Telekom MMS

EXPERIENCE
BEYOND
DIGITAL

11.09.2023 II ULD Sommerakademie II Block 1 06

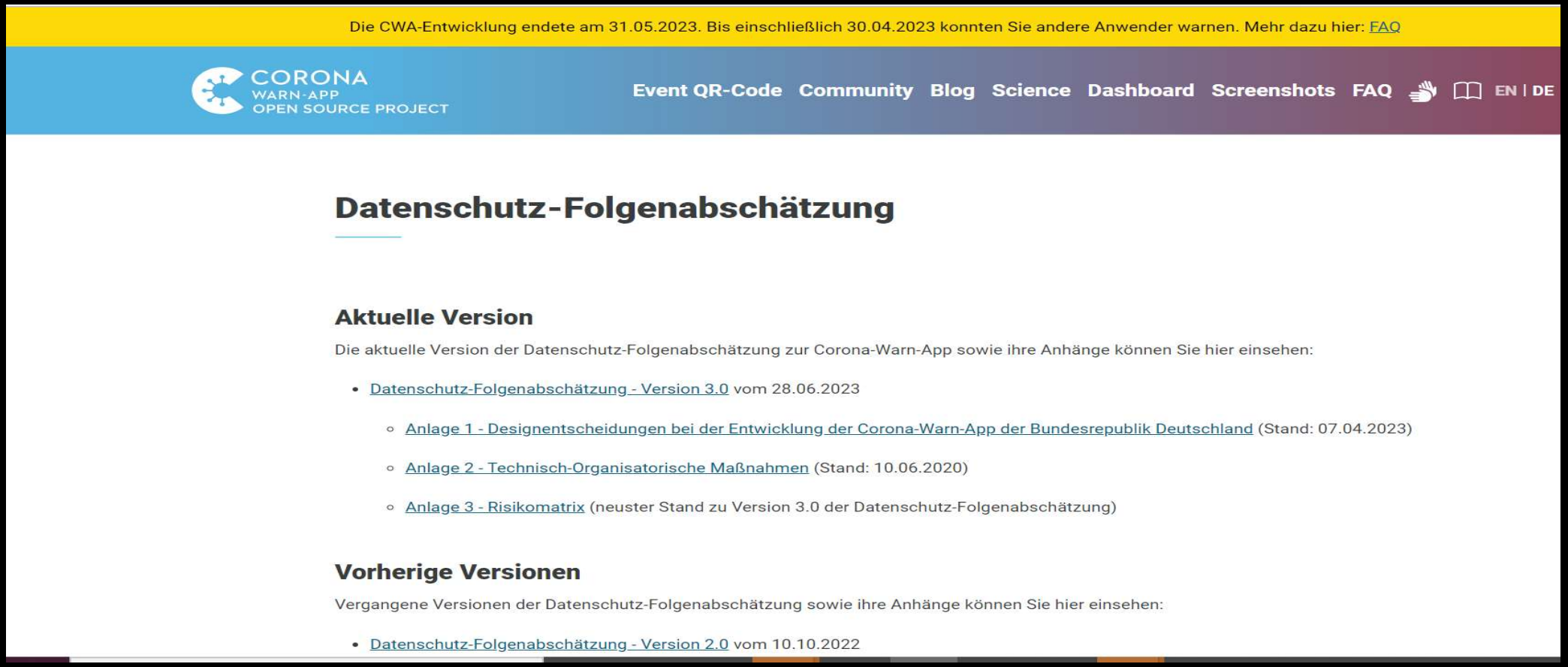
Entwicklungsbegleitende, risikobasierte Datenschutzberatung:

Das Erfolgsmodell hinter der deutschen Corona-Warn-App

Die Corona Warn-App: Retrospektive

CWA: Ein Open Source Projekt.

DSFA: Fortlaufende Veröffentlichung.



Die CWA-Entwicklung endete am 31.05.2023. Bis einschließlich 30.04.2023 konnten Sie andere Anwender warnen. Mehr dazu hier: FAQ

CORONA WARN-APP OPEN SOURCE PROJECT

Event QR-Code Community Blog Science Dashboard Screenshots FAQ EN | DE

Datenschutz-Folgenabschätzung

Aktuelle Version

Die aktuelle Version der Datenschutz-Folgenabschätzung zur Corona-Warn-App sowie ihre Anhänge können Sie hier einsehen:

- Datenschutz-Folgenabschätzung - Version 3.0 vom 28.06.2023
  - Anlage 1 - Designentscheidungen bei der Entwicklung der Corona-Warn-App der Bundesrepublik Deutschland (Stand: 07.04.2023)
  - Anlage 2 - Technisch-Organisatorische Maßnahmen (Stand: 10.06.2020)
  - Anlage 3 - Risikomatrix (neuster Stand zu Version 3.0 der Datenschutz-Folgenabschätzung)

Vorherige Versionen

Vergangene Versionen der Datenschutz-Folgenabschätzung sowie ihre Anhänge können Sie hier einsehen:

- Datenschutz-Folgenabschätzung - Version 2.0 vom 10.10.2022

Workstream Datenschutz: Themenschwerpunkte.

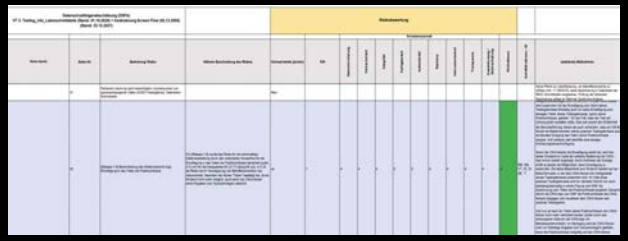
Datenschutzkonzepte für CWA-Backend

(initial + fortlaufend aktualisiert):

- ✓ DSK Rahmenkonzept
- ✓ DSK Testresult Server
- ✓ DSK Verifikations Server
- ✓ DSK Verifikations Hotline
- ✓ Designentscheidungen

Unterstützung der Datenschutzfolgenabschätzung des RKI (initial und fortlaufende Durchführung der Risikobewertungen):

- ✓ VT „Tracing, Warnung“
- ✓ VT „Hotline“
- ✓ VT „Laboranbindungen“
- ✓ VT „Impfzertifikate“
- ✓ VT „EFGS“
- ✓ VT „Datenspende“

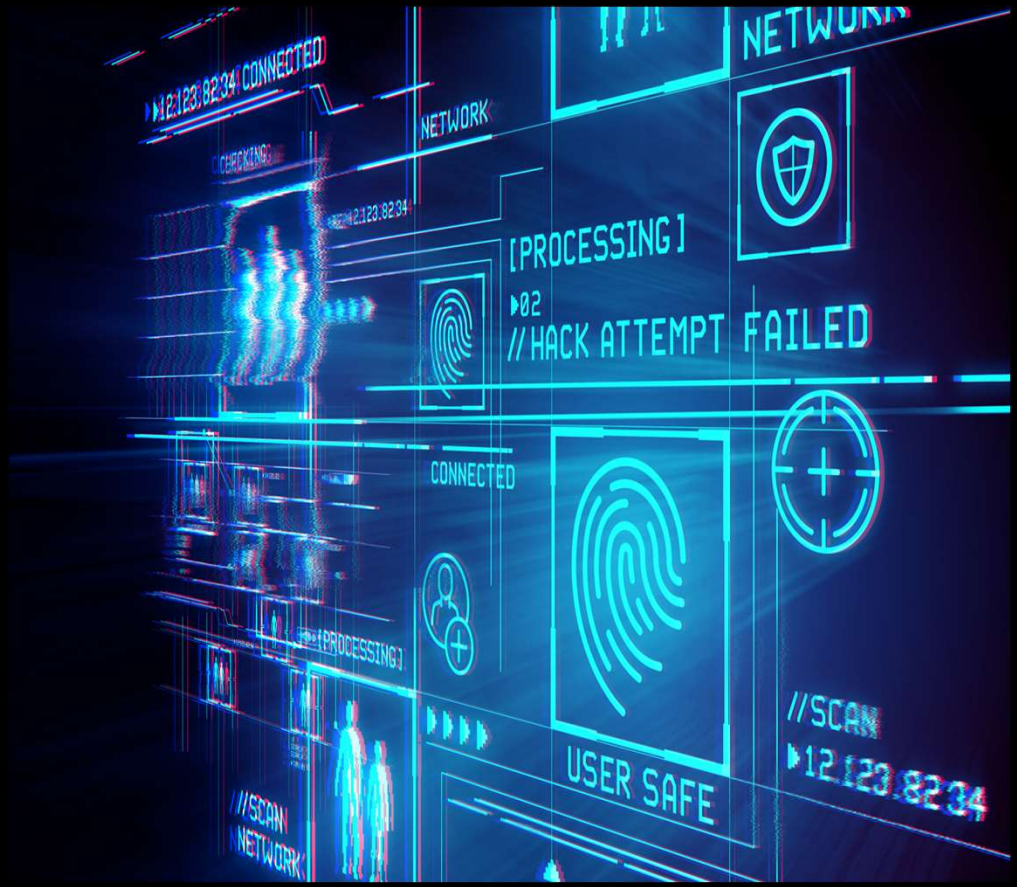


entwicklungsbegleitende, risikobasierte Datenschutzberatung

- ✓ Privacy by design / default
- ✓ Umsetzung Datenschutzprozesse durch TSI (Betroffenenanfragen, Meldung Datenschutzvorfälle)
- ✓ Kommunikation mit Datenschutzbeauftragten des RKI, Aufsichtsbehörde(n)

Privacy@CWA: ZDF.

- Projektlaufzeit: 37 Monate (05/ 2020 05/ 2023)
- 10.764 MMS Projektstunden
- 1.772 Dateien archiviert (Lieferungen an RKI)
- < 10 Meldungen (pot.) DS Vorfälle an GPR / RKI
- < 2 Meldungen an HessDSB (keine Rügen)



Privacy@CWA: 3 Jahre als project flow .

04.05.2020: F rst Call
09./12.06.: DSFA@BfD
15.06.2020: GoL ve
16.06.: PK der Bundes reg erung

- 01.07.2020: TAN Hotl ne
- 16.07.2020: K ckoff EFGS
- 15.10.2020: Doku EFGS

- 03.11.2020: QR Code Dubletten
- 10.12.2020: Release 1.10 (KTB)

- 01/21 + 02/21
Release 1.11-1.13
(Begegnungsh stor e)
Evaluat onsber cht

- 03/21 05/21

Release 1.13 (DDP)
Release 1.14 (KTB-Erweiterung)
Release 1.15 (Schweiz-Anbindung)
Release 2.0 (Eventregistrierung)
Release 2.1 (Schnelltestanbindung)
Release 2.2 (Schnelltestprofil)
Release 2.3 (Impfnachweis)

- 06/21 09/21

Release 2.4
Release 2.5 (Familienfunktion Genesenenzertifikat)
Release 2.6 (Validation Rules)
Release 2.7 (Signaturprüfung)
Release 2.8
Release 2.9 (Sachsenfeature)
Release 2.10 (Druckfunktion+Benach. Auffrischu...

10/21 02/22:

Release 2.11
Release 2.12
Release 2.13
Release 2.14
Release 2.15 (Validation Service)

11/ 21: nteroperab l tät m t LUCA

01/22 05/22
Release 2.16 2.18

- 03/22
Revokat on L sten
v a Magenta CDN

- 07/22 09/22
Release 2.21 2.27
2.27: Anze ge Befre ung Maskenpfl cht

01-02/23: Erstellung Löschkonzepte CWA Backend nfrastruktur
+ Labore / Schnelltestpartner (PoC Portal)

01/23 05/ 23:
31.01.23: Abschaltung Hotl ne
Release 3.0: Schnelltest Feature
Release 3.2.(1) (Abschaltung
+ „V elen Dank Screen)

31.05.2023: Ende Projektvertrag m t BMG
31.06.2023: Löschprotokolle l egen vor!

Organisatorische Rahmenbedingungen: Herausforderung Projektmanagement

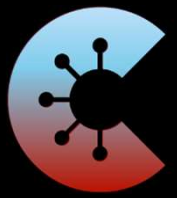
In 5 Wochen zum ersten Release der CWA.

Kernfrage: Wie können wir ein System gestalten, welches die geforderten Anwendungszwecke erfüllt und dabei die Rechte und Freiheiten der Betroffenen so wenig wie möglich einschränkt ?

Das erreichen wir durch:

- **Kooperation von Entwicklern, Security und Privacy**
- **Umsetzung von Datenschutzanforderungen**
  - Empfehlungen aus der Forschung
  - Best practice Erfahrungen
  - Unternehmensinterne Anforderungen
- **Zusätzliche Maßnahmen**
  - Externe Überprüfungen
  - Datenschutzfolgenabschätzung

Beispiel Corona Warn App:



- **Gemeinsame Architekturentscheidungen**
  - Anlage 1 zum DSFA Bericht der CWA
- **Externe Anforderungen**
  - Empfehlungen EDSA
  - Prüfsteine CCC
  - FIfF DSFA
  - Begleitung der Entwicklung durch den BfDI
- **Weitere Rahmenbedingungen**
  - https://github.com/corona-warn-app
  - Veröffentlichung der DSFA

Zusammenarbeit im Projekt.

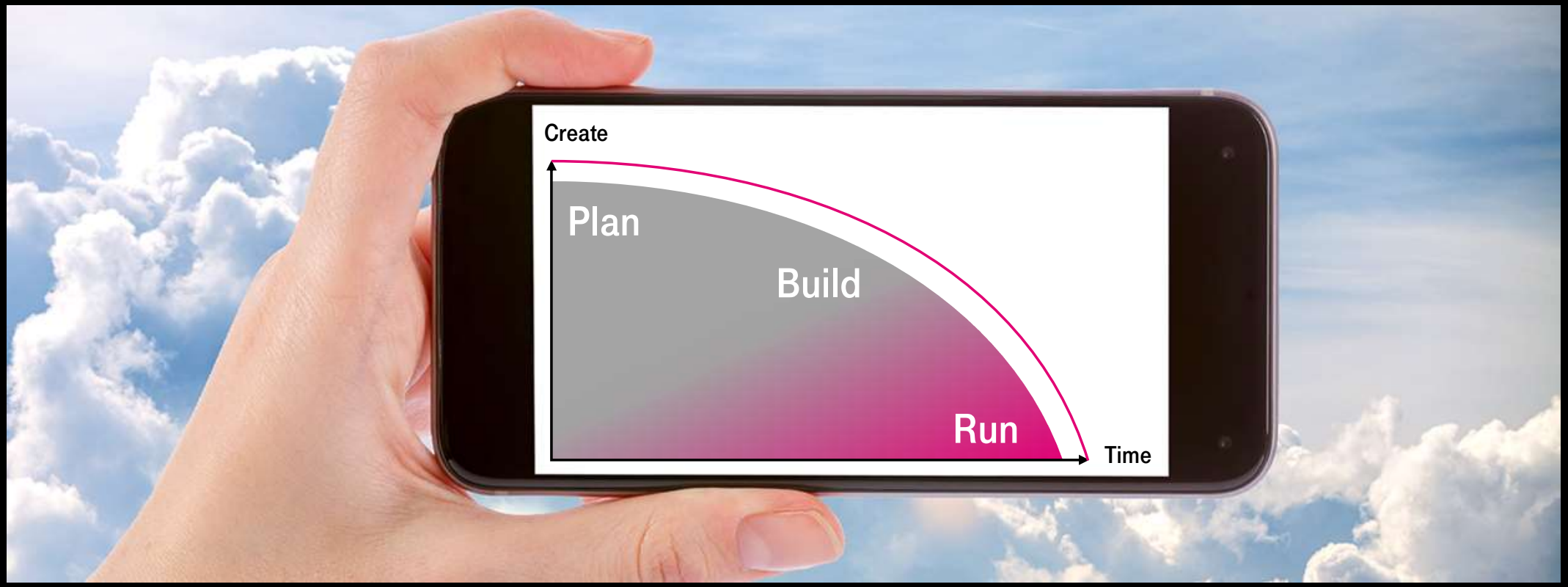
Beteiligte Rollen

- Produktverantwortliche / Auftraggeber
- IT-Architekt*innen / Entwickler*innen
- IT-Betrieb / Dienstleister
- Datenschutzberater*innen
- IT-Security
- Legal
- Risikomanagement

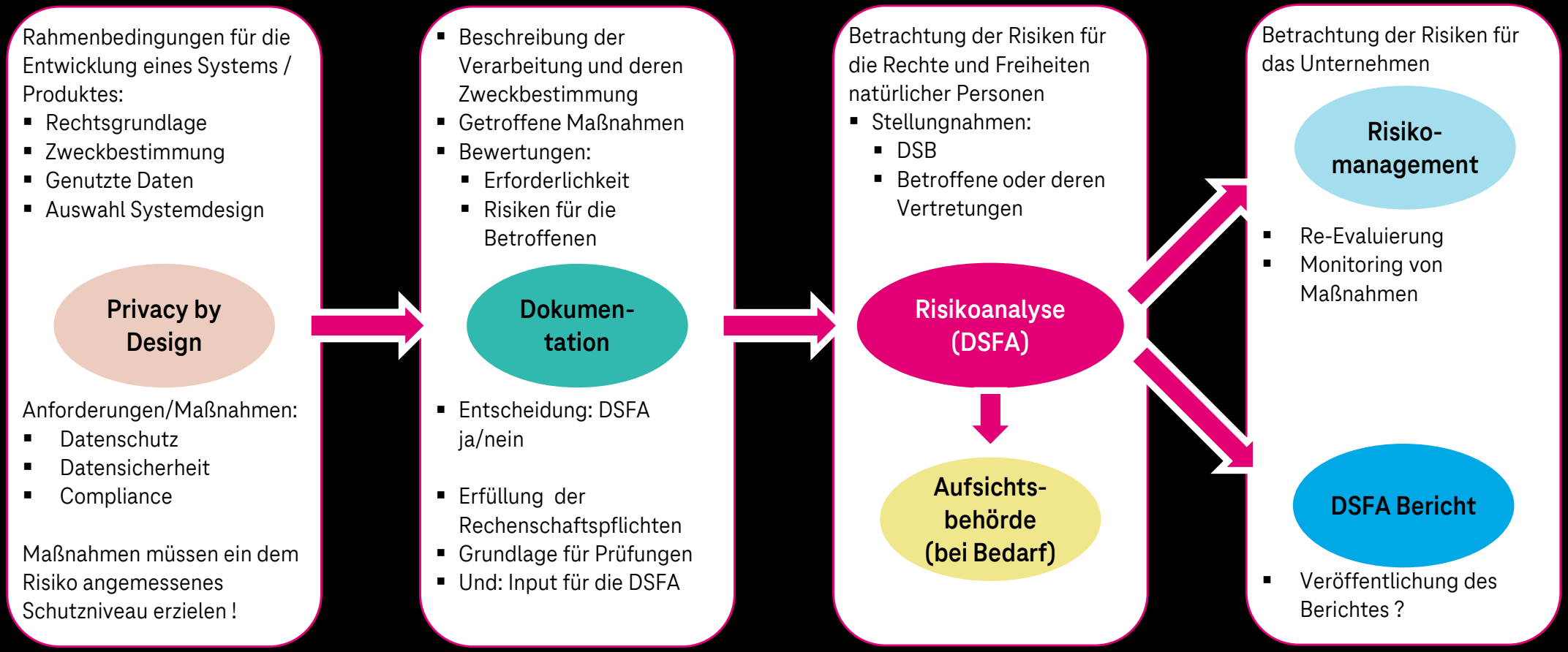
Formate der Zusammenarbeit

- Stakeholdermeetings
- Daily Scrums (Gesamtprojekt / Einzelteams)
- Scoping / Deep Dive
- Threat Modelling Workshops
- DSFA / Risikoworkshops
- Abstimmungsworkshops mit Aufsichtsbehörde

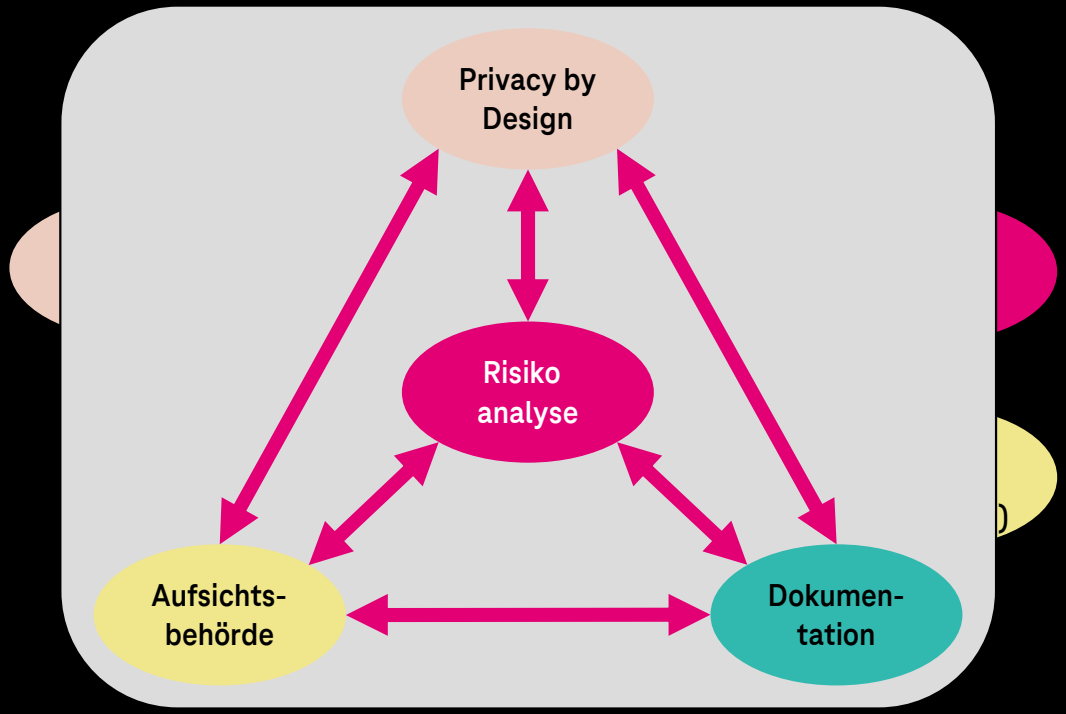
Frühzeitige Beteiligung sichert den größten Gestaltungsspielraum.

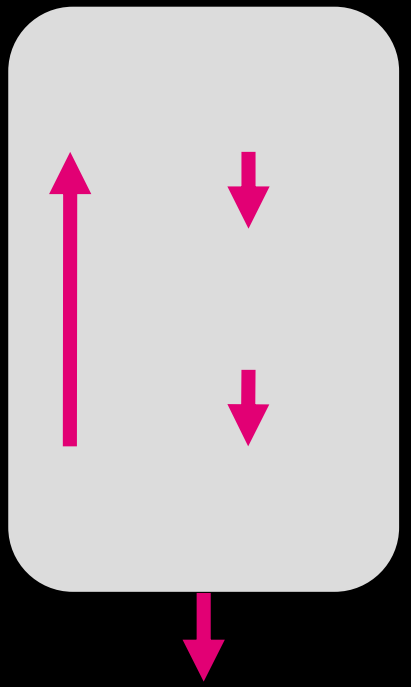


Einzelne Phasen auf dem Weg zur Datenschutzfolgeabschätzung.



Integration der einzelnen Phasen.



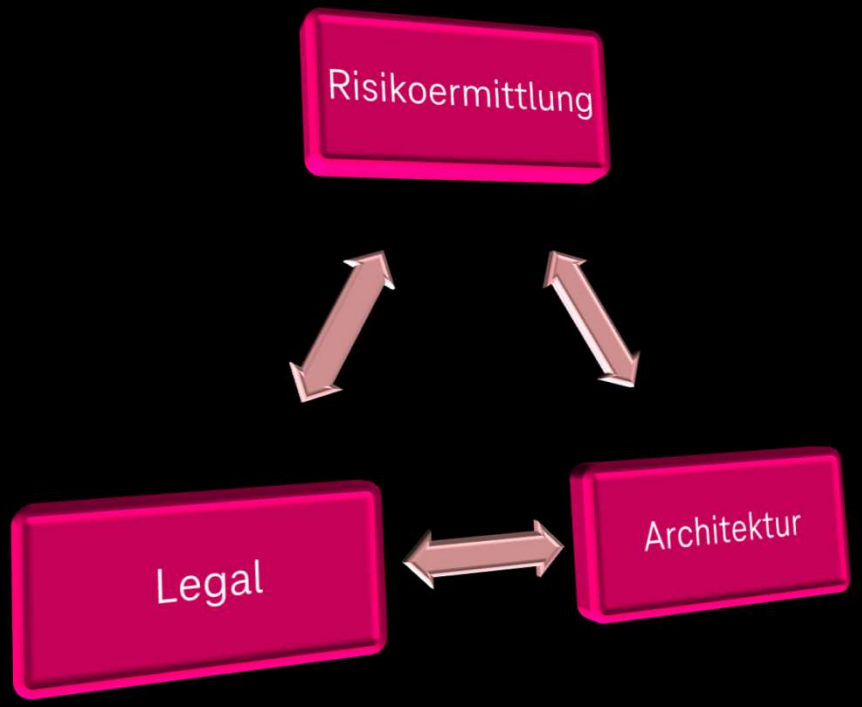


Die hier dargestellte Integration der Aufsichtsbehörde in den Prozess stellt sicherlich eine Ausnahme dar.


Risikobasiertes Vorgehen

Frühzeitige Risikoermittlung sichert höchstmögliche Gestaltung.

- **Architektur:** privacy / security by design, Beeinflussung technischer Spezifikation der Komponenten, Datenfluss, Monitoring u.a.
- **Entwicklung:** Umsetzung / Implementierung der Anforderungen, konkrete Lösungsfindung / Maßnahmenvarianz
- **Legal:** Rechtsgrundlage, Vertragsarten, Vertragspartner, -umfang, vertragliche Spezifikationen von DV, Haftungsklauseln, DL-Steuerung
- **Security/ Operation:** TOM, Prozessgestaltung
- **Kommunikation /Marketing:** DSFA als Teil des Produkts



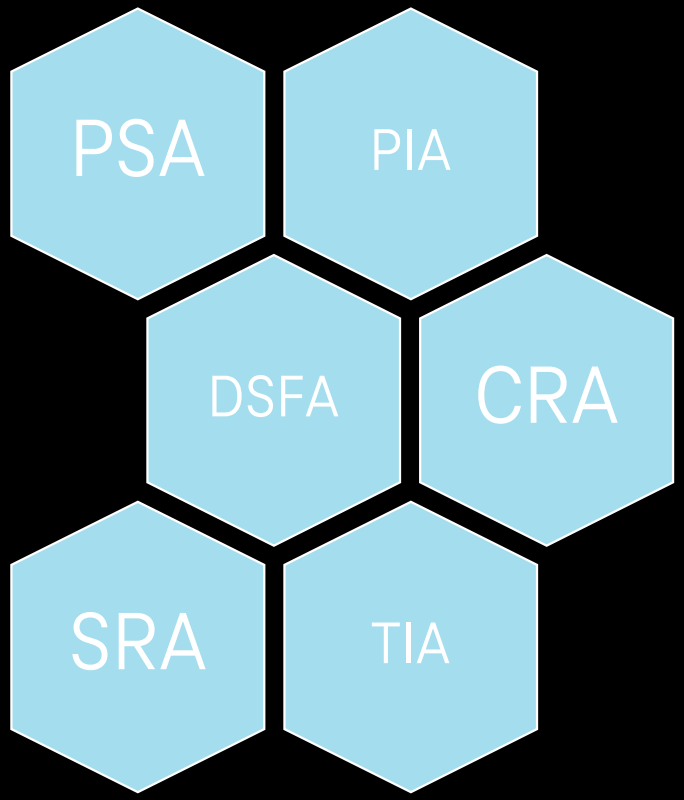
Unterschiedliche Aspekte von Risikobetrachtungen.

Was wird geschützt? (personenbezogene Daten von durch Datenverarbeitung Betroffenen, Informationen des Unternehmens …)

Schutzziele? [Informationelle Selbstbestimmung/ Rechte und Freiheiten betroffener Personen, Unternehmenssicht: Reputation, Geschäftsgeheimnisse, Assets und Umsatz, Schutz vor monetären Risiken (Bußgelder, Schadensersatz]

Wovor wird geschützt? (Schutz vor Datenmissbrauch, Datenpannen / Unternehmenssicht: Schutz vor Zerstörung, Manipulation …)

Wie wird geschützt? (Technische und organisatorische Maßnahmen)



Kombination von Risikobetrachtungen aus Betroffenen- und Unternehmenssicht!

Vielfältige Wege zur Risikoermittlung.

Risikoermittlung anhand potentieller Auswirkungen

Quelle

Ereignis

Auswirkung

Risikoermittlung anhand Nichterfüllung von Gewährleistungszielen

Eintrittswahrscheinlichkeit

×

Schwere des möglichen Schadens

Risikoermittlung anhand von Schadensszenarien

Angreifermodelle und -motivationen

Angriffsarten

Risiko Identifikation:
Modellierung von Risiko-Szenarien

Risiko/ "Ereignisgruppen" aus dem DSFA Handbuch (Fraunhofer).

Unbefugte oder unrechtmäßige Verarbeitung	Für die Betroffenen intransparente Verarbeitung	Unbefugte Weitergabe personenbezogener Daten oder unbefugter Zugriff auf diese	Unbefugte Übermittlung personenbezogener Daten (in ein Drittland)
Unabsichtlicher Verlust oder unabsichtliche Beschädigung personenbezogener Daten	Missachtung der Betroffenenrechte	Nutzung personenbezogener Daten zu neuen oder anderen Zwecken	Verarbeitung von als Nebenprodukt anfallenden und unerwarteten personenbezogenen Daten
Verarbeitung unrichtiger personenbezogener Daten	Fehlerhafte Verarbeitung personenbezogener Daten (technische Fehler, Programmfehler, menschliche Fehler)	Verarbeitung personenbezogener Daten über Speicherfrist hinaus,	Risiken für betroffene Personen, die sich aus der Verarbeitung ihrer personenbezogenen Daten selbst ergeben.

Die Dimensionen der Risikoanalyse

Bewertungskriterien und Dimensionen

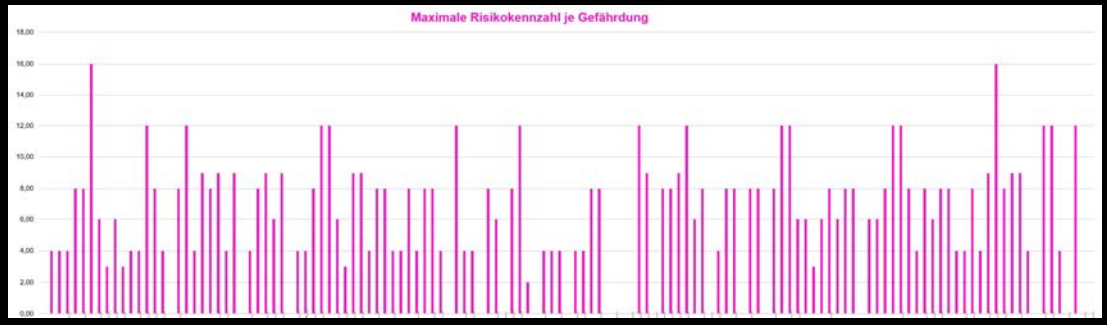
- Eintrittswahrscheinlichkeit (gering, mittel, hoch, sehr hoch) mit Ausprägungen im Hinblick auf Häufigkeit und erforderliches know how von Angreifern je Stufe
- Schadenskategorien (gering, mittel, hoch, sehr hoch) mit Ausprägungen im Hinblick auf die Rechte und Freiheiten der Betroffenen

Zusätzliche Aspekte

- Ausgeprägtes und szenariobezogenes Angreifermodell (> 10 Angreiferrollen, charakterisiert durch know how, Motivation und verfügbaren Ressourcen)
- Konkrete Beschreibung möglicher Angriffsarten (>10); Kombinationen sind möglich
- Differenzierung nach Betroffenengruppen möglich

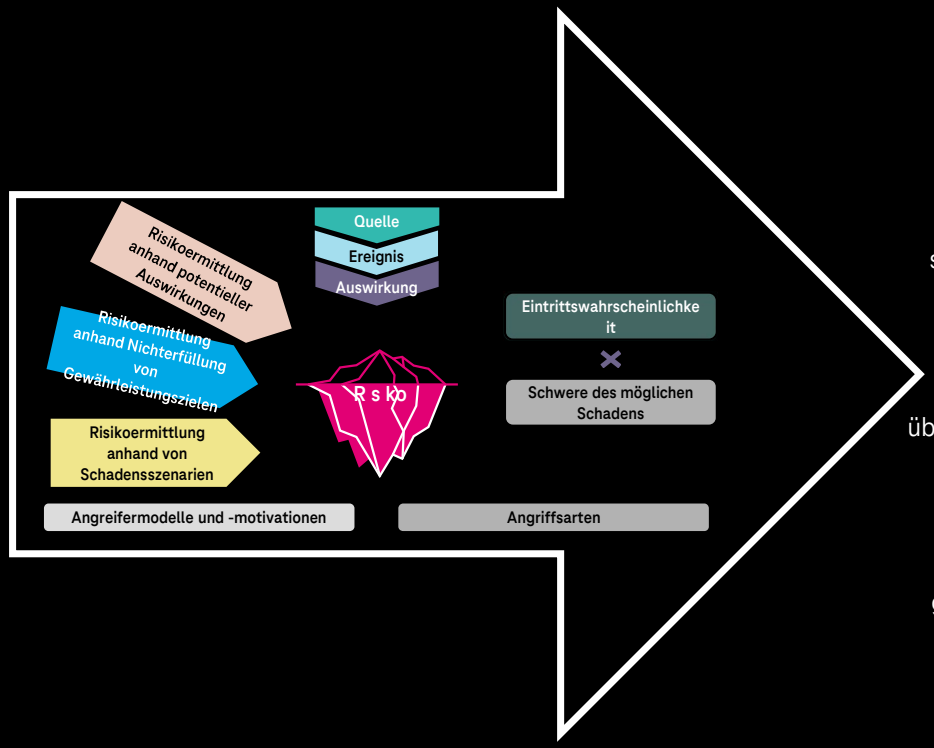
Risiken / Bedrohungen

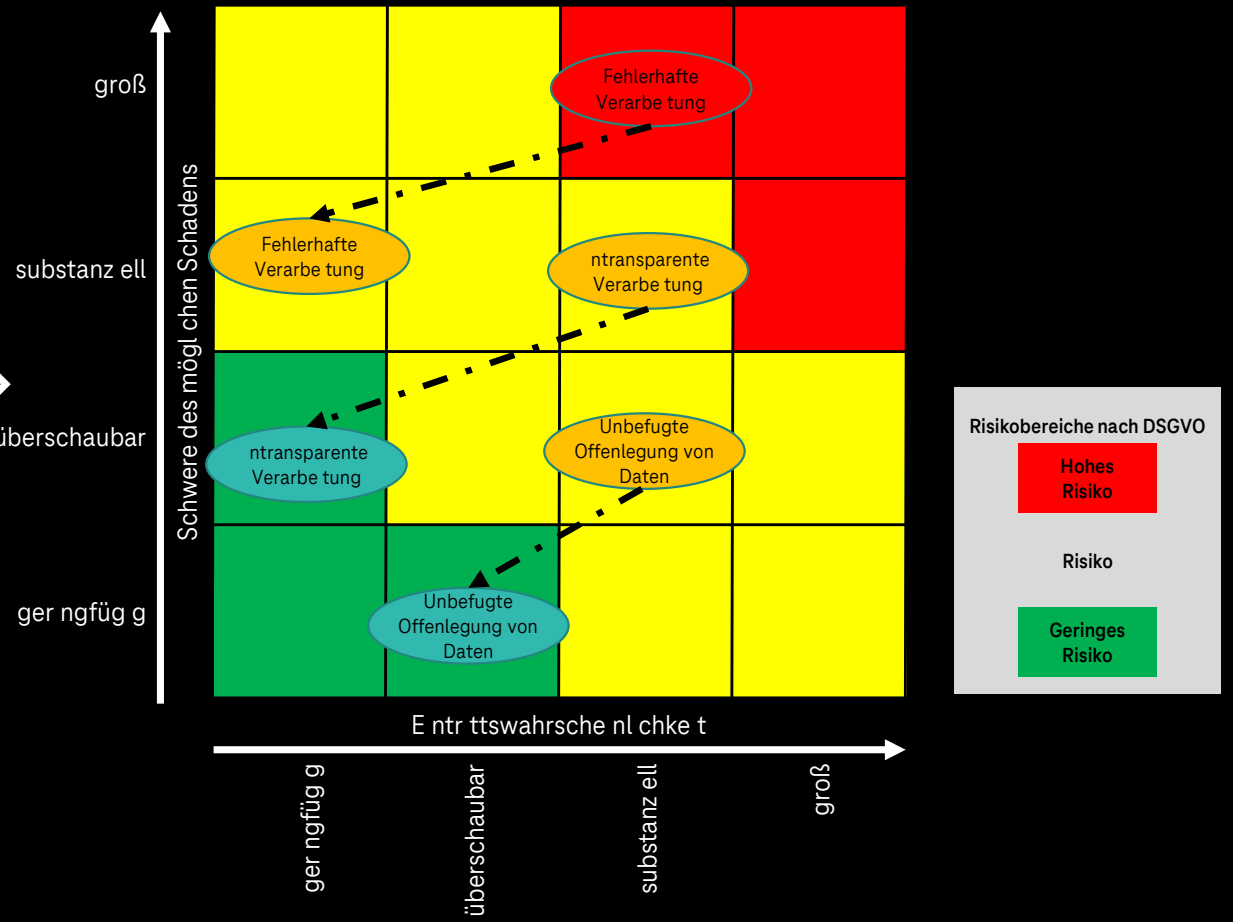
- Abgeleitet aus dem DSFA Handbuch von Fraunhofer, detailliert auf Grundlage des Angreifermodells, der Angriffsarten und der Kreativität erfahrener Datenschutz und IT Sicherheitsexpert*innen
- Spezifisch eingeschätzt in Bezug auf die Gewährleistungsziele des Standard Datenschutzmodells
- Jeweils der höchste Wert wird multipliziert mit der angenommenen Eintrittswahrscheinlichkeit



Risikobewertung – Risikohöhe, Schutzniveau, Restrisiko

Datenschutzfolgenabschätzung: Visualisierung von Risiken und deren Veränderung.





Konkrete Schadensszenarien pro Ereignisgruppe (Beispiel CWA).

Risiko-Quelle	Bedrohung/ Risiko	Schwachstelle (ja/nein)	EW	Datenminimierung	Vertraulichkeit	Integrität	Verfügbarkeit	Authentizität	Resilienz	Intervenierbarkeit	Transparenz	Zweckbindung /	Risikoklasse	Soll-Maßnahmen - ID	(etablierte) Maßnahmen
	Unbefugte Offenlegung von und Zugang zu Daten														
R1-CWA-Nutzer	Bewusste/ Unbewusste Erteilung von nicht-notwendigen Berechtigungen an CWA-Betreiber	Ja	1	4	4	4	0	0	0	2	4	4	4	DM, VT, IG, TR, ZB	Sicherheitseinstellungen Handynutzung / Restrisiko beim Nutzer - Designentscheidung D-2-2
R2-Hacker	Zugang / Zugriff trotz fehlender und unzureichender Berechtigungen zu Smartphone/ CWA/ ENF/ inkl. Elevation of Privilege (Ausweiten der Rechte)	Ja	2	4	4	4	0	0	0	2	4	4	8	DM, VT, IG, TR, ZB	Empfehlungen Handynutzung / Designentscheidungen (Containerisierung CWA - Designentscheidung D-2-2
R4-Apple / Google	Unbefugter Zugriff von Plattformen, die Kontaktereignisse ermitteln, auch für NutzerInnen ohne CWA	Ja	3	4	4	4	0	0	0	2	4	4	12	DM, VT, IG, TR, ZB	Dokument Designentscheidungen - Designentscheidungen zur Nutzung API


Designentscheidungen:
Bestimmung technisch und
organisatorischer Maßnahmen

Anlage 1: Designentscheidungen.

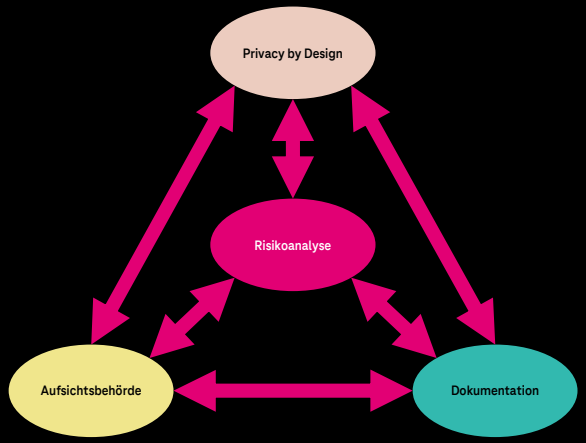
Beschreibung	ID	Quelle der Anforderung	Designentscheidungen/Bewertungen	Quelle
Begegnungshistorie Die Risikobegegnungen und Begegnungen mit niedrigem Risiko sollen tageweise im Kontakt-Tagebuch dargestellt werden. Damit kann der CWA-Nutzer nachvollziehen, an welchen Tagen die Risiko-Bewertung der CWA welches Risiko ermittelt hat. Die tageweise Darstellung erlaubt es besser als die aggregierende Darstellung (Begegnungen mit niedrigem Risiko an „x" Tagen / Begegnungen an „x" Tagen mit erhöhtem Risiko) in einem 14 Tage-Zeitraum (+ dem heutigen Tag) zu bewerten, an welchen Tagen ein erhöhtes Risiko erstmals oder auch wiederholt vorlag. Dies ermöglicht den CWA-Nutzern besser einzuschätzen, ob nach Feststellung des jeweiligen Risikos Änderungen des eigenen Verhaltens (z.B. Vermeidung bestimmter Orte oder von Treffen mit bestimmten Personenkreisen) angezeigt sind, um sich selbst, aber vor allem auch die eigenen Kontaktpersonen zu schützen. Eine Infektionskette kann - auch ohne Zutun der Gesundheitsbehörden im Rahmen der Kontaktverfolgung - schnell durch die Selbst-Isolation der CWA-Nutzer erreicht werden. Die aggregierte Darstellung ohne konkrete	D-2-4a		**Aufklärung der CWA-Nutzer zur Vermeidung von Fehlinterpretationen und „falscher Verdächtigung"** ✓ Mit der CWA-Version 1.2 wird die Information und Aufklärung über Funktionsweise und Aussagegehalt der Begegnungshistorie mehrschichtig durch Informationstexte erfolgen (Release-Info, Onboarding-Hinweis, FAQ). In der Kalenderansicht wird ein spezifischer Risikohinweis integriert und eingeblendet. Sofern etwa für einen Tag eine Risikobegegnung oder eine Begegnung mit niedrigem Risiko festgestellt wurde, wird ein ausdrücklicher Zusatz an dem jeweiligen Eintrag eingeblendet werden, dass diese Aussage nicht in direktem Zusammenhang mit den erfassten Personen oder Orten im Kontakt-Tagebuch stehen muss. ⚠ Die mit der Darstellung der Begegnungshistorie verbundenen Re-Identifizierungsrisiken und das Risiko einer falschen Verdächtigung wurde im Rahmen der DSFA bewertet.	CWA DSK v1.12, 6.6.1, DSK Rahmenkonzept v1.12, Kap. 14.28.19 (Risikobeschreibung)

Zusammenfassung

3 Säulen des Erfolgs.

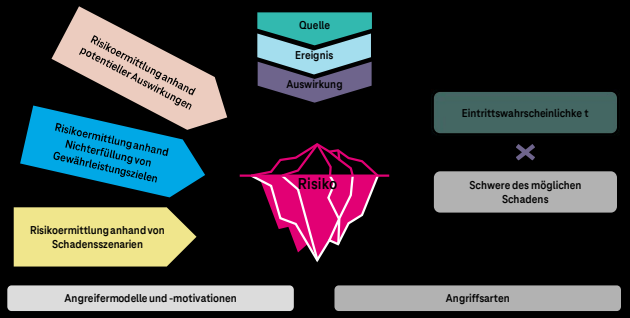
Entwicklungsbegleitende Datenschutzberatung

- Frühzeitige Beteiligung
- Zusammenarbeit von Entwicklung, Datenschutz, IT Sicherheit
- Privacy by Design, Dokumentation und Risikobewertung integrieren



Datenschutzfolgenabschätzung

- Angepasste Risikoermittlung
- Konkrete Vorstellungen von Angreifermodelle, Angriffsarten und Bewertungskriterien
- Detaillierte Betrachtungen entlang von Gewährleistungszielen
- Erfahrung und Kreativität



Risikomanagement

- DSFA Ergebnisse als Input für das Risikomanagement im Unternehmen
- Unterstützung bei der Bewertung von Unternehmensrisiken
- Integration von expliziten Risikobetrachtungen in die Datenschutzberatung

Wie wir mit Expertise, Innovation und Risikomanagement Lösungen ermöglichen:

1. interdisziplinäres Team mit technischem und juristischem KnowHow *(„Privacy engineering“)*

2. Privacy by Design *(„Privacy enables solutions!“)*

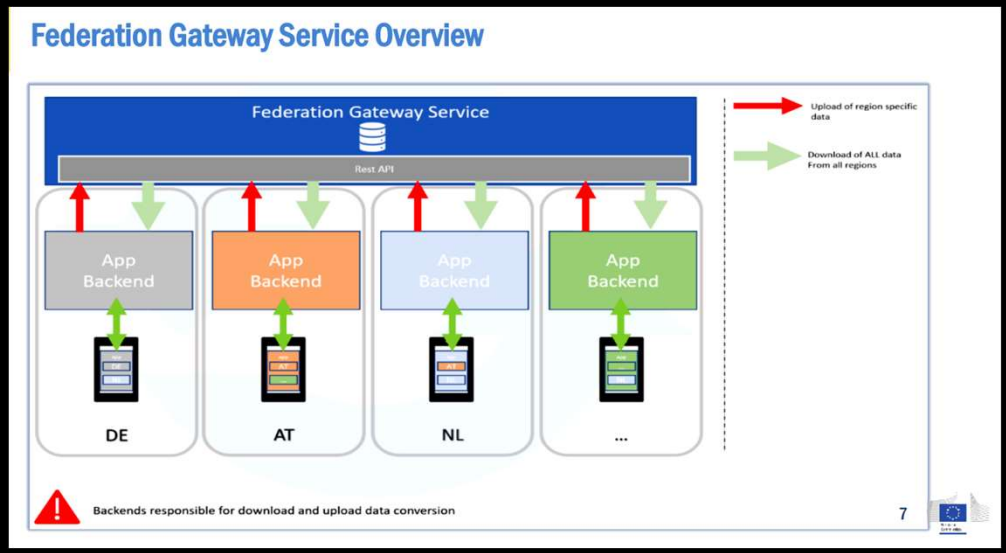
3. risikobasierte Datenschutzberatung von Konzeption bis zur Außerbetriebnahme *(„Holistic privacy consulting“)*

Entwicklungsbegleitende, risikobasierte Datenschutzberatung.

IT Projekte mit komplexen (Funktions) Anforderungen:

EFGS

Digital Covid Certificate



Weitere T Cloudifizierungsprojekte (Hyperscaler) in Arbeit...

T-Systems | Google Cloud

T-Systems Sovereign Cloud powered by Google Cloud