INTEGRATION VON DATENSCHUTZANFORDERUNGEN IN UNTERNEHMENSINTERNE ENTWICKLUNGSPROZESSE

DR. CLAUS D. ULMER, SVP GROUP PRIVACY DEUTSCHE TELEKOM

RISIKOFELDER IM DATENSCHUTZ

Verantwortliche Stelle.

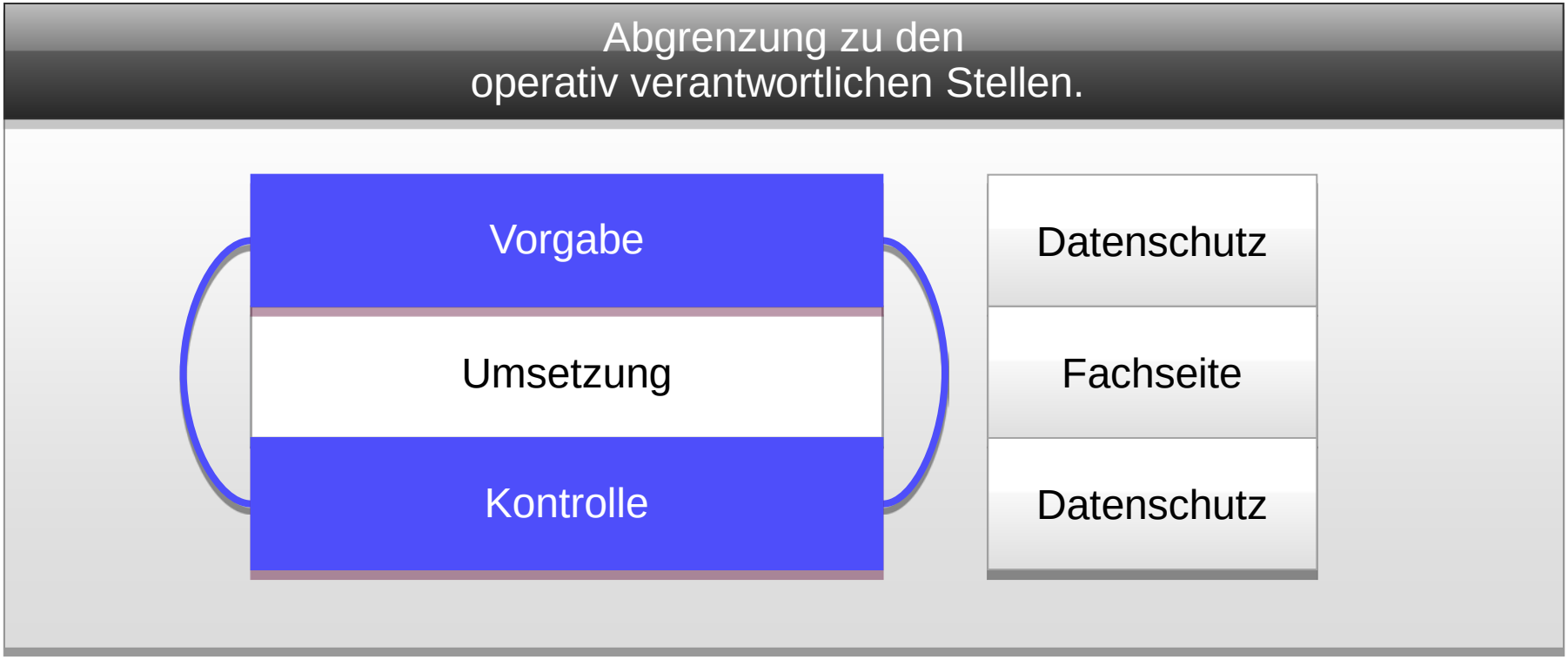
Strafverfolgungsrisiko.

Kommunikations-
/Reputationsrisiko.

Kosten-/Investitionsrisiko.

Betriebsrisiko.

DIE ZENTRALE AUFGABE DES DATENSCHUTZBEAUFTRAGTEN



Risikobasierte Betreuung von Entwicklungen und Projekten

PRIVACY & SECURITY ASSESSMENT (PSA)
DIE DESIGNKRITERIEN

- **Frühzeitigkeit**
- **Priorisierung**
- **Harmonisierung**
- **Standardisierung**
- **Verlässlichkeit**

- Sicherstellen der frühzeitige Einbindung von Datenschutz & Sicherheit.
- Hochkomplexe und kritische Projekte werden identifiziert und individuell beraten.
- Vermeidung von Doppelarbeiten für Datenschutz & Sicherheit
- Sicherstellung einheitlicher Bewertungsmaßstäbe für Datenschutz & Sicherheit
- Modularer, anforderungsbasierter Ansatz für sichere Umsetzung aller Maßnahmen im Projekt

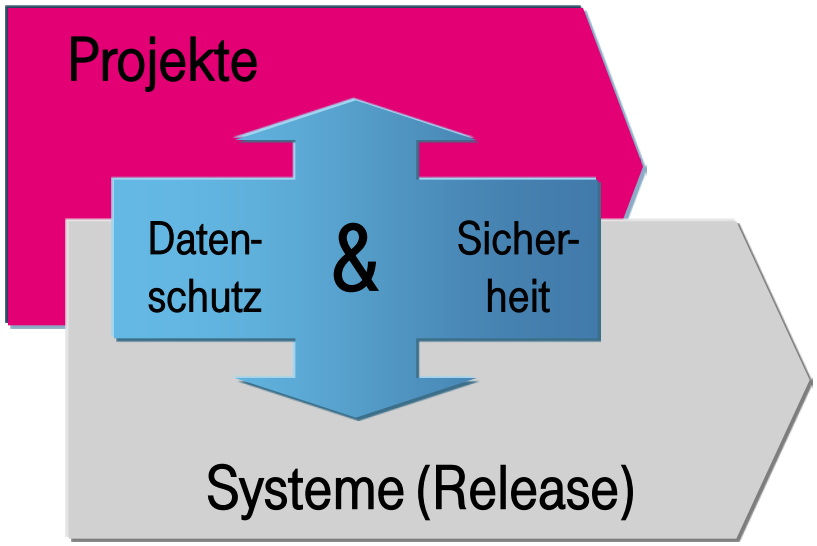
PRIVACY & SECURITY ASSESSMENT (PSA) INTEGRALER BESTANDTEIL DER ENTWICKLUNG

inhaltlich:

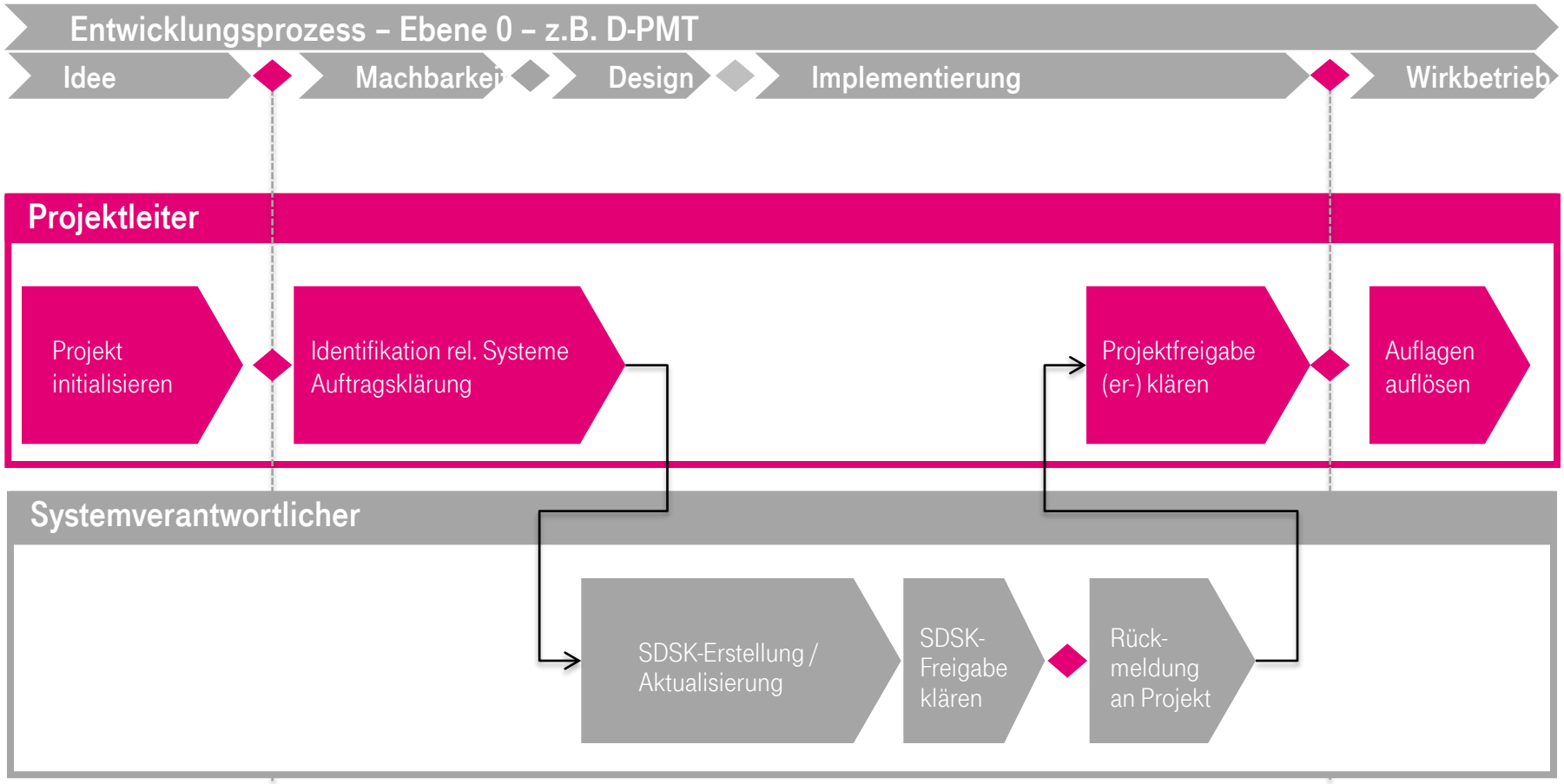
- Datenschutz & Sicherheit als integraler Bestandteil der:
  - Entwicklungsprozesse (PMT, E4R, D2S, ...)
  - Projektarbeit
  - Systembetrachtung
- Beratung, Dokumentation und Freigabe zu Sicherheit und Datenschutz

geografisch:

- in Deutschland verbindlich
- Einführung international seit 2011



PRIVACY & SECURITY ASSESSMENT (PSA)
VEREINFACHTER ABLAUF DES PSA-PROZESSES



PRIVACY & SECURITY ASSESSMENT (PSA)
DIE PSA DOKUMENTE

Jede Ebene arbeitet mit einem Dokument.

PSA-Freigabedokument

- Liste betroffener Systeme
- Konformitätserklärung der Systemverantwortlichen

Freigabeerklärung

Projektleiter

Standardisiertes Datenschutz & Sicherheitskonzept (SDSK)

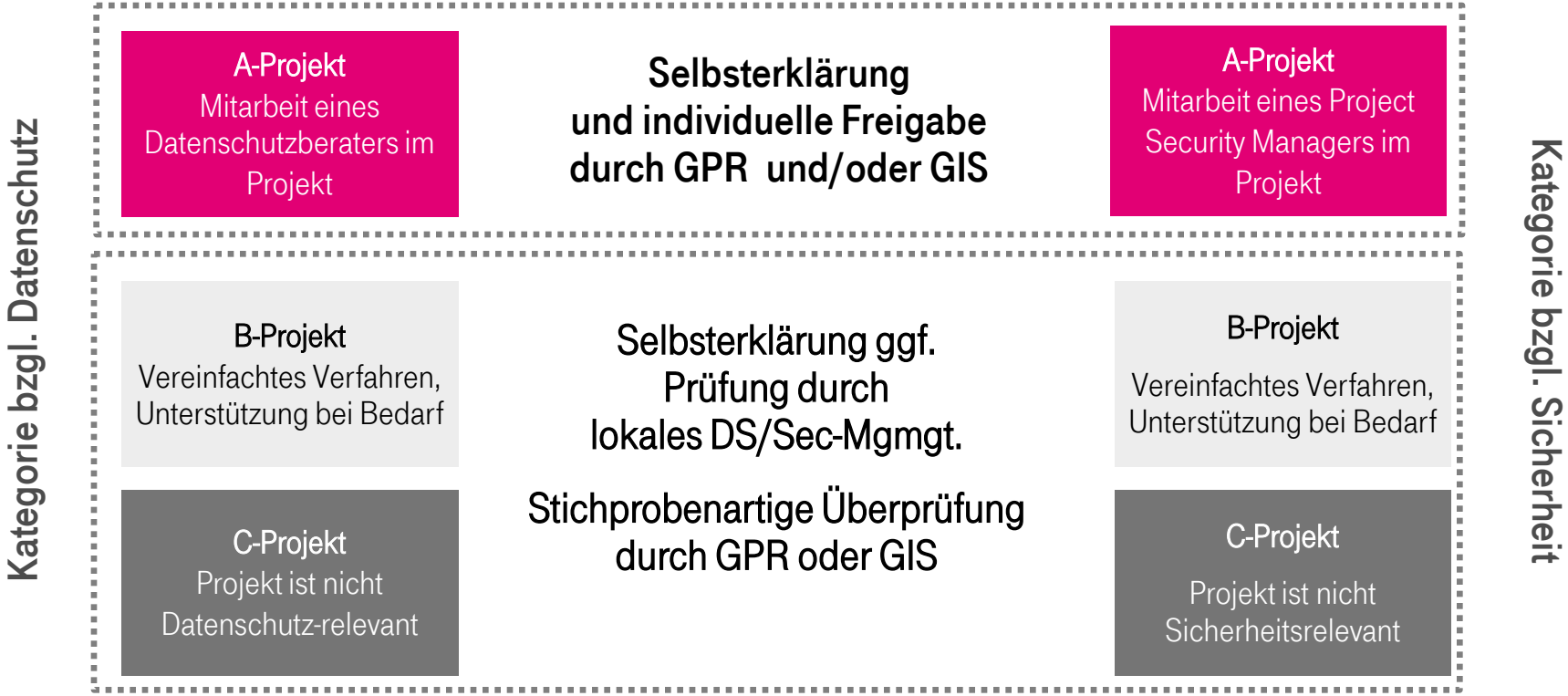
- Systembeschreibung
- Berechtigungskonzept
- Datenschutzinformation
- Anforderungskataloge
- Maßnahmenplanung

SDSK Deckblatt

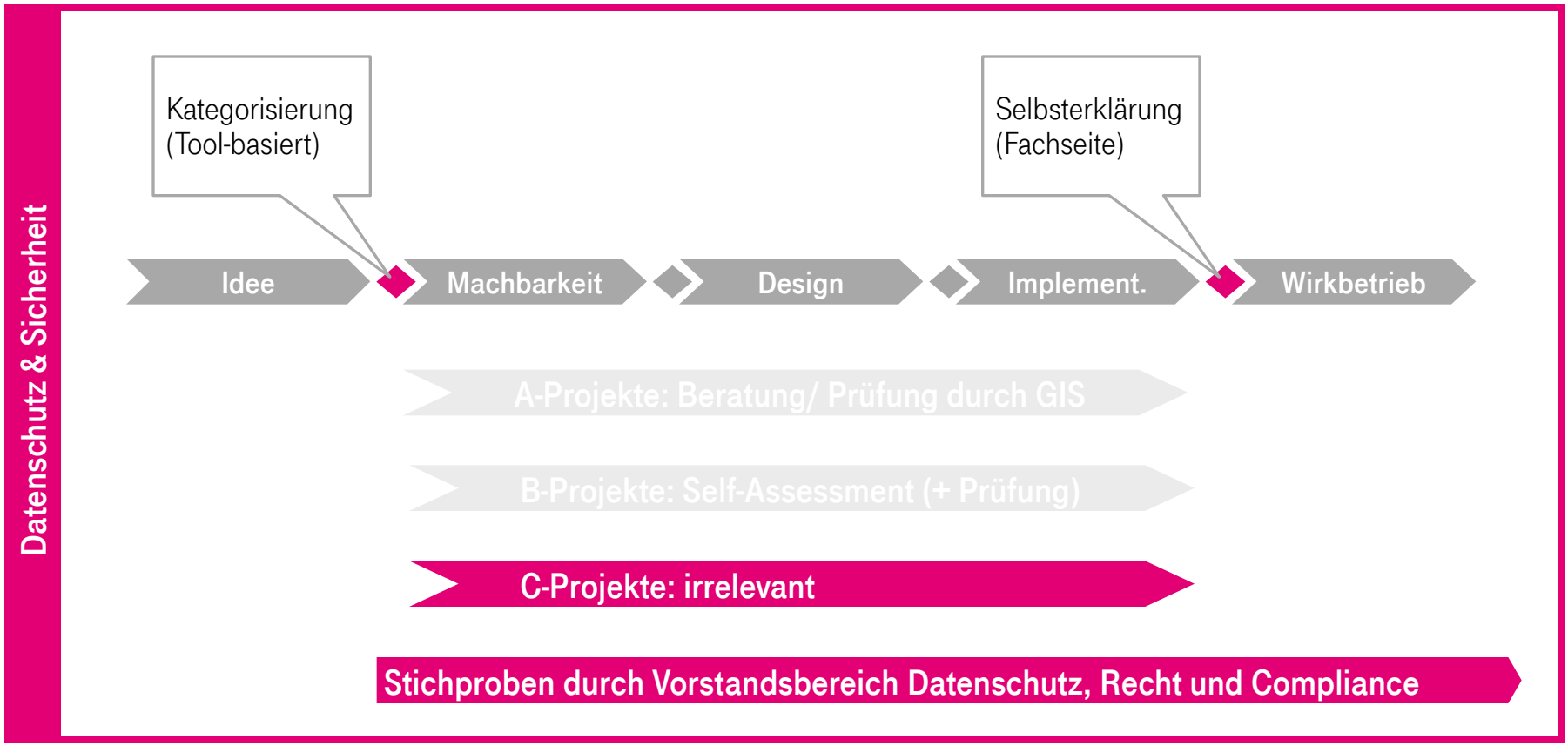
Systembeschreibung

System-verantwortlicher

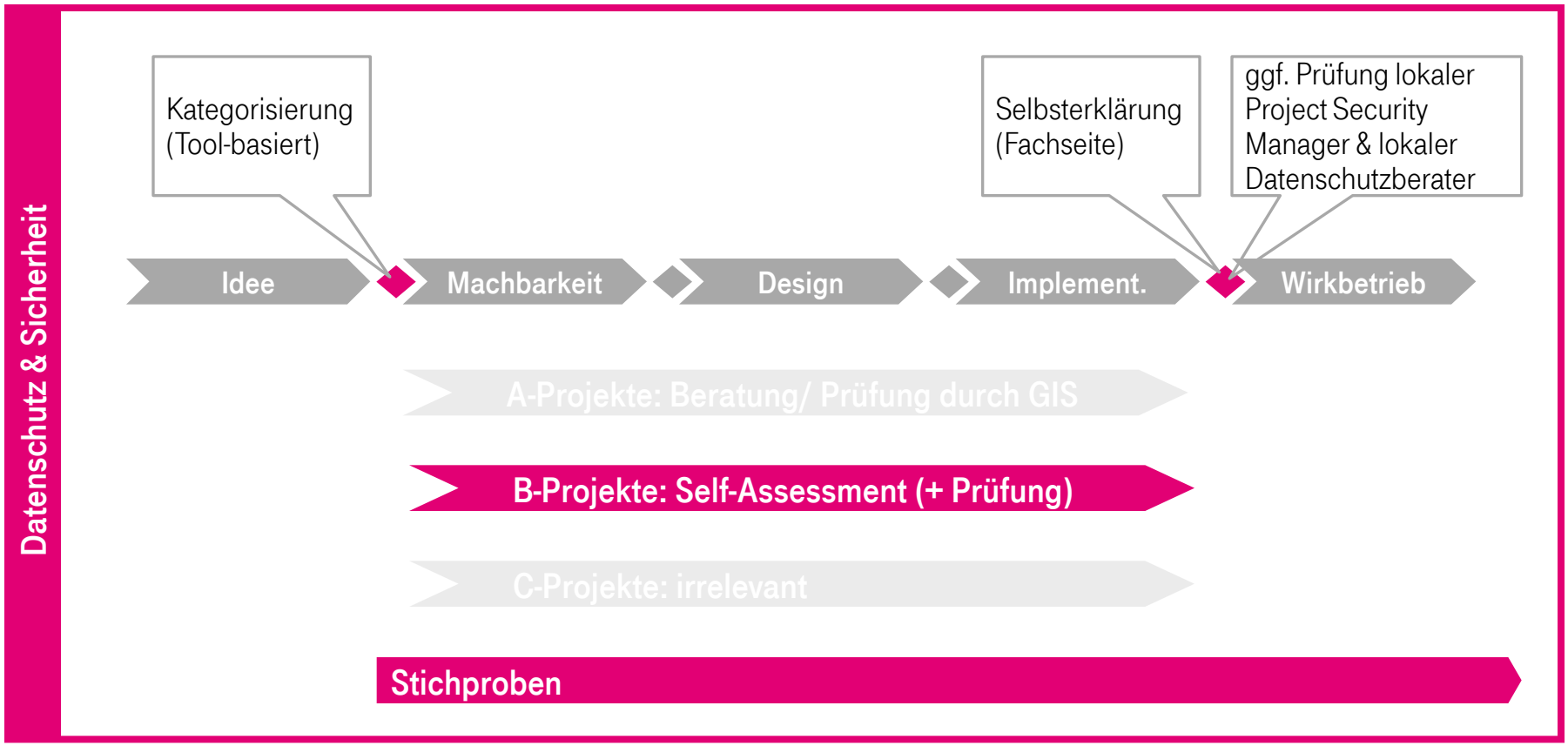
PRIVACY & SECURITY ASSESSMENT (PSA)
DIE PSA-KATEGORIE



PRIVACY & SECURITY ASSESSMENT (PSA)
PSA-KATEGORIE - C



PRIVACY & SECURITY ASSESSMENT (PSA)
PSA-KATEGORIE - B



PRIVACY & SECURITY ASSESSMENT (PSA)
PSA-KATEGORIE - A

Security

Idee → Machbarkeit → Design → Implement. → Wirkbetrieb

Kategorisierung (Tool-basiert)

A-Projekte: Beratung/ Prüfung durch GIS

B-Projekte: Self-Assessment (+ Prüfung)

C-Projekte: irrelevant

Freigabe GIS

Selbsterklärung (Fachseite)

Datenschutz

Idee → Machbarkeit → Design → Implement. → Wirkbetrieb

Adobe Acrobat-Dokumen

A-Projekte: Beratung/ Prüfung durch GPR

B-Projekte: Self-Assessment (+Prüfung)

C-Projekte: irrelevant

Umsetzungsbestätigung Fachseite **+ Abnahme GPR**

Selbsterklärung (Fachseite)

Persönliche Erstberatung, Verifizierung und Bestätigung der Kategorisierung

Rahmenfreigabe GPR auf Basis Prüfprotokoll aus Erstberatung

Realitätschecks mittels optionaler **Fokus Audits** *)

*) Nach Entscheidung des DSB kann das Fokusaudit entweder vor oder nach Gate 3 erfolgen.

GPR – Group Privacy; GIS – Group IT Security

PRIVACY & SECURITY ASSESSMENT (PSA) GRUNDLAGEN - ZUSAMMENFASSUNG

Datenschutz & Sicherheit werden in einem Verfahren gebündelt – das spart Ressourcen.

Entwicklungsbegleitendes Arbeiten spart weitere Ressourcen im Rahmen des PSA-Verfahrens.

Die Anforderungen von Datenschutz & Sicherheit sind harmonisiert, aufeinander abgestimmt, standardisiert und fixiert. Somit sind sie nachvollziehbar und bilden eine verlässliche Basis.

Aus der Kategorisierung ergeben sich die Zuständigkeiten, Aufgaben und Ergebnisse.

Zwei Formulare bestimmen und begleiten den Prozess vom Start an:
PSA-Freigabedokument für Projekte, SDSK für Systeme.

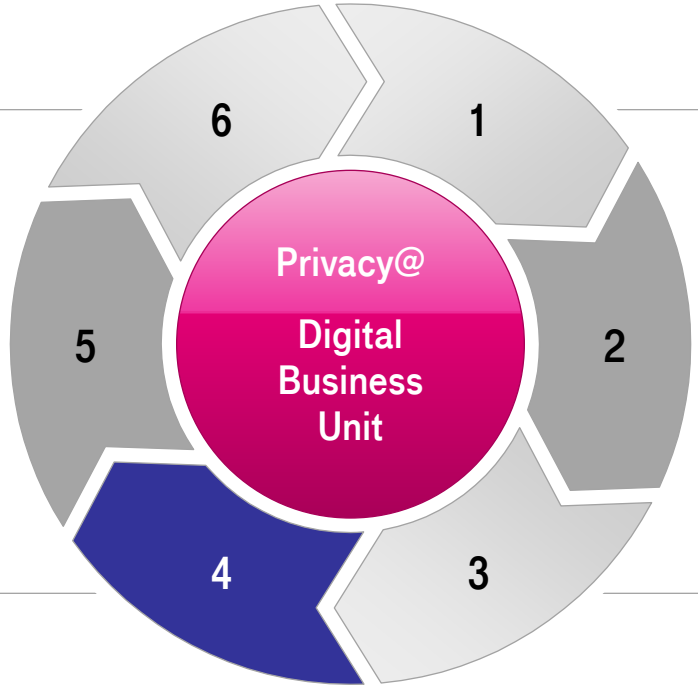
Projekte und Systeme werden unterschiedlich betrachtet.

ERGEBNISSE AUS PSA-VERFAHREN
CLOUD LÖSUNGEN BEI DEUTSCHE TELEKOM

Freigabe / Statement Of Compliance

Technische und organisatorische Vorgaben implementiert

Rechtsgrundlage vorhanden; Vertragskonstrukt vollständig datenschutzkonform

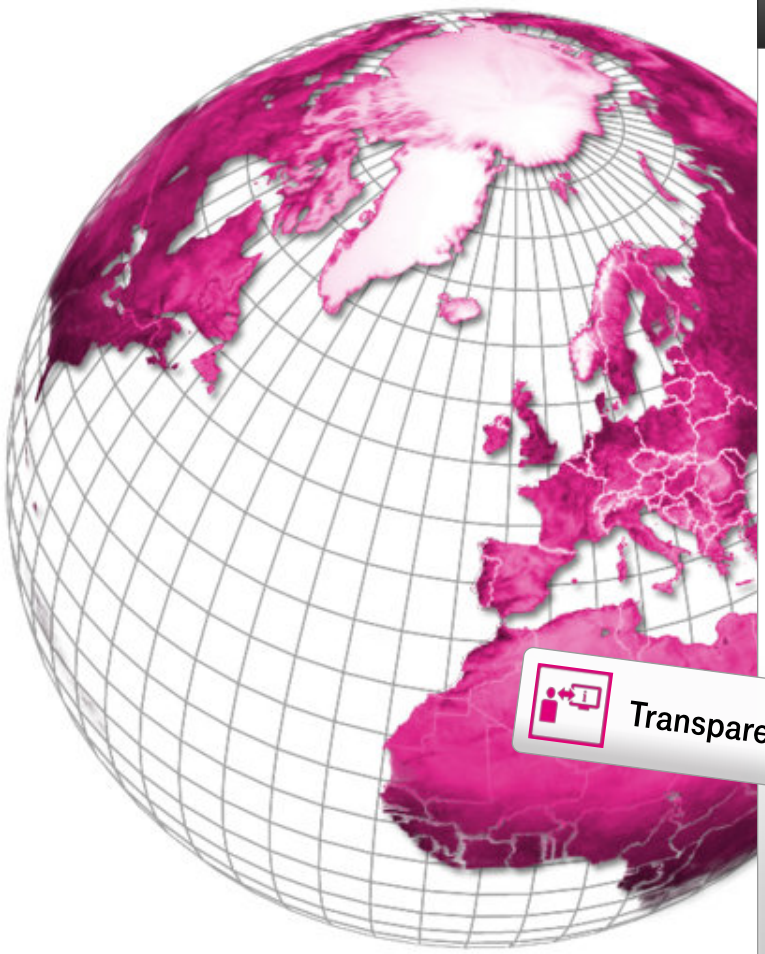


Geschäftsmodell durch Group Privacy geprüft

Projekt ist kategorisiert

Projekt ist angemessen dokumentiert

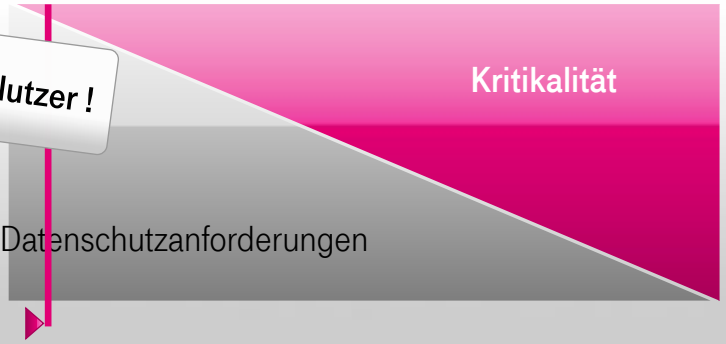
KATEGORISIERUNG VON ANBIETERN IM BUSINESS MARKET PLACE



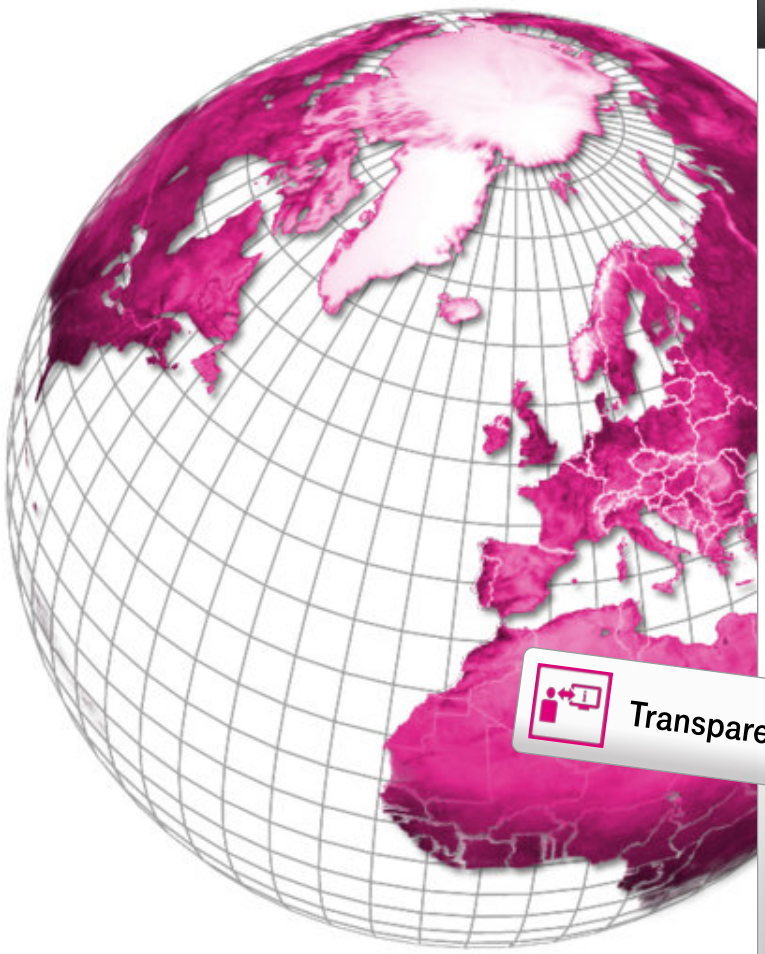
„Stufe 1“ Konzernstandard bei Vertragsgestaltung mit internationalen Partnern bei BMP

Partner setzt die Konzernvorgaben ohne wesentliche Einschränkungen um: „High-Level“:

Transparenz für Nutzer !



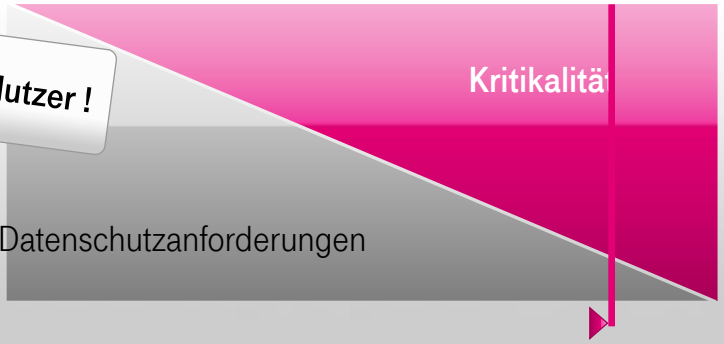
KATEGORISIERUNG VON ANBIETERN IM BUSINESS MARKET PLACE



„Stufe 4“ausschließlich zu Bedingungen des Partners (Not! Validated)

Partner setzt die Konzernvorgaben nicht um oder eine Validierung kann nicht erfolgen.

Transparenz für Nutzer !



KATEGORISIERUNG - PRIVACY DASHBOARD
TRANSPARENZ FÜR DIE NUTZER

Grundsätze

- Standardisierte Beschreibung der angebotenen Cloud Services
- Alle Services werden in gleicher Struktur beschrieben
- Beschreibung der datenschutzrechtlich relevanten Aspekte
- Beschreibungen sind kurz und prägnant gehalten
- Grundlage zur Beurteilung der einzelnen Cloud Services durch den Kunden
- Leicht auffindbar

Details

- Vertragliche Fragen
  - Genutzte Vertragsstandards, Unternehmen; Kontrollrechte
- Organisatorische Fragen
  - Beschreibung der Produktion Zugriffsberechtigungen auf D Penetrationstests; externe Te
- Technische Fragen
  - Beschreibung der Datenflüss Löschverfahren; Sicherung d Übertragungsweg; Speicheru

KATEGORISIERUNG - PRIVACY DASHBOARD

TRANSPARENZ FÜR DEN NUTZER

1.STARTSEITE BMP

- Information auf der Startseite des Businessmarketplace pro gezeigter App
- Icon Land (Ort des Datenhosting) und Icon Schloss (Infos zu Applikationsbetrieb)
- Info in Icons und Mousover

2. PRODUKT-/ MICROSITE

- Information auf der Produktseite oder Microsites
- Icon Land (Ort des Datenhosting) und Icon Schloss (Infos zu Applikationsbetrieb)
- Info in Icons und 2-3 Sätzen pro Produkt

3. INFOPORTAL BMP

- Information auf Infoportal des Business Marketplace oder Microsites
- Detaillierte Infos zu Hosting-Standort (Wo liegen meine Daten?) , Applikationsbetrieb (Wer hat Zugriff darauf?) , Vertrags-Standards (Welche Verträge liegen zu Grunde?) Kontrollrechte (Wie kann ich als Kunde Kontrolle ausüben?) Rechnung getragen werden

Icons und Mouseover (2 Merkmale)

Icons und Text (2 Merkmale)

Icons und Text (4 Merkmale)

KATEGORISIERUNG - PRIVACY DASHBOARD

ÜBERBLICK ICONS/BEDEUTUNG

Hosting-Standort: Wo Ihre Daten gespeichert werden.

Datenspeicherung in Deutschland

Datenspeicherung in der EU

Datenspeicherung in der Schweiz

Datenspeicherung außerhalb EU & Schweiz

KATEGORISIERUNG - PRIVACY DASHBOARD
ÜBERBLICK ICONS/BEDEUTUNG

Applikationsbetrieb: Wer den Service betreibt und damit Zugriff auf Ihre Daten hat.

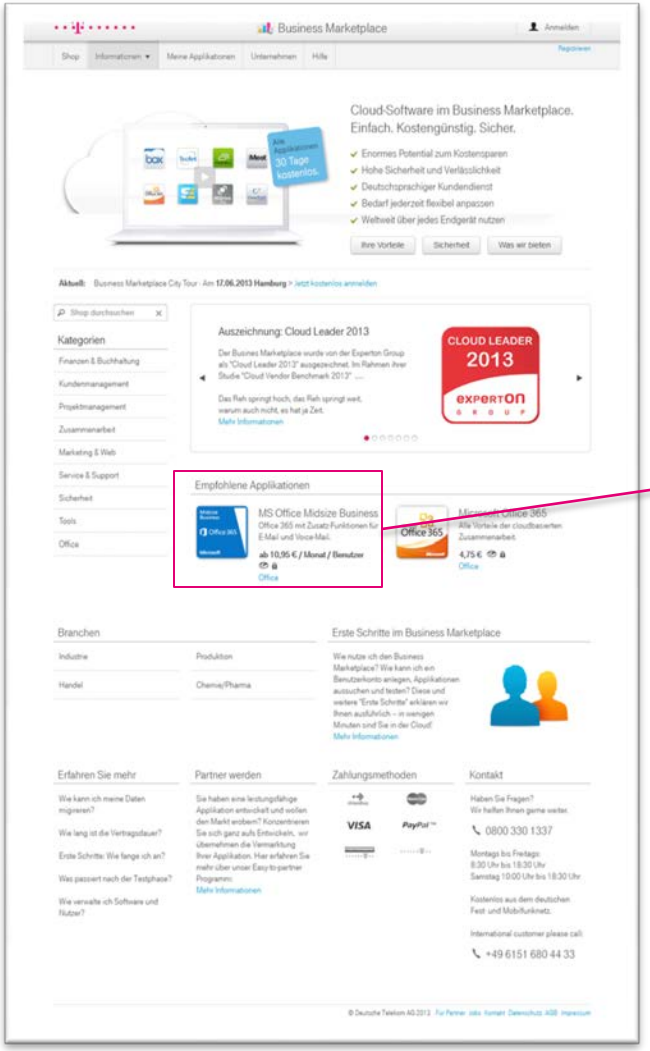
Der Betrieb erfolgt durch die Deutsche Telekom. Es kommen die hohen Sicherheitsstandards der Deutschen Telekom zur Anwendung.

Der Betrieb erfolgt auf der IT-Infrastruktur der Deutschen Telekom durch den Partner. Es kommen die hohen Sicherheitsstandards der Deutschen Telekom zur Anwendung.

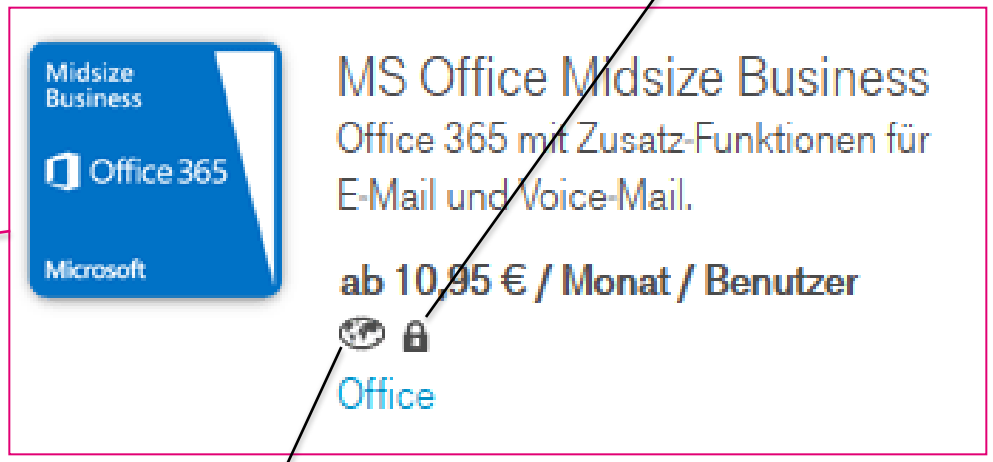
Der Betrieb der „Applikation“ und der IT-Infrastruktur erfolgt durch den Partner. Es erfolgt eine regelmäßige Überprüfung der Sicherheitsstandards durch die Deutsche Telekom.

KATEGORISIERUNG - PRIVACY DASHBOARD

STARTSEITE BUSINESS MARKETPLACE



Office 365 wird durch unseren Partner betrieben.



Datenspeicherung außerhalb EU & Schweiz

DISKUSSION.