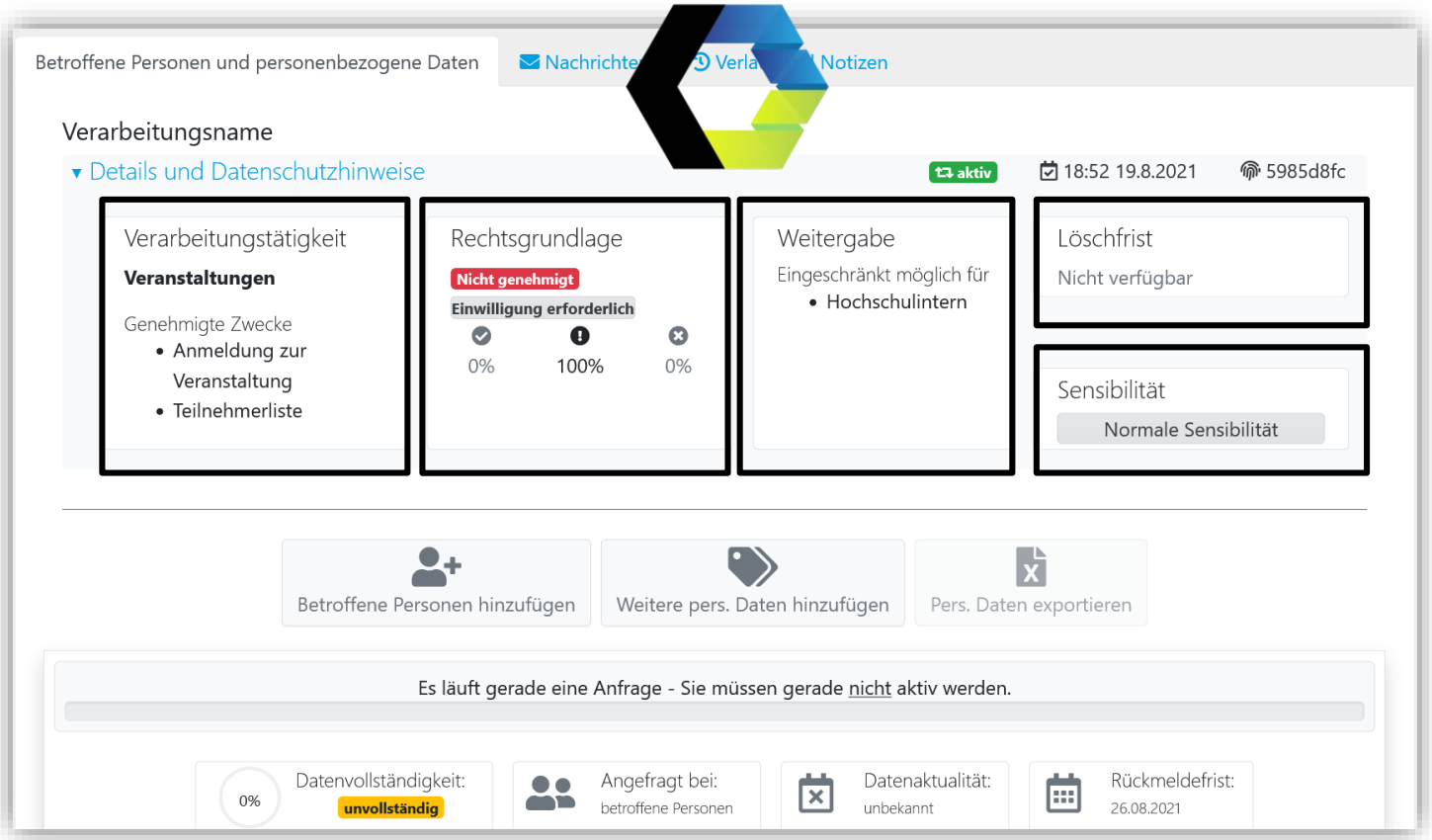
- Unabhängigkeit bei Entwicklung und Deployment
  → Förderlich für die Umsetzung des „Privacy Now“ Ansatzes



Umsetzung

- Wiederverwendbarkeit
  → Evaluierte UI-Konzepte verpackt in UI-Bibliotheken

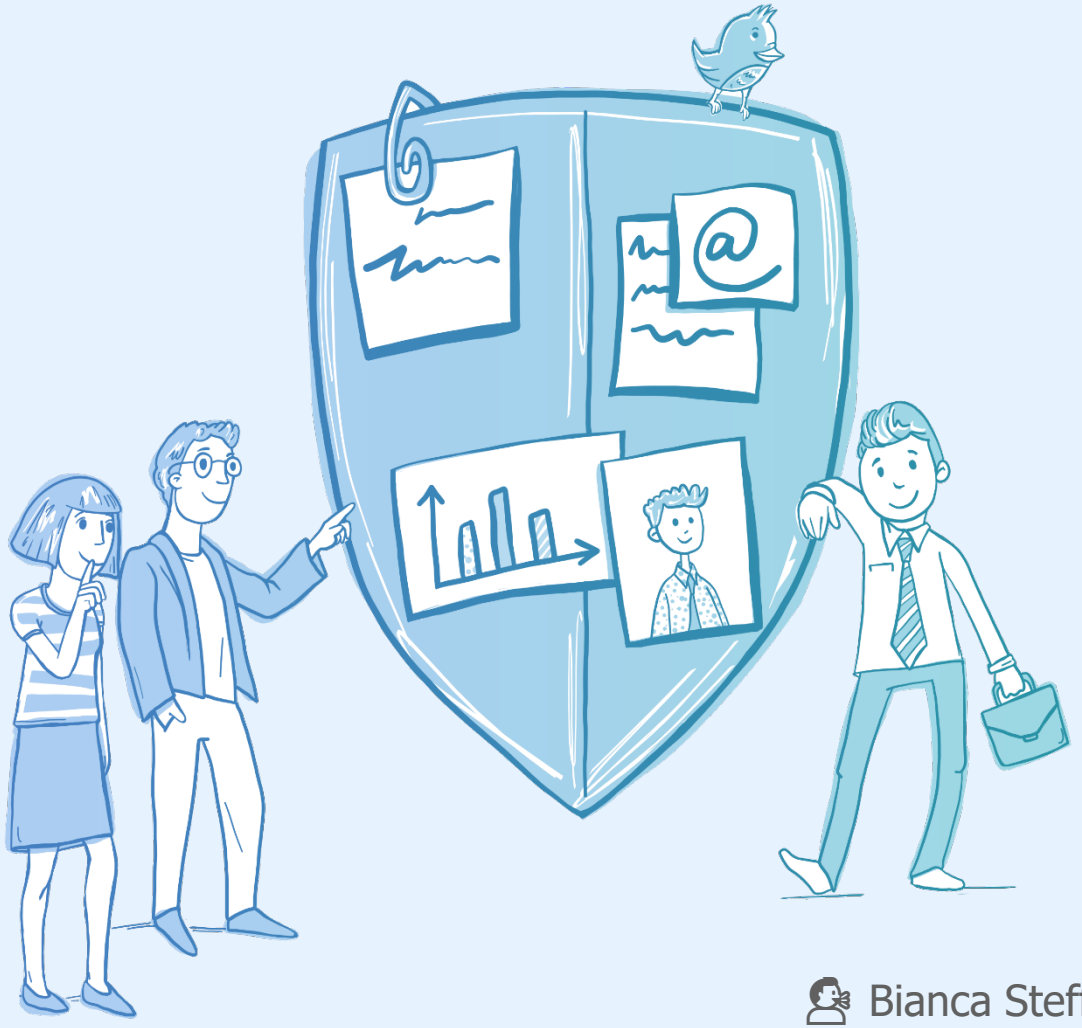




Weiterführende Informationen

Was?	Wo?
Architektur und Werkzeuge	• Deliverable 4.1 – Integrationskonzept • Deliverable 5.2 – Demonstrator H-BRS • Jan Tolsdorf, Florian Dehling und Luigi Lo Iacono: „Data Cart – Co-designing a tool for the GDPR-compliant handling of personal data by employees" under submission (2022)
Einführungskonzept	• Deliverable 3.1 – Dokumentation der Konzepte zur Erstellung und Einführung von Privacy Dashboards • Florian Dehling, Denis Feth, Svenja Polst, Bianca Steffes und Jan Tolsdorf: „Components and Architecture for the Implementation of Technology-driven Employee Data Protection" in Proceedings of the International Conference on Trust, Privacy and Security Digital Business (TrustBUS 2021)

Werkzeuge



Bianca Steffes bianca.steffes@uni-saarland.de

Anonymisierungsmethoden

Unterstützung des Datenschutzes durch Technik

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Anonymisierung

Eine Anonymisierung liegt vor, wenn ein Datum derart verändert wird, dass **keinerlei Bezug** mehr zu einer Person hergestellt werden kann.

(Die DSGVO ist auf anonymisierte Daten nicht anwendbar.)

Bestehende Anonymisierungslösungen

Entfernen des direkten Identifikators

myfactory

SAP

Salesforce

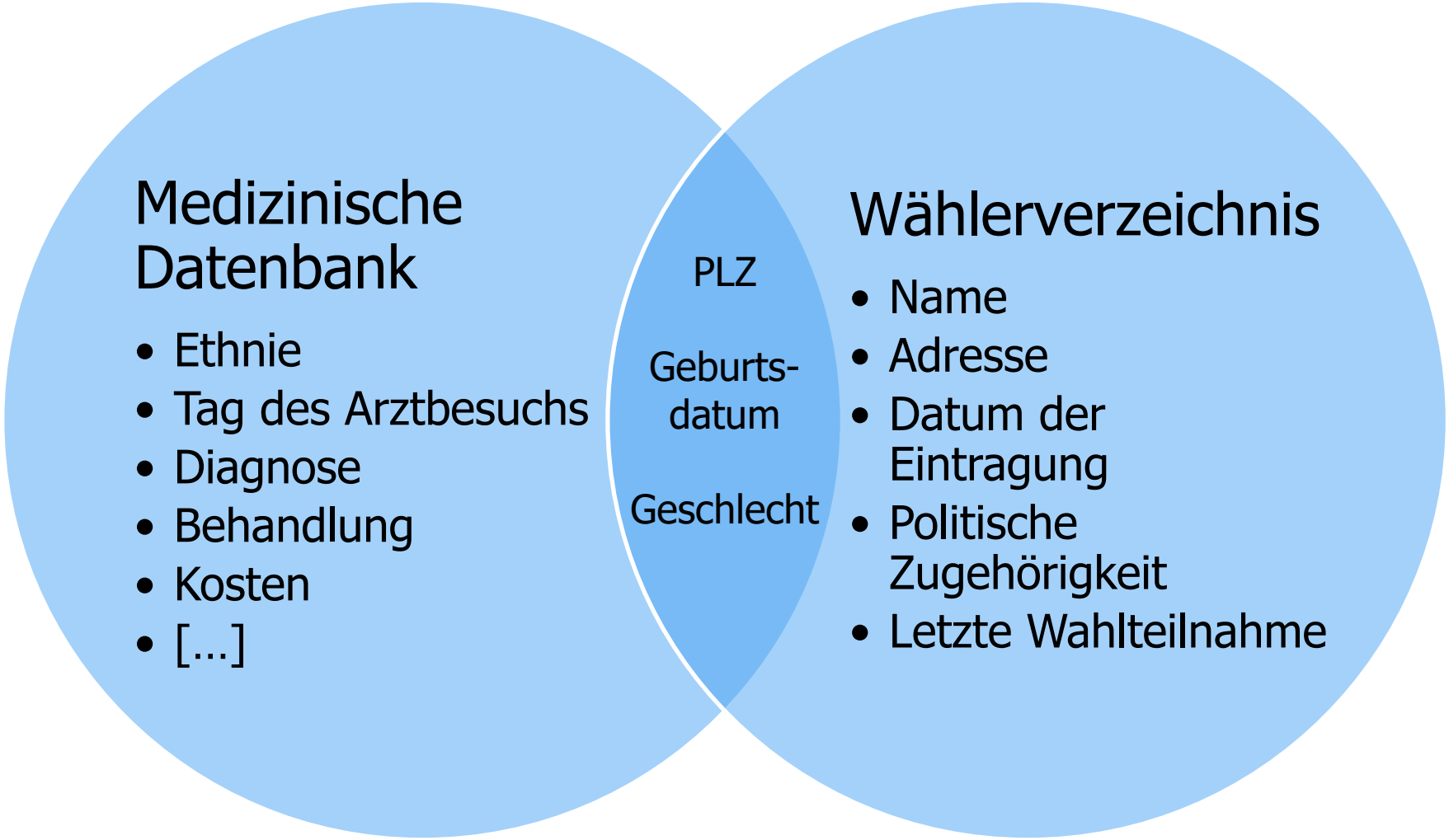
ANON

k-Anonymität

Entfernung des Identifikators (1/2)

Geburtsjahr	Postleitzahl	Geschlecht	Diagnose
1982	66123	Männlich	Migräne
1982	66123	Männlich	Erkältung
1983	66123	Männlich	Rheuma
1983	66123	Männlich	Depression
1985	66119	Weiblich	Heuschnupfen
1985	66119	Weiblich	Hypochondrie
1983	66123	Weiblich	Übergewicht
1983	66123	Weiblich	Migräne

Entfernung des Identifikators (2/2)



k-Anonymität (1/2)

k = 4

Geburtsjahr	PLZ	Geschlecht	Diagnose
1982	66123	Männlich	Migräne
1982	66123	Männlich	Erkältung
1983	66123	Männlich	Rheuma
1983	66123	Männlich	Depression
1985	66119	Weiblich	Depression
1985	66119	Weiblich	Erkältung
1983	66123	Weiblich	Übergewicht
1983	66123	Weiblich	Migräne

Geburtsjahr	PLZ	Geschlecht	Diagnose
1982-1983	66123	Männlich	Migräne
1982-1983	66123	Männlich	Erkältung
1982-1983	66123	Männlich	Rheuma
1982-1983	66123	Männlich	Depression
1983-1985	66*	Weiblich	Depression
1983-1985	66*	Weiblich	Erkältung
1983-1985	66*	Weiblich	Übergewicht
1983-1985	66*	Weiblich	Migräne

k-Anonymität (2/2)

TrUSD

Angriffsmöglichkeiten

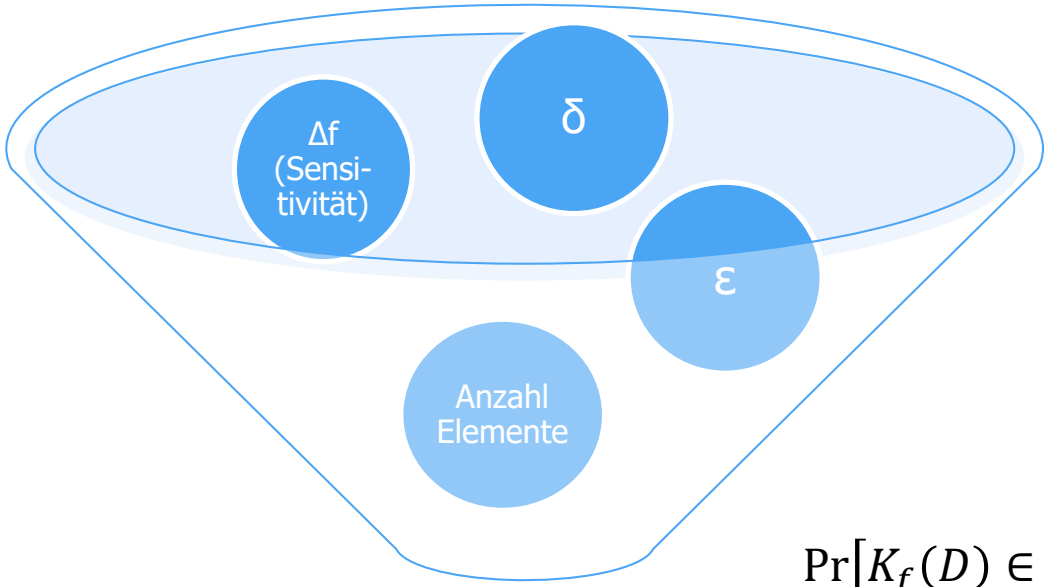
- komplementäre Veröffentlichung
- Homogenitätsangriff
- Hintergrund-/Zusatzwissen

Verbleibende Problematik

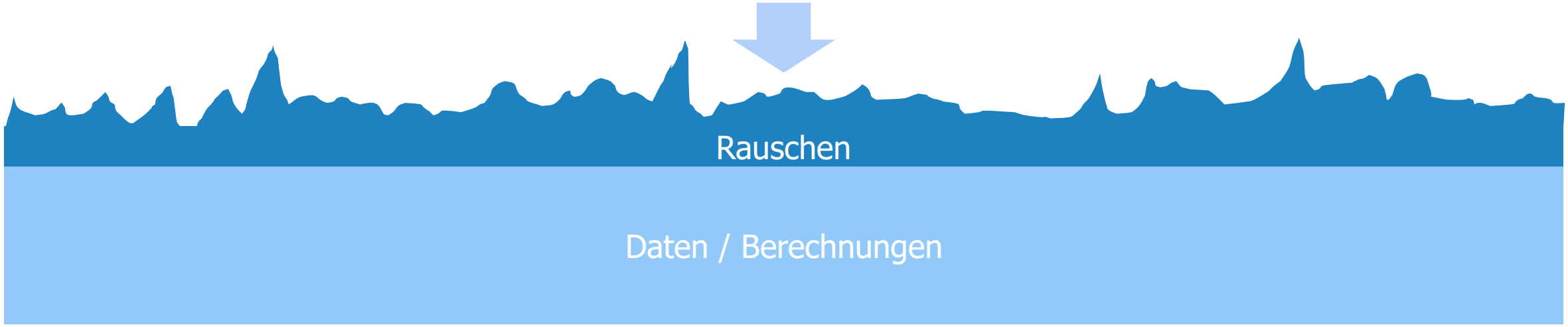
- Der Quasi-Identifikator kann nicht effizient automatisiert bestimmt werden.
- Es birgt immer noch das Risiko eines Anonymitätsverlusts.

Differential Privacy (1/4)

$$g = f(X) + Lap(\Delta f / \varepsilon)$$

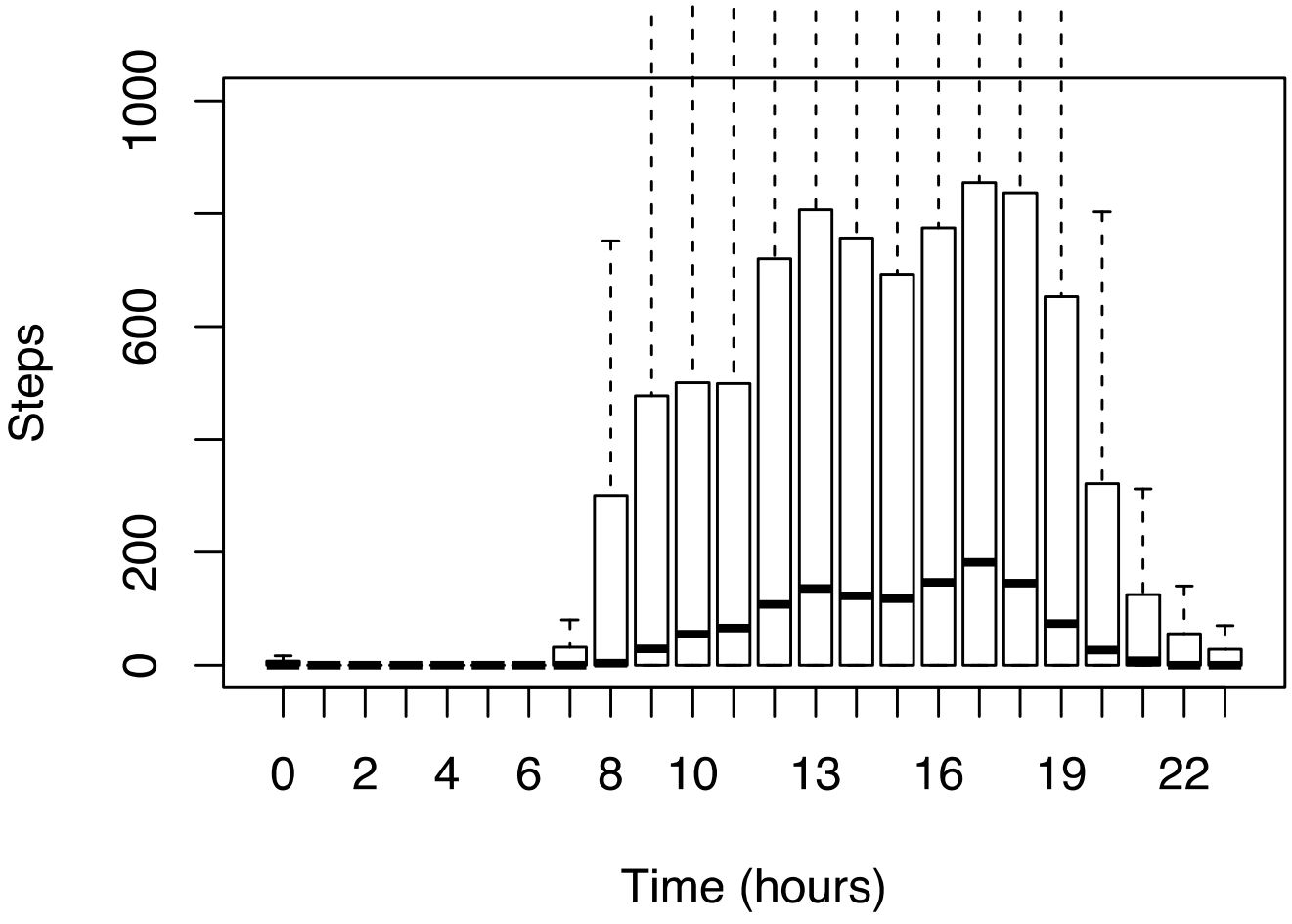


$$\Pr[K_f(D) \in s] \leq e^{\varepsilon} * \Pr[K_f(D') \in s] + \delta$$



Differential Privacy (2/4)

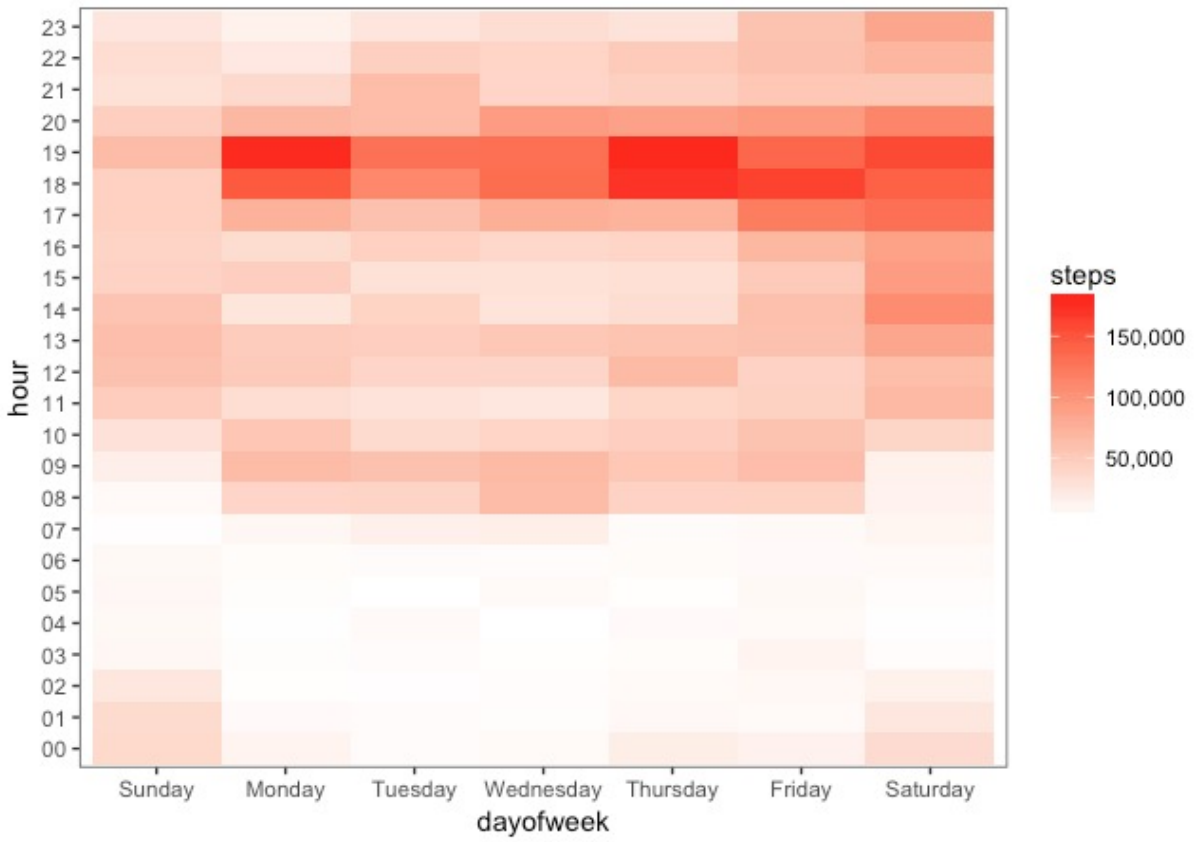
- Es wird eine große Menge an Daten benötigt.
- Ungeeignet für konkrete Daten wie Telefonnummer oder Namen
- Gut geeignet für sensible Daten wie Gesundheitsdaten.
- Abfragen sind begrenzt.



Differential Privacy (3/4)

- Anhand der Schrittdaten der Mitarbeiter möchte ein Restaurant die Auslastung seiner Mitarbeiter bestimmen.

- Es wird keine detaillierte Betrachtung jedes einzelnen Mitarbeiters benötigt, sondern nur eine aggregierte Ansicht.



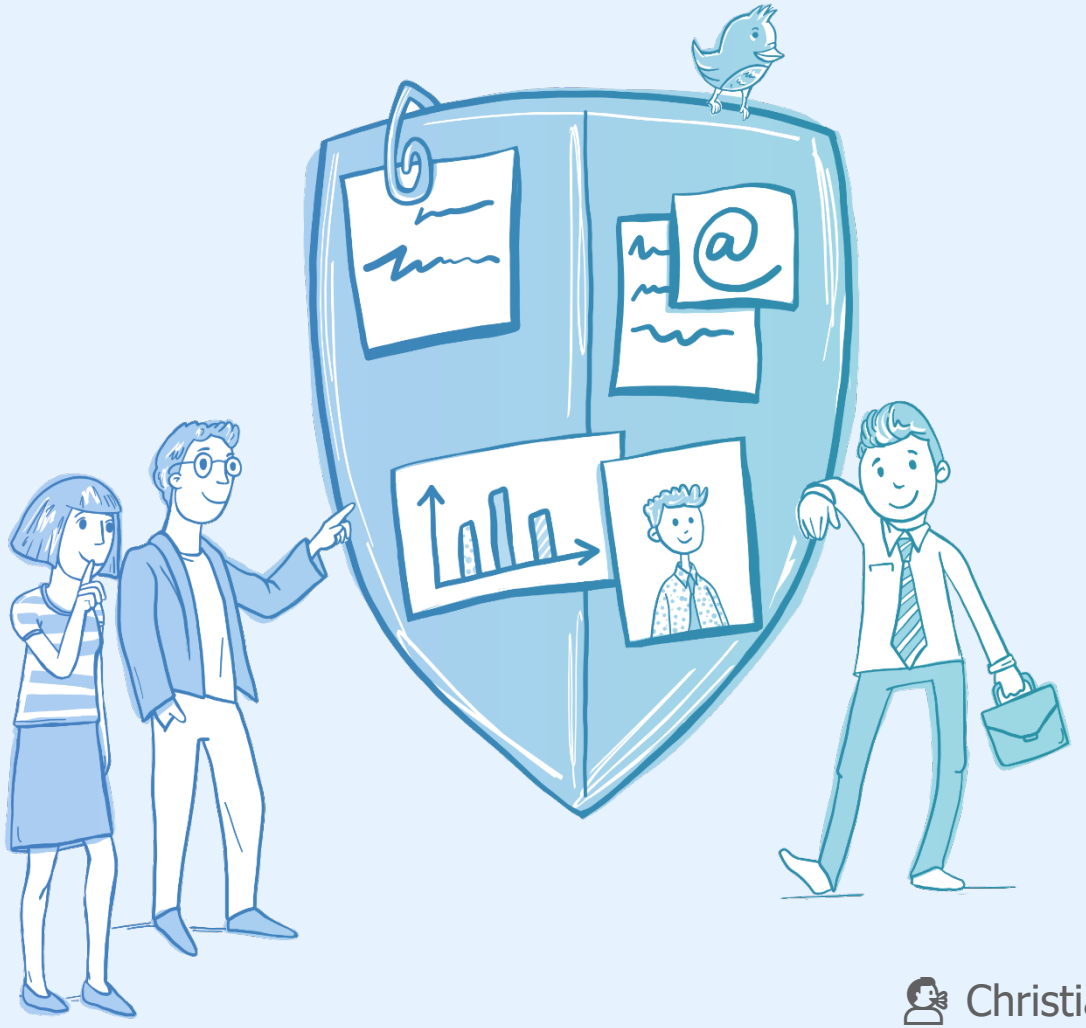
Differential Privacy (4/4)

Vorteile	Nachteile
Mathematische Garantie für Privacy	Begrenzte Anzahl an Analysemethoden
Mehr Bereitschaft Daten zur Verfügung zu stellen	Begrenzte Anzahl an Anfragen
Vertrauensgewinn bei den Mitarbeitern	Ungenauere Ergebnisse

Weiterführende Informationen

Was?	Wo?
Allgemeine Informationen zu Werkzeugen zur Anonymisierung	• Deliverable 4.1 - Werkzeuge für Transparenz, Selbstbestimmung und deren Umsetzung
Bestehende Softwarelösungen	• ANON: http://www.tmf-ev.de/Desktopmodules/Bring2Mind/DMX/Download.aspx?EntryId=22185&PortalId=0 und https://www.tmf-ev.de/Produkte/Uebersicht/ctl/ArticleView/mid/807/articleId/1290/P100201.aspx • myfactory: https://www.myfactory.com/start.aspx • Salesforce: https://mind-force.de/knowhow/salesforce-dsgvo/ und https://appexchange.salesforce.com/appxListingDetail?listingId=a0N3A00000FADZgUAP • SAP: https://www.sap.com/about/trust-center/data-privacy.html und https://en.libelle.com/products/datamasking

Konzepte



Christian Bosse christian.bosse@ita-kl.de

Partizipatives Vorgehensmodell

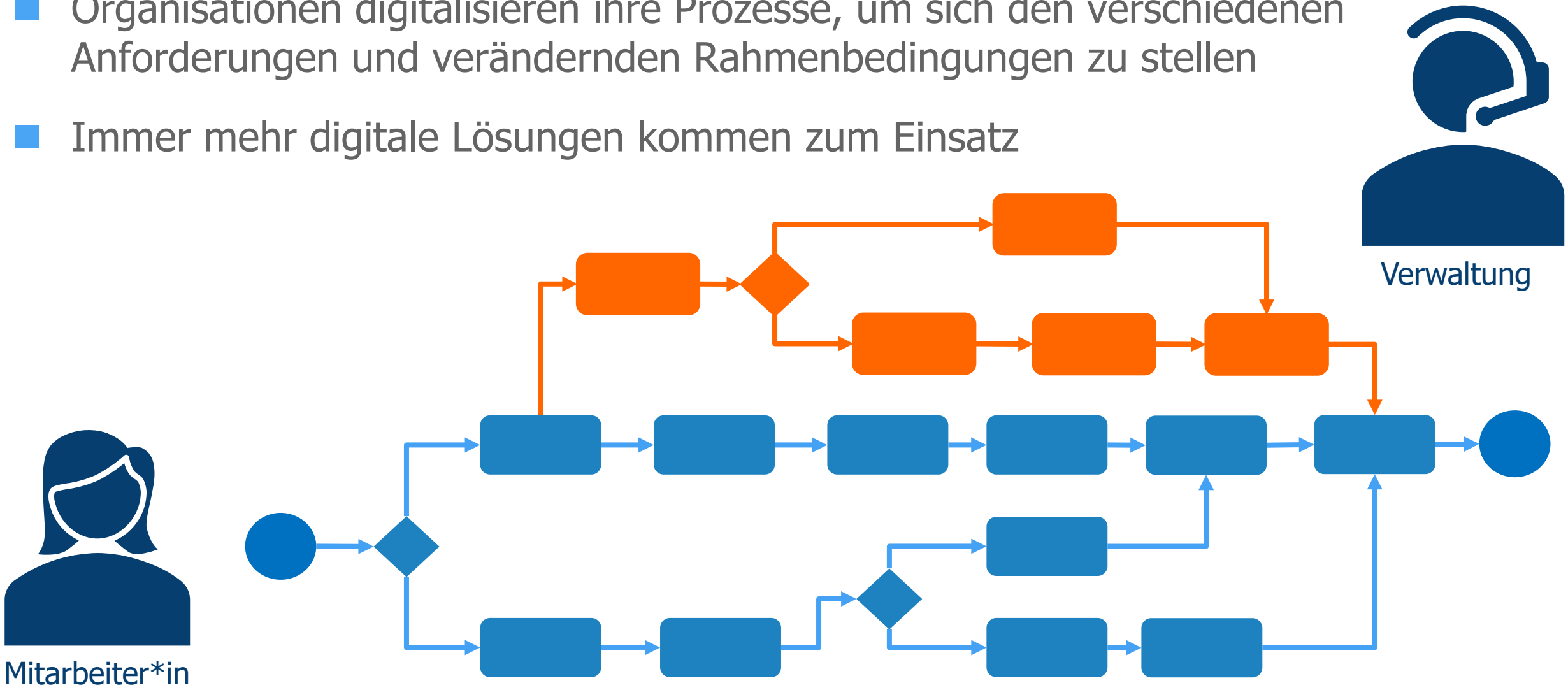
Die Technologieeinführung erfolgreich gestalten

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Warum sollten Nutzer*innen bei der Technologieeinführung einbezogen werden?

Motivation

- Organisationen digitalisieren ihre Prozesse, um sich den verschiedenen Anforderungen und verändernden Rahmenbedingungen zu stellen
- Immer mehr digitale Lösungen kommen zum Einsatz



Motivation

Warum soll ich das auch noch machen? Ich hab schon genug zu tun!

Warum zieht sich die Software nicht die Daten aus dem bestehenden System? Es sind doch alle Infos vorhanden!

Noch ein Programm mehr, in dem ich mich anmelden soll? Das dauert alles ewig und ist zu viel parallel!

Wie funktioniert die neue Software überhaupt?

Was muss ich machen, um die neue Software nicht nutzen zu müssen?

Wie kann ein Privacy-Dashboard erfolgreich eingeführt werden?

Orientierung am digitalen Transformationsprozess

Planungsphase

- Gemeinsame **Vision mit Zielen** der Organisation erarbeiten
- **Information** bzgl. der gesetzlichen und organisationsinternen Regelungen
- **Sensibilisierung** der Beschäftigten für den Wandel bzw. das Thema (Beschäftigten-) Datenschutz
- **Bewusstsein schaffen** für die eigene Rolle im Wandel und bspw. Wert der eigenen sensiblen Daten
- **Transparenz herstellen** über das Vorhaben und die Prozesse, bspw. die Datenverarbeitung

Umsetzungsphase

- **Einbezug der Beschäftigten** in die Anforderungserhebung und Umsetzung in der Organisation
- Betrachtung der aktuellen **Arbeitsprozesse** (Ist-Analyse) und Anpassung (Soll-Prozesse)
- Identifikation und Definition von **technischen Schnittstellen**
- Passgenaue Entwicklung von relevanten **Kompetenzen** abhängig von den Personas
- Regelmäßige **Information** über Status und Fortschritt

Auswertungsphase

- **Ansprechpartner und Befähiger** etablieren
- **Unterstützungsbedarfe** identifizieren
- Häufige Probleme/ Fragen und deren **Lösungsansätze** dokumentieren
- **Funktionsfähigkeit und Passgenauigkeit** evaluieren
- **Akzeptanz** bei den Beschäftigten evaluieren
- Möglichkeiten der **Optimierung** reflektieren

Phasen und Methoden im Vorgehensmodell

Sensibilisierung

- Schulungen allg. zu Datenschutz und aktueller Rechtslage
- (Weiter-) Entwicklung von internen Regeln und Prinzipien
- Fehlerkultur/ offene Unternehmenskultur etablieren
- Veränderungsbereit-schaft herstellen

Information

- Informations-veranstaltungen
- Projektsteckbrief
- Handreichung bzw. Projektflyer
- Vorführung von Imagefilmen oder Demonstration
- Mitarbeiterbeteiligung

Qualifizierung

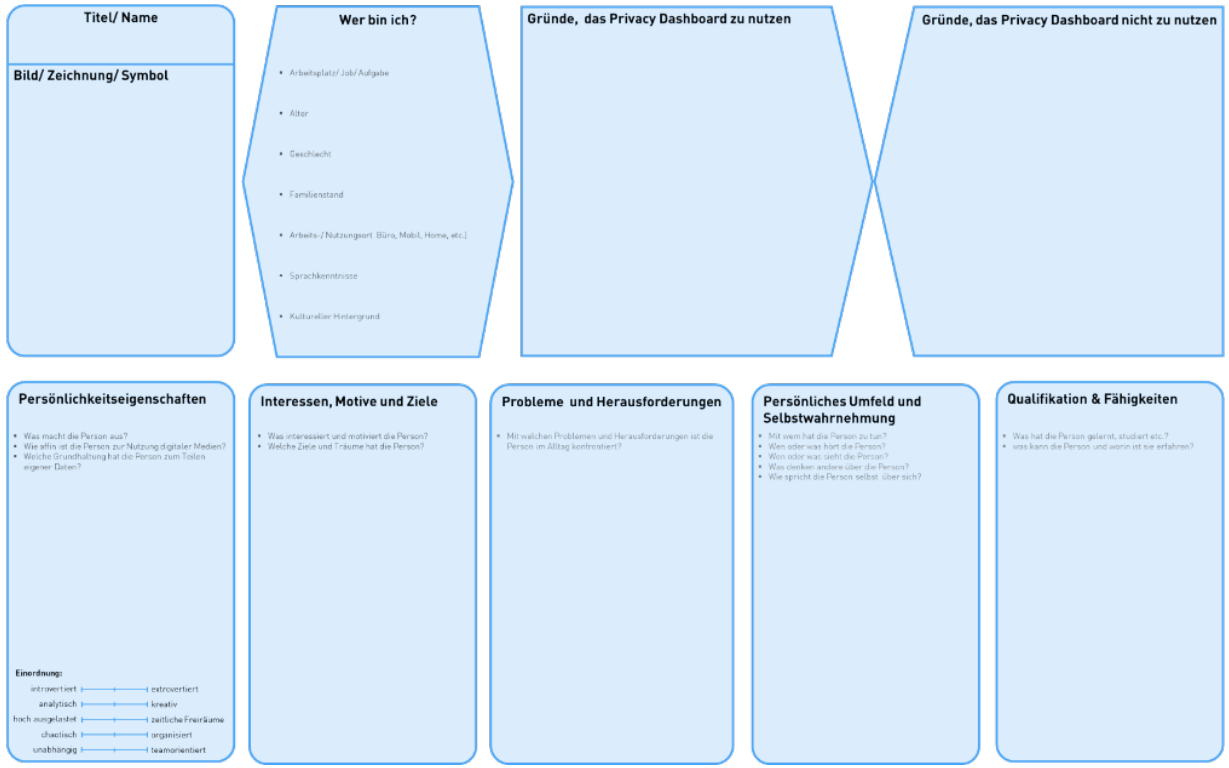
- Einführungsschulung (Training off the job)
- Vertiefungsschulung (Training on the job)
- Handbuch und/ oder Kurzanleitung zu zentralen Funktionen
- Praxisnahe Schulungsbeispiele

Unterstützung

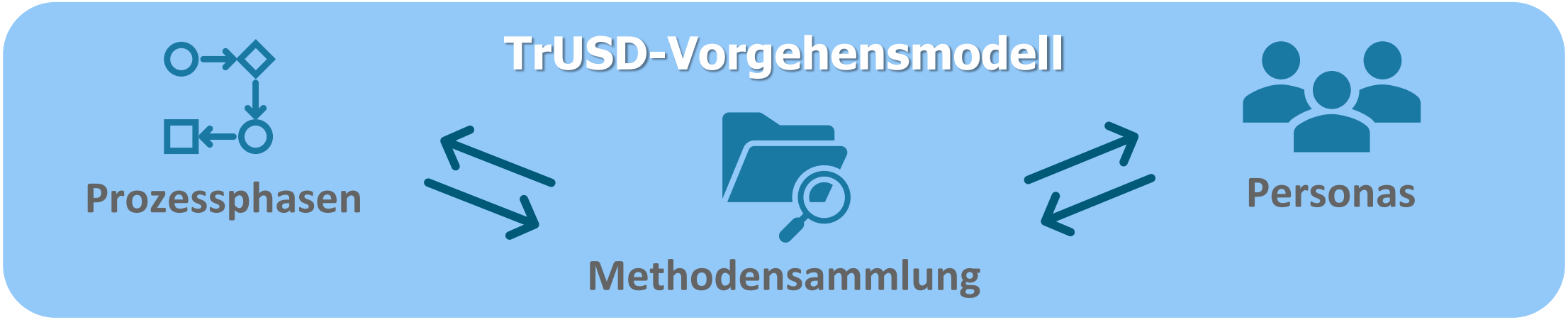
- Ansprechpartner/ Enabler etablieren
- Austausch-Formate (z.B. Info-Markt)
- Lern-Tandems bilden
- Entwicklung eines FAQs und/ oder Wikis

Betrachtung der Privacy-Personas

- Nicht alle Menschen sind gleich, sie unterscheiden sich in ihren:
  - Kompetenzen und Qualifikationen
  - (Vor-) Erfahrungen
  - Mentalen Modellen
  - Bedürfnissen und Anforderungen etc.
- Betrachtung der Beschäftigten und Abstraktion von entsprechenden Personas (archetypischen Nutzer) in der Organisation:
  - Entwicklung eigener Personas (Nutzertypen) mit Hilfe eines im Projekt entwickelten Persona-Templates und Workshop-Konzepts



Einführungskonzepte organisationsspezifisch ableiten



Organisationsspezifische Einführungskonzepte für Privacy-Dashboards

Einführungskonzepte organisationsspezifisch ableiten

Personas

Prozess-phasen

		Der unbekümmerte Mitarbeiter / die unbekümmerte Mitarbeiterin	Der verunsicherte Mitarbeiter / die verunsicherte Mitarbeiterin	Der pragmatische Mitarbeiter / die pragmatische Mitarbeiterin	Der geübte Mitarbeiter / die geübte Mitarbeiterin	Der passionierte Mitarbeiter / die passionierte Mitarbeiterin
Sensibilisierung	Informationsveranstaltung	●				
	Informationsbroschüre					
	Visionsentwicklung					
Information	Projektsteckbrief				●	
	Kraftfeld-Analyse					
	SWOT-Analyse					
	Demonstrator-Vorführung	●				
	Kick-off Veranstaltung				●	
Qualifizierung	Schulung (Einführung)	●				
	Vertiefende Schulung				●	
	Schulungsaufgaben/ Tutorials	●				
	Benutzerhandbuch					
Support	Ansprechpartner	●				
	Austauschbörse					
	FAQ					
	Wiki				●	

- Informationsveranstaltung „Datenschutz“
- Aushang „Projektsteckbrief“
- Vorführung von Demonstratoren
- Kick-off Veranstaltung
- Grundlagenschulung zur Einführung
- …

Weiterführende Informationen

Was?	Wo?
Arbeitswissenschaftliche Grundlagen	• Deliverable 7.2 – Bericht über die arbeitswissenschaftlichen Anforderungen an Privacy Dashboards bzw. an ein Vorgehensmodell zu deren betrieblicher Umsetzung • Tolsdorf, J.; Bosse, C.K.; Dietrich, A.; Feth, D.; Schmitt, H. (2020): Privatheit am Arbeitsplatz. Transparenz und Selbstbestimmung bei Arbeit 4.0. Datenschutz und Datensicherheit, 44(3), S. 176-181. Verfügbar unter URL: https://rdcu.be/b187e
Vorgehensmodell & Personas	• Deliverable 2.3 – Dokumentation des Vorgehensmodells • Projektergebnis: Einführung von Privacy-Dashboards – Leitfaden für Unternehmen • Bosse, C.K.; Dietrich, A.; Schmitt, H. (2021): IT-Rahmenwerk für den Beschäftigtendatenschutz. Technologieeinführung aus rechtlicher und arbeitswissenschaftlicher Perspektive. In: Reussner, R. H., Koziolek, A.; Heinrich, R. (Hrsg.), INFORMATIK 2020, S. 815-828. Bonn: Gesellschaft für Informatik. Verfügbar unter URL: https://dl.gi.de/bitstream/handle/20.500.12116/34785/C19-1.pdf?sequence=1&isAllowed=y • Bosse, C.K.; Dietrich, A.; Kelbert, P.; Küchler, H.; Schmitt, H.; Tolsdorf, J.; Weßner, A. (2020): Beschäftigtendatenschutz: Rechtliche Anforderungen und technische Lösungskonzepte. In: Schweighofer, E.; Hötzendorfer, W.; Kummer, F.; Saarenpää, A. (Hrsg.) Verantwortungsbewusste Digitalisierung. Tagungsband des 23. Internationalen Rechtsinformatik Symposions IRIS 2020, S. 175-182. Vachendorf: Nova MD.
Ableitung von Einführungskonzepten	• Deliverable 3.1 – Dokumentation der Konzepte zur Erstellung und Einführung von Privacy Dashboards

Agenda

I. **Big Picture**
Die Ideen hinter dem Projekt »TrUSD«.

II. **Umsetzungsbeispiele**
So können Privacy-Dashboards in der Praxis gestaltet sein.

III. **Werkzeugkasten**
So können Sie das Privacy-Dashboard auf Ihr Unternehmen maßschneidern.

IV. **Lessons Learned**
(Überraschende) Erkenntnisse aus dem Projekt.

V. **Diskussionsrunde**
Offene Punkte, Ausblick.

Lessons Learned

(Überraschende) Erkenntnisse aus dem Projekt.

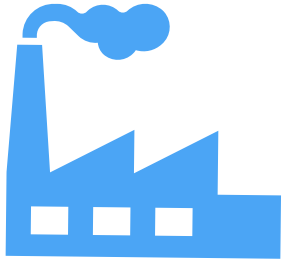
GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

Privacy Dashboards sind immer für die anderen Unternehmen gut.

Würden Sie Privacy-Dashboards bei sich einsetzen?

„setzt eine bestimmte Unternehmenskultur voraus"

„Mitarbeiter werden PDB nicht nutzen"
„kein Interesse"
„erst bei Störfall"



„je größer, desto sinnvoller"
„auf einen Schlag viele Personen"

„eher Ergänzungsinstrument"

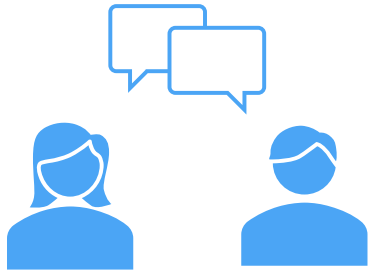
„PDB kann schnell zum Tragen kommen"

„Mitarbeiter fragen eher persönlich nach"

Privacy-Dashboards lösen nicht alle Datenschutzprobleme im Unternehmen.

Privacy-Dashboards schützen nicht vor…

Phishing



Zwischenmenschliche Beeinflussung

Anpassung an das Verhalten der Gruppe

Schlechte Voreinstellungen

Druck durch Vorgesetzte

Datennutzer wollen rechtskonform handeln, wissen aber nicht wie.

Privacy-Dashboards bringen Klarheit

Ohne Privacy-Dashboard

- Unklare Regeln
- Unwissenheit
- Unsicherheit
- Kompliziert
- Abhängigkeiten von anderen Abteilungen
- Dezentrale Datenablage
- …

Mit Privacy-Dashboard

- Klare Handlungsanweisungen
- Checklisten und Vorlagen
- Organisationsweites einheitliches Vorgehen
- Zentraler Zugriff auf Daten
- …

Privacy-Dashboards können die Privatsphäre gefährden.

Das sollte man beachten

Höhere Transparenz
→ mehr Daten mit Personenbezug

Dashboard basiert selbst auf Daten
→ widerspricht Datenminimierung

Zentrales System
→ Attraktives Angriffsziel

Verweigerte Einwilligungen behindern Kollegen
→ Sozialer Druck entsteht.

Privacy-Dashboards können zu Misstrauen führen.

Privacy-Dashboards müssen mit Bedacht eingeführt werden

Höhere Transparenz
→ Misstrauen unter den Beschäftigten

Wissen um die Verarbeitung personenbezogener Daten
→ Verhaltensänderungen.

Wissen um den Umfang der Datenverarbeitung
→ Gefühl der Überwachung und Steuerung

Offener Umgang mit der Datenverarbeitung
→ Mögliche Übersensibilisierung

Mitarbeiter vertrauen ihrem eigenen Arbeitgeber und ihren Kollegen.

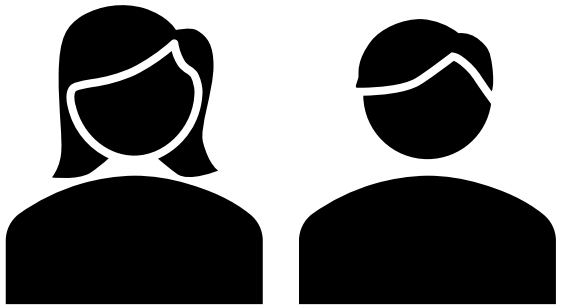
Aus Bequemlichkeit?

Vertrauen ist gut, Kontrolle ist (zu) kompliziert

Ich kann meine Kollegen ja nicht kontrollieren. Ich vertraue also darauf, dass sie die Daten nicht missbrauchen.

Ich habe absolut keine Ahnung wo meine Daten hingehen. Aber das ist wie bei Banken: Man geht einfach davon aus, dass alles gut ist.

Ich habe keine Lust jeden Tag 10000 Einstellungen vorzunehmen



Abschließende Diskussionsrunde

Leitfragen für die Diskussion

- Was sind für Ihr Unternehmen die größten **Mehrwerte**, die sich aus einem Privacy-Dashboard ergeben?
- Welche Bausteine sind für Sie als **Arbeitgeber** am relevantesten?
- Welche Bausteine sind für Sie als **Arbeitnehmer** am relevantesten?
- …

Vielen Dank!