Datenschutz im Unternehmen unter Berücksichtigung aktueller gerichtlicher Entscheidungen und gesellschaftlicher Entwicklungen

Dr. Claus-Dieter Ulmer
Senior Vice President, Konzernbeauftragter für den Datenschutz der Deutschen Telekom Gruppe
Saarbrücken, 13. Februar 2024

Datenschutz im Unternehmen

Datenschutz im Unternehmen: Wesentliche Elemente

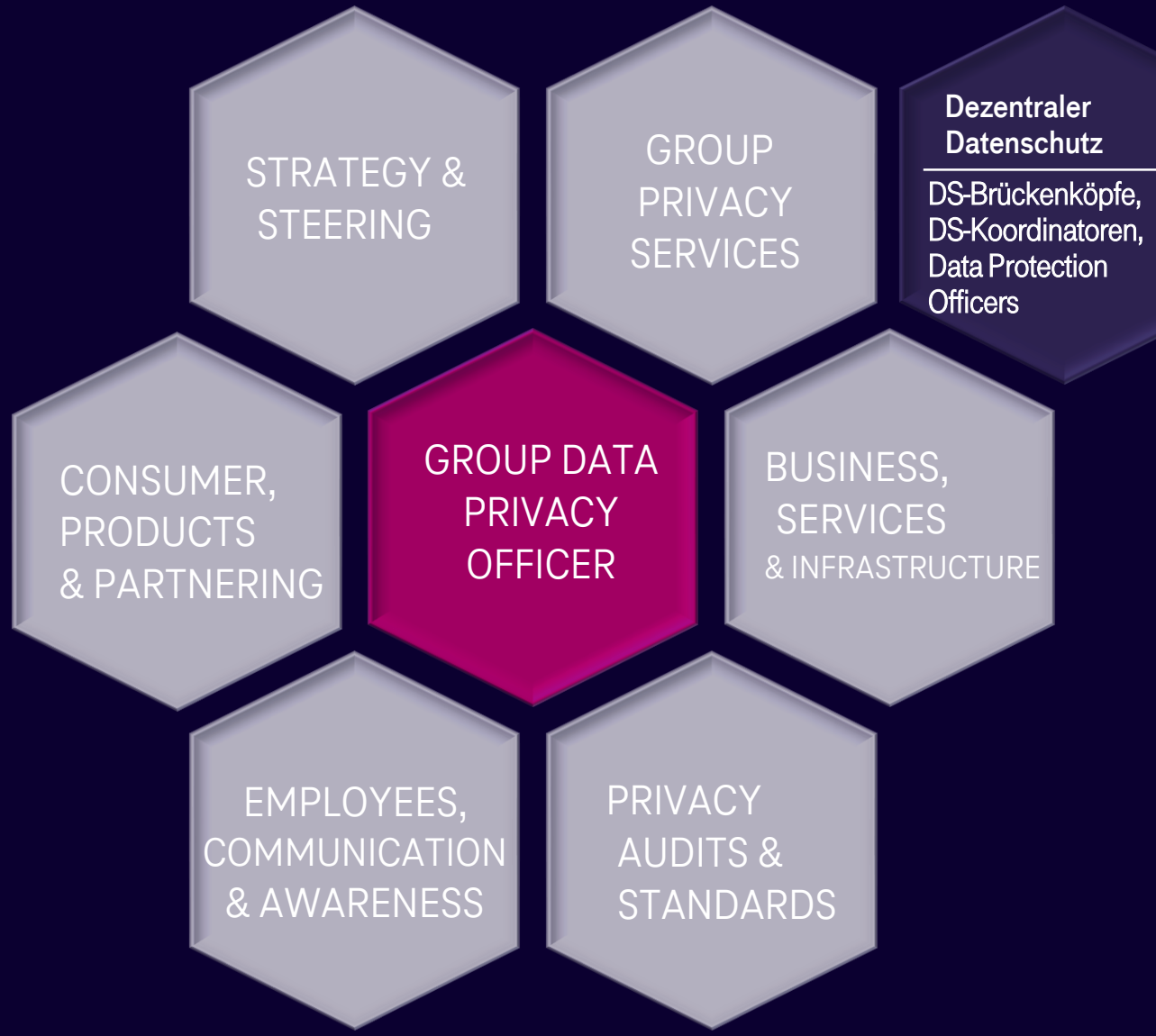
- Organisation, Verantwortlichkeiten
- Strategie – Mission
- Richtlinien, Anforderungen, Prozesse
- Beratung
- Kontrollen
- Awareness & Schulungen
- …

Organisation bei der Deutschen Telekom

Group Privacy – Mitarbeitende: 45

Nationale Datenschutzkoordinatoren: 113

International Data Protection Officers (DPOs, DPMs): 72



Verantwortlichkeiten im Datenschutz

Datenschutzbeauftragte(r)

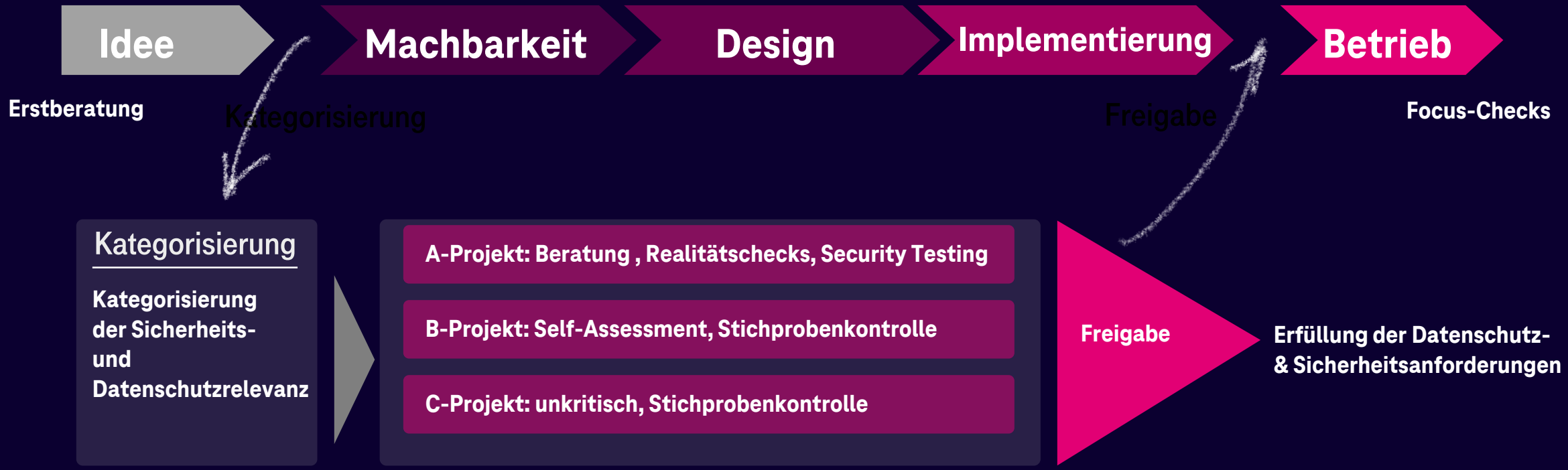
- Beratungs- und Kontrollfunktion
- Risikobewertung aus Datenschutz-Sicht
- Regelungen zur Erfüllung der Aufgaben der/des DSB
- Struktur der Datenschutzorganisation (z.B. DSB´s in Tochtergesellschaften, DS-Koordinatoren)
- Regelungen zur Compliance konformen Verarbeitung von Daten

Verantwortliche Stelle

- Compliance-Verantwortung – Risiko-Akzeptanz
- Daten-Verantwortung (Governance)
- Funktionen, die die Umsetzung der gesetzlichen Vorgaben sicherstellen
- Funktionen, die mit dem DSB als Beratungsinstanz zusammenarbeiten
- Einbindung des DSB

Zentrale Prozesse:

Datenschutzfolgenabschätzung / Privacy-Security-Assessment (PSA)



Ziele

- Integration von Sicherheit und Datenschutz in Produkt- und Systementwicklung
- Projektkategorisierung: Fokussierung wertvoller Ressourcen auf die größten Risiken
- Privacy/Security by Design – bedarfsgerechte Beratung prozessbegleitend
- Standardisierte Anforderungskataloge stellen komplexe Sachverhalte bedarfsgerecht der Fachseite zur Verfügung

Zentrale Prozesse: Datenschutzkontrollen

Risikobasierte Auditplanung

jährlich → risikobasiert → systematisch & formalisiert

Informationserhebung und Erstbewertung (Jan.-Sept.)

Sortierung und Validierung (Sept.)

Beschluss und Kommunikation (Dez.-Jan.)

Einholung zusätzlicher Expertise (Okt.-Nov.)

Zentralle Prozesse: Incidentmanagement

Vorfallprüfung → Verletzung des Schutzes personenbezogener Daten?

Risikoprüfung → Risikoeintritt für die Rechte und Freiheiten natürlicher Personen?

Fristgerechte Meldung → Meldung innerhalb von **72 h** an die zuständige Aufsichtsbehörde mit dem Sachverhalt (soweit schon aufgeklärt, ggf. nachreichen), Information des Betroffenen

Dokumentation → Dokumentation des Vorgangs (auch wenn die Vorfallprüfung eine Nichtmeldung ergibt), so dass die Einhaltung des Art. 33 überprüft werden kann.

Zentralle Prozesse: Incidentmanagement
Meldeprozess

Datenschutzverstoß

erkannt durch

Operative Datenschutzbrückenköpfe

Datenschutzkoordinatoren

Mitarbeitende

Sonstige (KLZ, Cert)

meldet an

GROUP DATA PRIVACY OFFICER

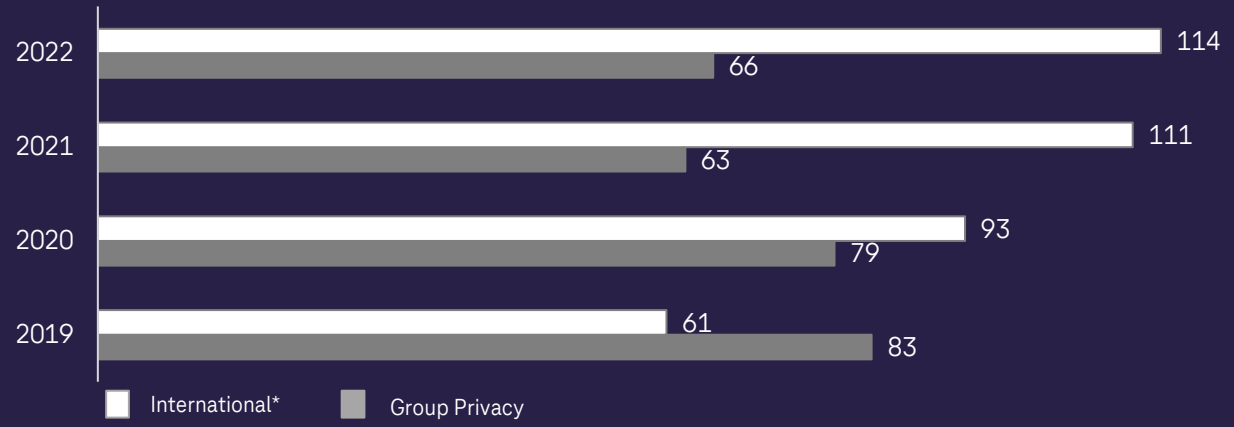
datenschutz@telekom.de

Datenschutz im Unternehmen: Zahlen, Daten & Fakten

Wesentliche Kennzahlen (2/2)

Steigerung der Datenschutzkontrollen in 2022

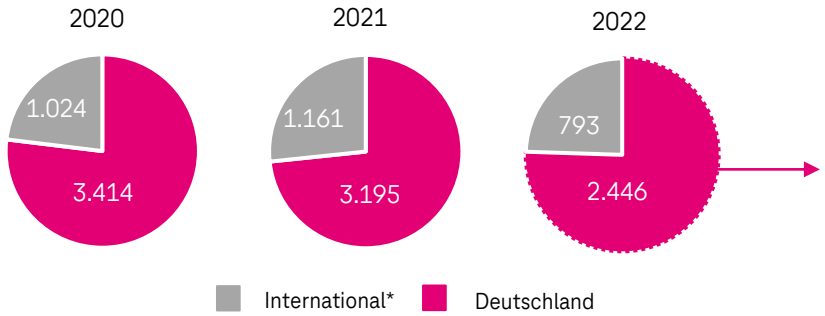
Datenschutz-kontrollen durchgeführt



Nutzung Privacy & Security Assessment Verfahren (PSA) leicht reduziert

Privacy & Security Assessment Verfahren

Verfahren insgesamt National & International*



von den 2.446 PSA-Verfahren in Deutschland waren 494 sog. A-Verfahren (begleitet durch Group Privacy)

32 Länder und 89 Gesellschaften

Konzerndatenschutzaudit (KDSA) 2022

ÜBERDURCHSCHNITTLICHES GESAMTERGEBNIS

- **alle zwei Jahre**
- **wichtiger Indikator des allgemeinen Datenschutzniveaus im Konzern**
- Dabei werden die Wahrnehmung des Datenschutzes, die Aufklärung über den Datenschutz und das Handeln nach Datenschutzgrundsätzen gemessen.

21.308

Einladungen weltweit

76 %

Teilnahmequote

Awardwert Konzern*

88%

(+ 2 % Punkte zu 2020)

Awardwert: Der Awardwert ist das Gesamtergebnis aus unterschiedlich gewichteten Einzelergebnissen des KDSA

- Überdurchschnittliches Ergebnis (Wert ≥ 80)
- Durchschnittliches Ergebnis (Wert ≥ 60)
- Unterdurchschnittliches Ergebnis (Wert < 60)

Datenschutz im Unternehmen: Blick auf aktuelle Gesetzesentwicklungen

EXKURS: E-PRIVACY VERORDNUNG – POSITIONEN UNTERNEHMEN

WEITERVERARBEITUNG VON METADATEN – WIE IN DER DSGVO

Regelungsanpassung zur Weiterverarbeitung von Kommunikationsmetadaten an die Regeln der DSGVO, damit die Weiterverarbeitung von Metadaten auch ohne Einwilligung möglich ist, wenn u.a. pseudonyme Daten genutzt werden.

GLEICHE REGELUNGEN FÜR DIE GLEICHE ART VON DATEN

für Daten mit

Gleiche Regel für Daten mit vergleichbarer Kritikalität: Präzise Standortdaten, die via GPS von Apps genutzt werden, sind weniger strikt reguliert als die nicht so präzisen Standortdaten, die Mobilfunkbetreiber von ihren Funkmasten bekommen.

ANGEMESSENE UMSETZUNGSFRIST

Implementierungsfrist für die Umsetzung in den Unternehmen.

Telekommunikation- Telemedien-Datenschutz-Gesetz (TTDSG)

Mit dem TTDSG sollen die notwendigen Anpassungen in der nationalen Gesetzgebung zum Datenschutz in der digitalen Kommunikation an die DSGVO vorgenommen werden:

- Umsetzung der EuGH und BGH-Rechtsprechung zu „Planet 49“ – strengere Auslegung des TMG
- Zusammenführung der bislang künstlich getrennten Datenschutz-Regelungen zur Telekommunikation und den Telemedien
- Keine Regelungen zu „Bestandsdaten“-Datenschutz i.S. der früheren TKG-Regelungen mehr. Diese unterfallen der DSGVO (wie auch im übrigen nationalen Recht der EU)
- Reduktion auf das Notwendige – allgemeine Regelungen der DSGVO gestärkt
- Keine gesonderten Regelungen zu Informationsrechten
- Keine gesonderten Regelungen zu Anforderungen an die Einwilligung
- Dienste zur Verwaltung persönlicher Informationen sollen zugelassen sein (PIMS - Privacy Information Management System)

Orientierungshilfen der Datenschutzkonferenz

Telekommunikation- Telemedien-Datenschutz-Gesetz (TTDSG)

§ 25 TTDSG – Schutz der Privatsphäre bei Endeinrichtungen

- Speicherung von und Zugriff auf Daten in der Endeinrichtung nur, wenn Nutzer informiert ist und eingewilligt hat (Abs. 1)
- Keine Einwilligung erforderlich, wenn
  - zur Durchführung einer Nachrichtenübertragung über das öffentliche TK-Netz
  - unbedingt erforderlich für die Durchführung eines vom Nutzer gewünschten Telemediendienstes

§ 26 TTDSG – Anerkannte Dienste zur Einwilligungsverwaltung, Endnutzereinstellungen

- Enge Voraussetzungen, insbesondere strenge Zweckbindung und kein wirtschaftliches Eigeninteresse

TTDSG und Cookies

Gestaltung von Cookie-Bannern:

Solange die abstrakten gesetzlichen Anforderungen (§ 25 TTDSG) eingehalten sind, bleibt es dem Verwender überlassen, wie er die Cookie-Banner konkret gestaltet.

Transparenz + **Nachvollziehbarkeit** + **Zweckbeschränkung** + ...

"Transparency & Consent Framework„ (TCF) Version 2.2 des „Interactive Advertising Bureau“ (IAB)

News & E-Mail bei t-online.de

t-online.de

Aktuelle Nachrichte... | Nachrichten, aktuell... | News & E-Mail bei t... | Aktuelle Nachrichte... | ZEIT ONLINE | Nach... | DER SPIEGEL | Onlin... | heise online - IT-Ne... | Golem.de: IT-News f... | netzpolitik.org | POLITICO – Europea... | Willis Towers Watson | Alle Lesezeichen

Wetter DAX +0,14% Telefonverzeichnisse Lotto Telekom Services PUR-Abo Login

t-online.
Nachrichten für Deutschland

Politik Ukraine Regional

• Live | Newsblog zu der

Mehrere V
Blockade

dem, was wir wollen"

t-online.

Direkt zum E-Mail-Center

Wie wollen Sie t-online nutzen?

Kostenfrei mit Werbung

Nutzen Sie t-online wie gewohnt mit der üblichen Werbung und Tracking. Details finden Sie in den **Datenschutzhinweisen** und dem **Datenschutz-Manager**.

ZUSTIMMEN

Mit Ihrem Klick erteilen Sie eine Einwilligung gemäß § 25 Abs. 1 TTDSG i.V.m. Art. 6 Abs. 1 lit. a) DSGVO, die Sie in unserem Datenschutz-Manager jederzeit **individuell anpassen** können.

...oder mit t-online PUR-Abo

Nutzen Sie t-online nahezu werbefrei und ohne Werbetracking für 2,99€/ Monat, monatlich kündbar. Details finden Sie in den **Datenschutzhinweisen (PUR)**.

JETZT SICHERN

Bereits PUR-Abonnent? **Hier einloggen**
Mehr Informationen zum PUR-Abo auf t-online finden Sie in den **häufig gestellten Fragen (FAQs)**.

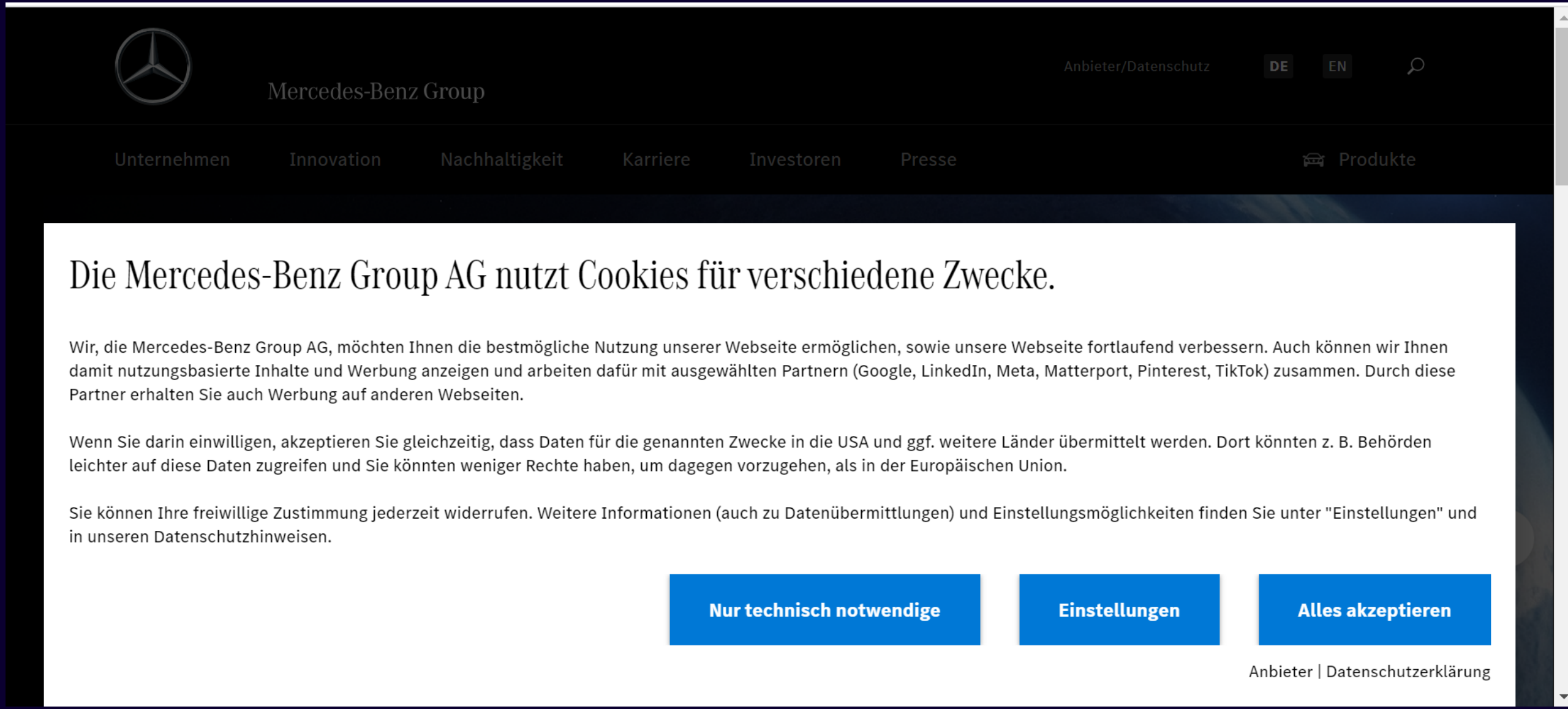
Für die Nutzung mit Werbung:

Wir und unsere 200 Partner erheben und verarbeiten personenbezogene Daten (wie z.B. IP-Adressen, Cookies oder Geräte-Kennungen), um unser Webangebot zu verbessern und zu finanzieren. Die Verarbeitung kann auch außerhalb der EU/EWR erfolgen, wo unter Umständen kein vergleichbares Datenschutzniveau herrscht, z.B. in den USA. Weitere Informationen zu den Orten der Verarbeitung finden Sie hier. Die Verarbeitung erfolgt dabei zu den folgenden Zwecken:

- **Personalisierte Anzeigen & Inhalte, Werbetracking und Zugriff auf Ihr Endgerät**
- **Einbindung externer Inhalte**
- **Push-Benachrichtigungen / Kommunikation**

Im **Datenschutz-Manager** finden Sie eine detaillierte Übersicht, welche Partner zu welchen Zwecken Daten verarbeiten, insbesondere auch, welche **Partner** Nutzerprofile auf Basis der erhobenen Daten erstellen. Für die Verarbeitung Ihrer Daten benötigen wir dabei Ihre Einwilligung.

Impressum Datenschutzhinweise Datenschutzhinweise (PUR) Nutzungsbedingungen


Mercedes-Benz Group
Anbieter/Datenschutz
DE
EN
Unternehmen
Innovation
Nachhaltigkeit
Karriere
Investoren
Presse
Produkte
Die Mercedes-Benz Group AG nutzt Cookies für verschiedene Zwecke.
Wir, die Mercedes-Benz Group AG, möchten Ihnen die bestmögliche Nutzung unserer Webseite ermöglichen, sowie unsere Webseite fortlaufend verbessern. Auch können wir Ihnen damit nutzungsbasierte Inhalte und Werbung anzeigen und arbeiten dafür mit ausgewählten Partnern (Google, LinkedIn, Meta, Matterport, Pinterest, TikTok) zusammen. Durch diese Partner erhalten Sie auch Werbung auf anderen Webseiten.
Wenn Sie darin einwilligen, akzeptieren Sie gleichzeitig, dass Daten für die genannten Zwecke in die USA und ggf. weitere Länder übermittelt werden. Dort könnten z. B. Behörden leichter auf diese Daten zugreifen und Sie könnten weniger Rechte haben, um dagegen vorzugehen, als in der Europäischen Union.
Sie können Ihre freiwillige Zustimmung jederzeit widerrufen. Weitere Informationen (auch zu Datenübermittlungen) und Einstellungsmöglichkeiten finden Sie unter "Einstellungen" und in unseren Datenschutzhinweisen.
Nur technisch notwendige
Einstellungen
Alles akzeptieren
Anbieter | Datenschutzerklärung

TTDSG und „E-Mail Ansprache“?
Keine Regelung im TTDSG – Beurteilung nach DSGVO

Die E-Mail Adresse als solche ist ein Bestandsdatum und deshalb nicht vom TTDSG umfasst. Nur im Kontext eines direkten Austausches wird sie für eine Einzelkommunikation Teil der Nutzungsdaten.
Die E-Mail Adresse kann zur Kontaktaufnahme nach Auffassung der Aufsichtsbehörden unter Auslegung des Art. 6 Abs. 1 f) DSGVO wie folgt verwendet werden:

- Es besteht bereits ein Kontakt zwischen einem Nutzer und einem Unternehmen, z.B. durch eine Bestellung
- Das Unternehmen hat im Rahmen dieses Kontakts zulässiger Weise von der E-Mail Adresse Kenntnis erlangt
- Rechtsgrundlage zur Ansprache zu Marketingzwecken: berechtigtes Interesse gemäß Art. 6 Abs. 1 f) DSGVO (Erwägungsgrund 47 zur DSGVO und § 7 Abs. 3 UWG)
- Widerspruchsmöglichkeit bei Erhebung und jedem Versand

Datenschutz im Unternehmen Urteile und gesellschaftliche Entwicklungen

„Schrems II“ - Transfer-Impact-Assessment

Bewertungsprozess für Datenexporte: Wesentliche Bestandteile („Transfer-Impact-Assessment“)

Abstrakte Bewertung

Länder-Rechtsgutachten zum abstrakten Datenschutzniveau in datenempfangenden Ländern (z.B. USA, Russland, China) geben Auskunft über das abstrakt bestehende Risiko einer Datenübermittlung (Initialrisiko).

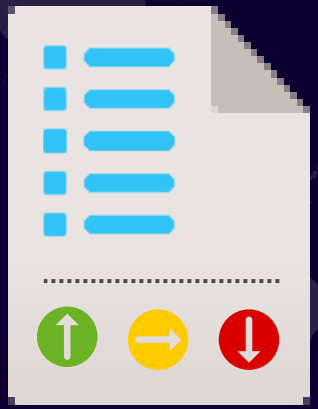
Criteria
Regulation on the processing of personal data
Regulation of public authority access to private data
Regulatory supervision
Rights of redress
International treaties
overall average
Initial Risk Assumption (IRA)

Konkrete Bewertung

Durch den Lieferantenfragebogen wird die konkrete Praxis beim Lieferanten sowie die Umsetzung von technischen und vertraglichen Maßnahmen zusätzlich überprüft und bewertet.

Abschließende Risikoeinordnung

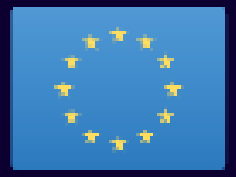
Das Ergebnis der abstrakten und konkreten Bewertung führt zu einer abschließenden Risikobewertung und der Feststellung, ob und wie ergänzende mitigierende Maßnahmen getroffen werden müssen.



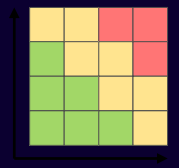
Ergebnisübernahme ins Privacy-Security Assessment (PSA)

Das Ergebnis fließt in den PSA-Prozess ein. Hier wird geprüft, ob die Datenverarbeitung insgesamt, also nicht nur die Datenexportproblematik, allen Datenschutz-Anforderungen entspricht.

„Schrems II“@Deutsche Telekom



In **20 EU-Ländern** und in mehr als **70 Unternehmen** wurden mehr als **3.000 Systeme** auf „Schrems II“ -Relevanz analysiert.



Mehr als **300 Transfer-Impact Assessments** wurden durchgeführt.

Zusätzlich wurden mehr als **20.000 Lieferanten** und ihre **Verträge** bewertet und die Verträge angepasst.

Data Privacy Framework USA/EU

- Bindende Rahmenbedingungen, um den Zugriff von U.S. Intelligence Services auf ein angemessenes Maß zu begrenzen
- Etablierung eines Data Protection Review Courts, um den EU-Bürgern den Rechtsweg gegen Überwachungsmaßnahmen zu eröffnen
- Maßnahmen zu Review und Monitoring …

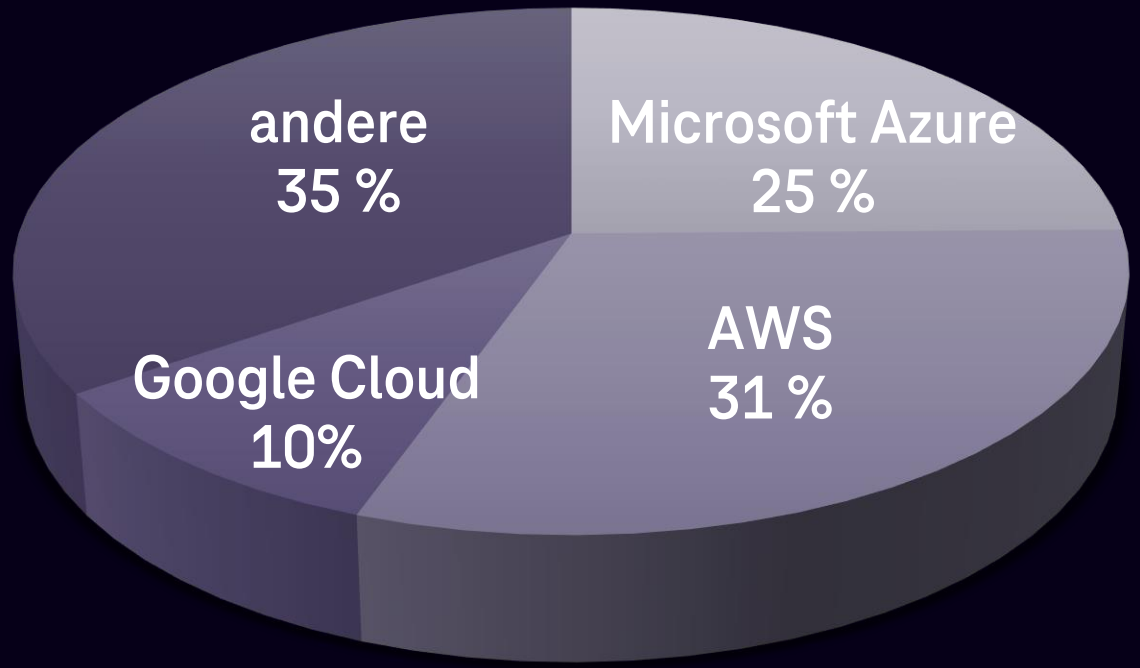
GAIA-X - the European Solution

Die Europäische Antwort auf die Globale Ressourcen-Verteilung?

Herausforderungen

- Investitionen & Vertrauen
- Europäische Steuerung
- Gleiche Chancen entwickeln
- Offenheit für alle EU Privacy Standards:
  - „Auditor“
  - CISPE*
  - EU Cloud Code of Conduct

* Cloud Infrastructure Services Providers in Europe



Quelle: Statista 2024

Künstliche Intelligenz
KI Anwendungsbereiche bei der Telekom

		USE CASES
NETZWERK / PRODUKTION		▪ Netzplanung und –Optimierung ▪ “Zero-touch operations” ▪ Predictive Maintenance
SALES		▪ Sales agent Support-Systeme ▪ Proaktive Vorhersagen/Prävention zu Kundenabwanderungen & Verpflichtung
PRODUKTE		▪ (Automatisierte) Produktempfehlungen ▪ Voice assistants / smart hubs
CUSTOMER SERVICE		▪ 24/7 Problemlösung ▪ Automatisiertes & verbessertes CRM inkl. Selbstbedienung
INTERNE PROZESSE		▪ Online marketing optimierung ▪ (Automatisierte) Finanzprognosen

Rahmenbedingungen zum Datenschutz in KI-Projekten

- **PSA-Verfahren***, insbesondere mit Definition der Zweck-bestimmung und Prüfung der rechtskonformen Nutzung aller Daten(quellen).

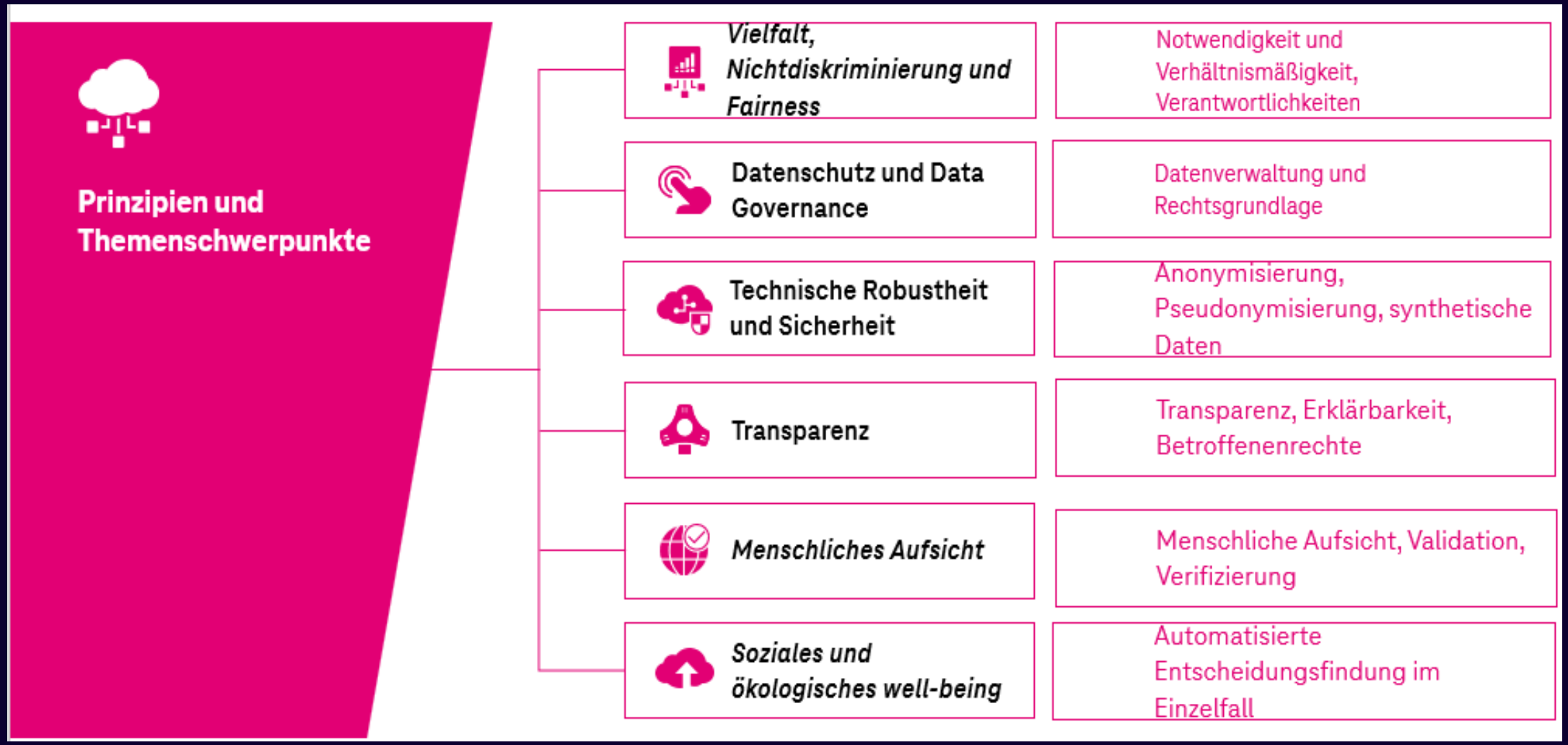
- **Kontrolle** durch Überwachung der KI-Entscheidungen u.a. auf Einhaltung der definierten Zweckbestimmung.

- **Transparenz** über Kriterien und die Gewichtung von KI-Entscheidungen.

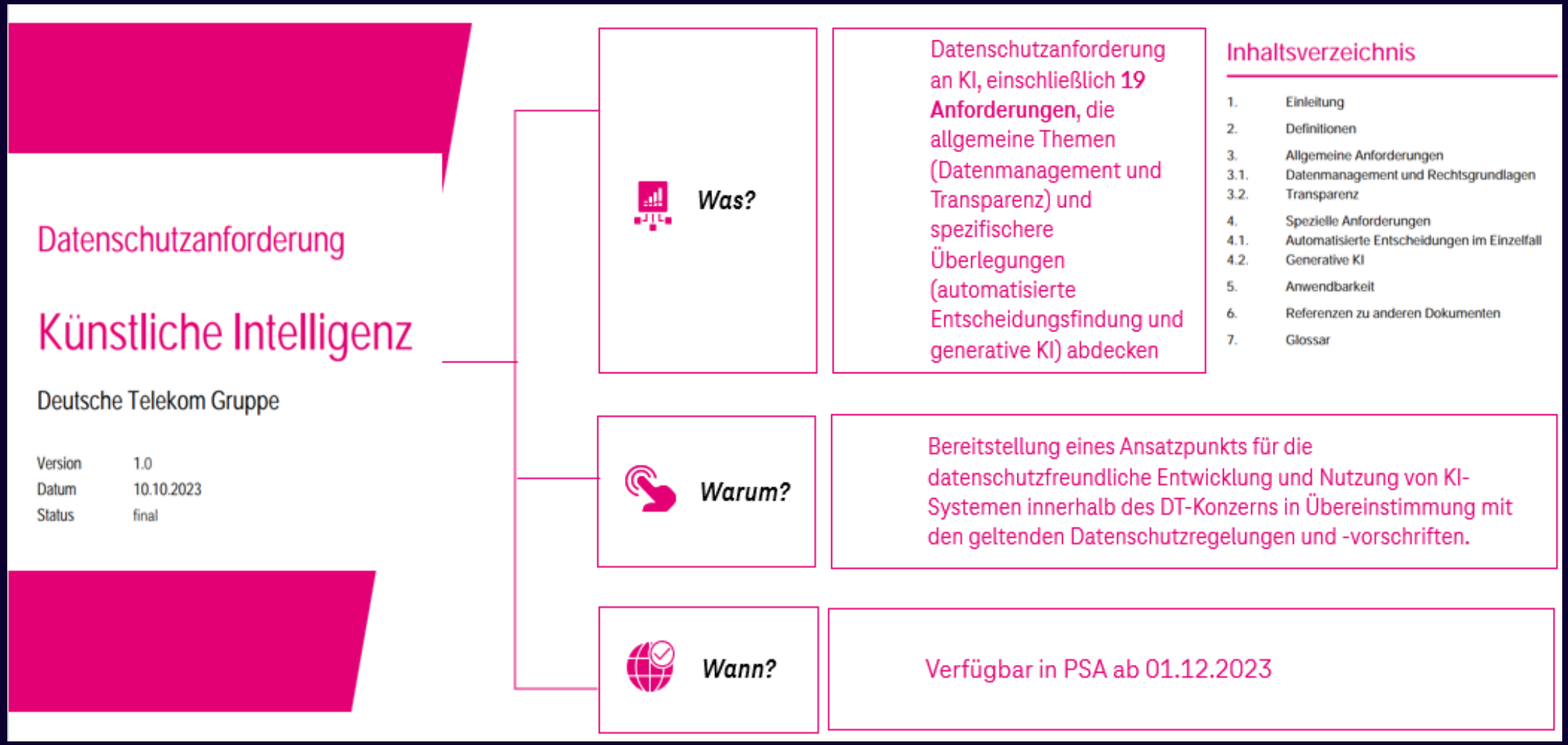
- **Information** für Kunden und Beschäftigte über Verwendung von KI-Systemen sowie Möglichkeit der Wahrnehmung von **Betroffenenrechten**

*Privacy-Security-Assessment

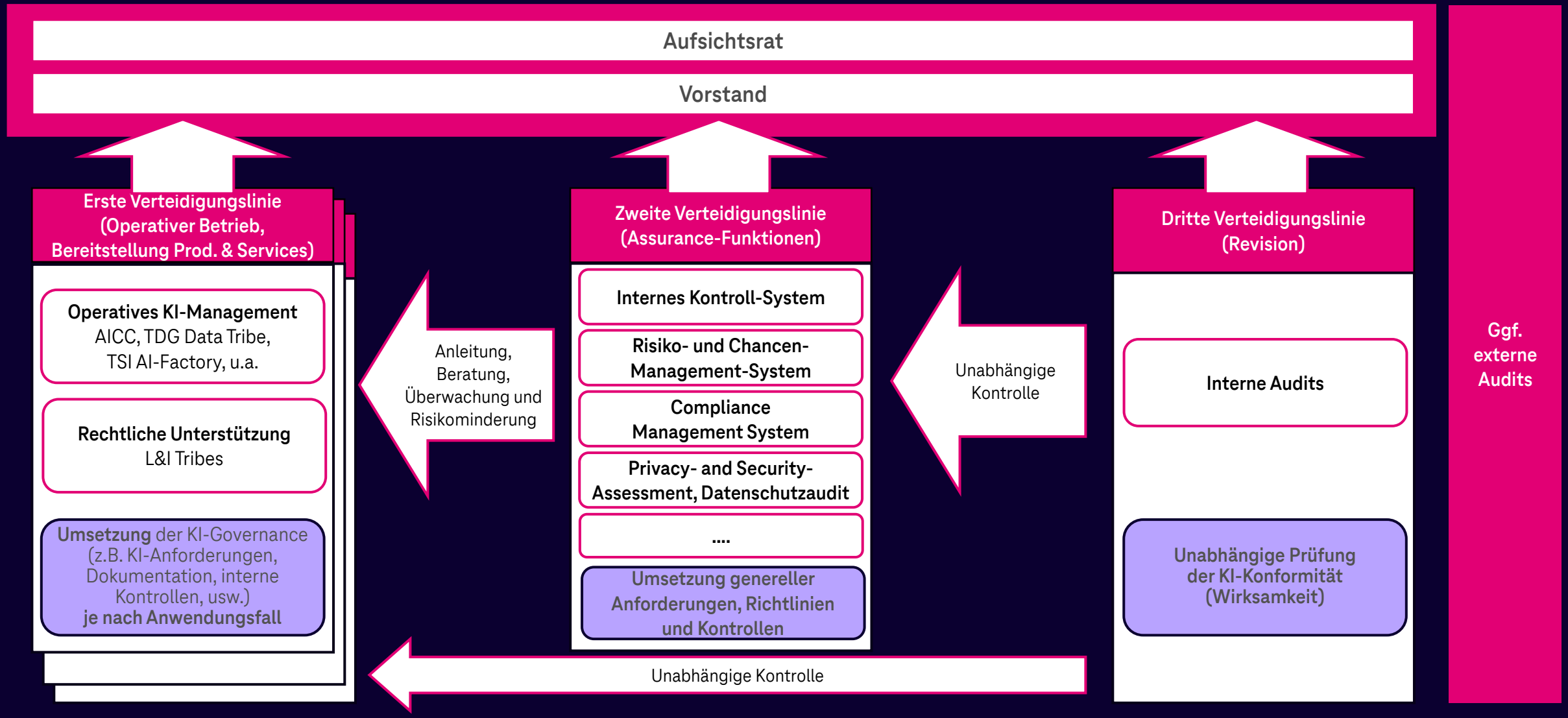
DSGVO, KI-Gesetz und Datenschutzanforderungen



Datenschutzanforderung KI in PSA



KI-Governance: Nutzung bestehender Strukturen im Konzern



AI-Recommendations der United Nations
The UN Special Rapporteur on the Right to Privacy

Im Juli 2015 hat der Menschrechtsrat der Vereinten Nationen **Prof. Joseph (Joe) Cannataci**, Professor an den Universitäten von **Malta** (Information Policy and Governance) und **Groningen** (Chair in European Information Policy and Technology Law) zum **Special Rapporteur** berufen.

Seine Aufgabe ist es:

"(*a*) To gather relevant information, including on international and national frameworks, national practices and experience, to study trends, developments and challenges in relation to the right to privacy and to make recommendations to ensure its promotion and protection, including in connection with the challenges arising from new technologies; …"

Um Entwicklungen und Trends im Unternehmensumfeld aufzunehmen und daraus mögliche Empfehlungen abzuleiten wurde die **Taskforce for the Right to Privacy in Corporations** gegründet und Mitglieder eingeladen.

Die Taskforce kümmert sich um datenschutzrechtliche Belange im Unternehmenskontext und versucht – wo möglich – einen einheitlichen Angang zu definieren.

UNITED NATIONS
HUMAN RIGHTS
OFFICE OF THE HIGH COMMISSIONER

A Special Rapporteur is an independent expert appointed by the Human Rights Council to examine and report back on a country situation or a specific human rights theme. This position is honorary and the expert is not United Nations staff nor paid for his/her work. The Special Rapporteurs are part of the Special Procedures of the Human Rights Council.

Entwurf von „AI“- Recommendations

Hintergrund:

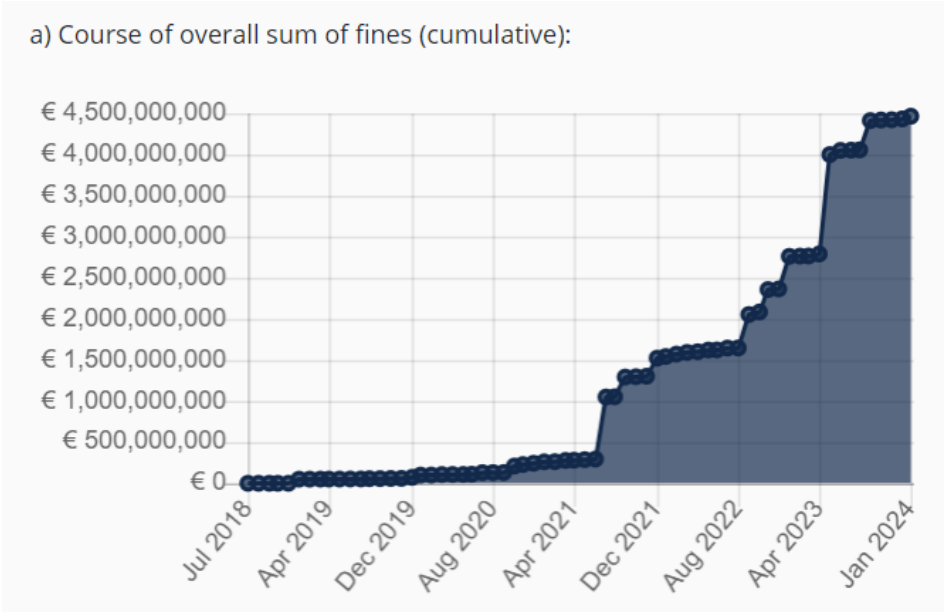
- Ausgangspunkt ist die Allgemeine Erklärung der Menschenrechte vom 10. Dezember 1948 (Resolution der Generalversammlung 217 A (III)
- Basis ist damit nicht regionales Recht
- Etablierte und bewährte Datenschutz-Grundsätze, insbesondere aus der Europäischen Union (DSGVO), sind Grundlage der Betrachtung
- Eine Arbeitsgruppe der Taskforce hat sich der Entwicklung des Entwurfs angenommen (Bestehend aus Elizabeth Coombs, UN SRP; Patrick Curry, BBFA; Jörg Thomas, Huawei; CD Ulmer, DTAG)

PDF
UN SRP Privacy

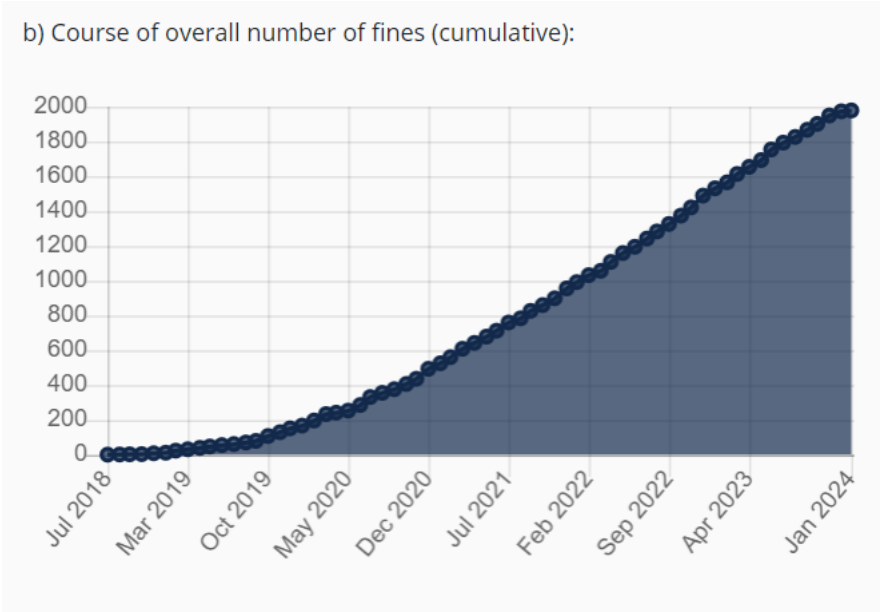
Datenschutz im Unternehmen: Neue Rechtsfolgen ...

Bußgeldentwicklung

a) Course of overall sum of fines (cumulative):



b) Course of overall number of fines (cumulative):



Quelle: enforcementtracker.com, 02/24

Beispiele:

- 10 Mio € gegen Uber Technologies Inc. Und Uber B.V. (Niederlande): 10 Mio. € wegen Verletzung von Informationspflichten und Betroffenenrechte von Fahrern
- 32 Mio. € gegen Amazon France Logistique (Frankreich) wegen Überwachung von Mitarbeitenden (Verletzung des Prinzips der Datenminimierung, der Informationspflichten, der Rechtmäßigkeit der Verarbeitung …)
- 345 Mio. € gegen Tik Tok Technology Limited (Irland) wegen Verstöße bezüglich der Verarbeitung von Daten Minderjähriger

Leitlinie des Europäischen Datenschutz-Ausschusses zur Berechnung von Bußgeldern (Juni 2023)

Bei Unternehmen mit einem weltweiten Jahresumsatz von **mehr als EUR 500 Mio.** wird zunächst der Jahresumsatz des vorangegangenen Geschäftsjahres und der **gesetzliche Bußgeldrahmen für den Verstoß (2 % oder 4%*)** ermittelt.

Anschließend sind **Korridore** für die Bußgeldhöhe festgelegt, abhängig von der Schwere des Verstoßes.

leichter Verstoß	mittlerer Verstoß	schwerer Verstoß
▪ 0 bis 0,2 % ▪ 0 bis 0,4 % des Jahresumsatzes	▪ 0,2 bis 0,4 % ▪ 0,4 bis 0,8 % des Jahresumsatzes	▪ 0,4 bis 2 % ▪ 0,8 bis 4 % des Jahresumsatzes

Der so errechnete Betrag kann abhängig von den konkreten Umständen des Einzelfalls erhöht oder reduziert werden.

*Ein Bußgeld bis zu 2% des Konzern-Jahresumsatzes kann gemäß Art. 83 Abs. 4 DSGVO z.B. für Fälle von Dokumentationsfehlern oder nicht ausreichenden technischen und organisatorischen Maßnahmen verhängt werden; bis zu 4% des Konzern-Jahresumsatzes sind möglich z.B. bei rechtswidriger Datenverarbeitung, etwa ohne Einholung einer Einwilligung (Art. 83 Abs. 5 DSGVO).

Datenschutz im Unternehmen: Neue Beratungsansätze ...

Privacy by Strategy

Unsere Vision

Wir schaffen ein Klima des Vertrauens

Wir ermöglichen zukunftsweisende und datenschutzfreundliche Lösungen in der digitalen Welt

EIN Datenschutz

Einheitliche Beratung auch auf internationaler Ebene

Ein Produkt. Eine Lösung von Group Privacy und den Datenschutzbeauftragten

Unsere Kunden sind unsere Partner

WIR HANDELN UNTERNEHMERISCH IM INTERESSE UND ZUM SCHUTZ DER DTAG

Unsere Veränderung

Datenschutz – 8 Steps up

Wir fördern Entscheidungsprozesse und eine proaktive Beratungsmentalität

Unser Wachstum

Ausgezeichnete 8-Sterne-Beratung

Wir pflegen ein risiko-orientiertes und strategisches Denken.
Unsere Leitlinien sind pragmatisch, transparent und verbindlich

Wir fördern Entscheidungsprozesse und eine **proaktive Beratungsmentalität**

Wir pflegen ein risiko-orientiertes und **strategisches Denken**

Wo stehen wir?

Die Digitalisierung nimmt Fahrt auf, und die Entwicklungszyklen – sofern überhaupt noch vorhanden – werden immer kürzer. Der Wettbewerb auf den relevanten Märkten nimmt zu.
Unternehmen müssen sich noch früher als bisher Orientierung verschaffen, wenn sie den Anschluss an die Welt von morgen und damit an ihre eigene Zukunft nicht verlieren wollen.

Die digitale Strategie eines Unternehmens muss kontinuierlich an die aktuellen Erfordernisse angepasst werden. Guter fachlicher Rat, der ein Unternehmen durch turbulente Zeiten führt, ist noch früher als bisher erforderlich. Dies gilt insbesondere für die Datenschutzberatung, da die meisten oder fast alle neuen digitalen Lösungen auf der Verarbeitung personenbezogener Daten beruhen – zumindest im Konzern Deutsche Telekom.

Daher greift der aktuelle „Privacy-by-Design“-Ansatz zu spät, um eine intelligente und ressourcen-schonende Umsetzung neuer digitaler Trends im Unternehmen zu ermöglichen. Dadurch wird „Privacy by Design“ jedoch nicht überflüssig. Privacy by Design ist der wichtigste Meilenstein vor der konkreten Gestaltung und Entwicklung einer digitalen Lösung.

Allerdings erst nachdem die Grundlagen durch den „Privacy-by-Strategy-“Ansatz gelegt wurden.

Was bedeutet „Privacy by Strategy“ konkret?

Unternehmen erhalten frühzeitig **Orientierung** über die **generelle Machbarkeit ihrer digitalen Strategie** und über die möglichen **Leitplanken** für die geplante strategische Ausrichtung.

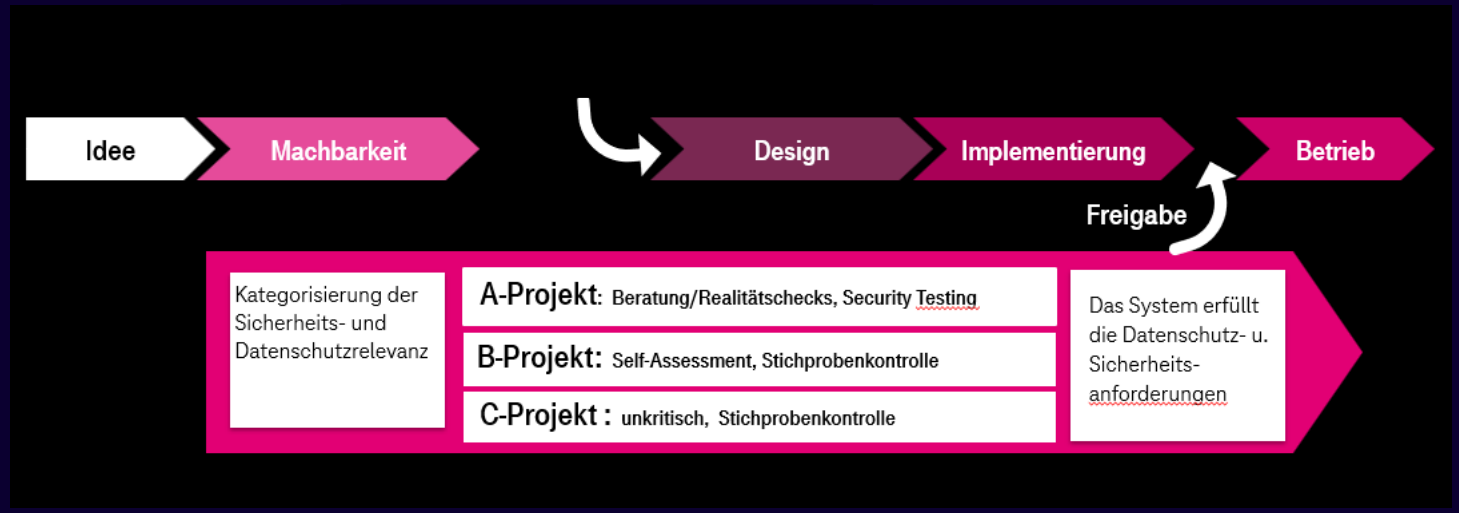
Unternehmen erhalten bereits in einem **sehr frühen Stadium** Unterstützung bei der Identifizierung strategischer Produkte, Lieferanten oder Partnerschaften.

Die **Datenschutzorganisation** kennt die aktuellen und kommenden **Trends auf dem digitalen Markt** und in den Datenschutz-Communities. Sie hält sich konti-nuierlich auf dem Laufenden, um die **Strategiekonzepte des Unternehmens** von Beginn an **begleiten** zu können.

Beratung – Privacy-Security-Assessment
Was kommt vor Privacy by Design?

1 ? ...

2 Privacy by Design



GPR-Stream: proaktive und strategische Beratung

Was ist zu tun

Information

- Regelmäßig **informieren**, was – unternehmensweit – in der Pipeline ist oder derzeit produziert wird/am Markt ist; sowohl im Hinblick auf **Innovationen** als auch auf den operativen Bereich - **Schwerpunktbereiche** -
- Informieren, worüber aktuell in den sozialen Medien und Datenschutz-Communities gesprochen wird - **Aufgreifen von „Datenschutztrends“ (Trend Radar) -**
- Erkennen von Ähnlichkeiten oder gemeinsamen Strukturen **– Aggregation -**

GPR-Stream: proaktive und strategische Beratung

Wie

Jour Fixe

- Regelmäßige **Jour Fixes** zwischen dem Datenschutzbeauftragten und **Vorstandsmitgliedern** – nicht nur Bericht der/des Datenschutzbeauftragten - , sondern Austausch über strategische Unternehmensperspektiven
- Regelmäßige Jour Fixes zwischen Group Privacy und Group Strategy Zusammenarbeit mit dem Bereich Sicherheit und anderen Stakeholdern **- Zusammenarbeit über Bereichsgrenzen hinweg -**

Datenschutzbeauftragter

- **sollte mit allen operativen Vorständen in regelmäßigem Austausch stehen.**
- Sicherstellen, dass die zukünftige Ausrichtung des Unternehmens und die konkreten Planungen aktuell sind – **Abdeckung aller Geschäftsfelder**
- Adressieren und Erörtern allgemeiner Datenschutzaspekte auf höchster Managementebene – **Tone from the top**
- Zustimmung der obersten Führungsebene als Argumentationshilfe nutzen – **hilft manchmal**

GPR-Stream: proaktive und strategische Beratung

Teilnahme an „Strategic Boards“

Gremien

Sicherstellen einer stabilen Beziehung zum Bereich Strategie und eines Sitzes in Innovation Boards und anderen Entscheidungsgremien auf operativer Ebene

- Der regelmäßige Austausch mit dem **Bereich Strategie** ist ein wesentliches Element des Privacy-by-Strategy-Ansatzes **- Blick in die Zukunft -**
- Der Bereich Strategie wäre auch der richtige Ort, um neue Ideen aus der Sicht des Datenschutzes einzubringen **- die Datenschutzorganisation als „Influencer“ -**
- Die „Product and Innovation Boards“ könnten im Rahmen ihres Austauschs über die aktuelle Planung über neue Produkte sprechen, die sich am Horizont abzeichnen **- Kommunikation ist alles ...**

GPR-Stream: proaktive und strategische Beratung

Schaffen schneller Entscheidungswege

Entscheidungswege

Wenn Diskrepanzen zwischen den Datenschutzempfehlungen und geschäftlichen „Erfordernissen“ auftreten, sollten **Entscheidungsgremien** eingerichtet sein, die gemeinsam entscheiden und Verantwortung übernehmen können.

- Da Unternehmen zunehmend der öffentlichen Wahrnehmung, Bußgelder für Datenschutzverletzungen und Gerichtsverfahren ausgesetzt sind, ist es wichtig, dass sich alle Managementebenen risikobasierter Entscheidungen bewusst sind – **Kommunikation -**
- Einrichten eines **Datenschutzrats** auf operativer Ebene – **unklare Sach- bzw. Rechtslage klären**
- Einrichten eines **Data Privacy Decision Board** auf oberster Managementebene – **schnelle endgültige Entscheidung**

GPR-Stream: proaktive und strategische Beratung

Umsetzung

Umsetzung

- Überprüfen der allgemeinen Datenschutzeinstellungen und Suchen nach alternativen Optionen - **Flexibilität** -
- Übertragen der aktuellen Entwicklungen im Unternehmen auf den Beratungsplan (Advice Map) – **Anwendbarkeit** -
- Sicherstellen, dass die Empfehlungen eingehalten werden - **Effektivität** -
- Vierteljährlich an das Group Privacy Leadership Team berichten, um die notwendigen weiteren Schritte zu erörtern - **Sensibilisierung und Fokussierung** -

GPR-Stream: proaktive und strategische Beratung

Vorbereitung des Unternehmens auf eine schnellere Umsetzung

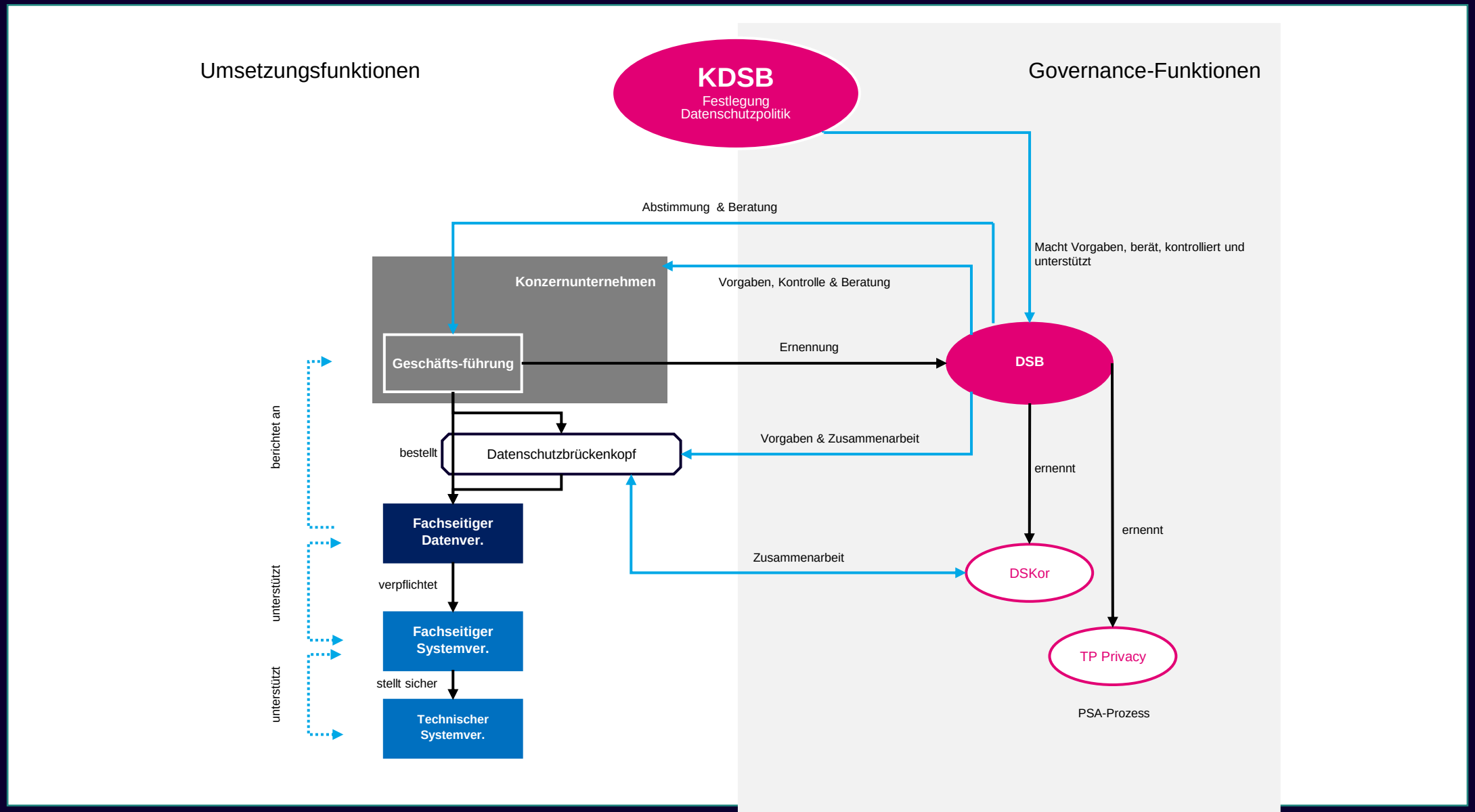
Strukuren

Nicht nur der Datenschutzbeauftragte und sein Team sondern auch das operative Management und seine Führungskräfte müssen sich ihrer Pflichten und Verantwortung bewusst sein:

Verantwortlichkeiten können delegiert werden

- Übertragene Verantwortlichkeiten auf n-1-Ebene (Geschäftsfelder) – Datenverantwortlicher
- Übertragene Verantwortlichkeiten auf operativer Ebene – fachlicher Systemverantwortlicher
- Gegebenenfalls übertragene Verantwortlichkeiten in der IT – Technischer Systemverantwortlicher

Privacy by Strategy - Strukturen



Vielen Dank!

telekom.com/datenschutz
datenschutz@telekom.de