DATENSCHUTZ IN DER PRAXIS

DR. CLAUS D. ULMER, GROUP DATA PRIVACY OFFICER DEUTSCHE TELEKOM

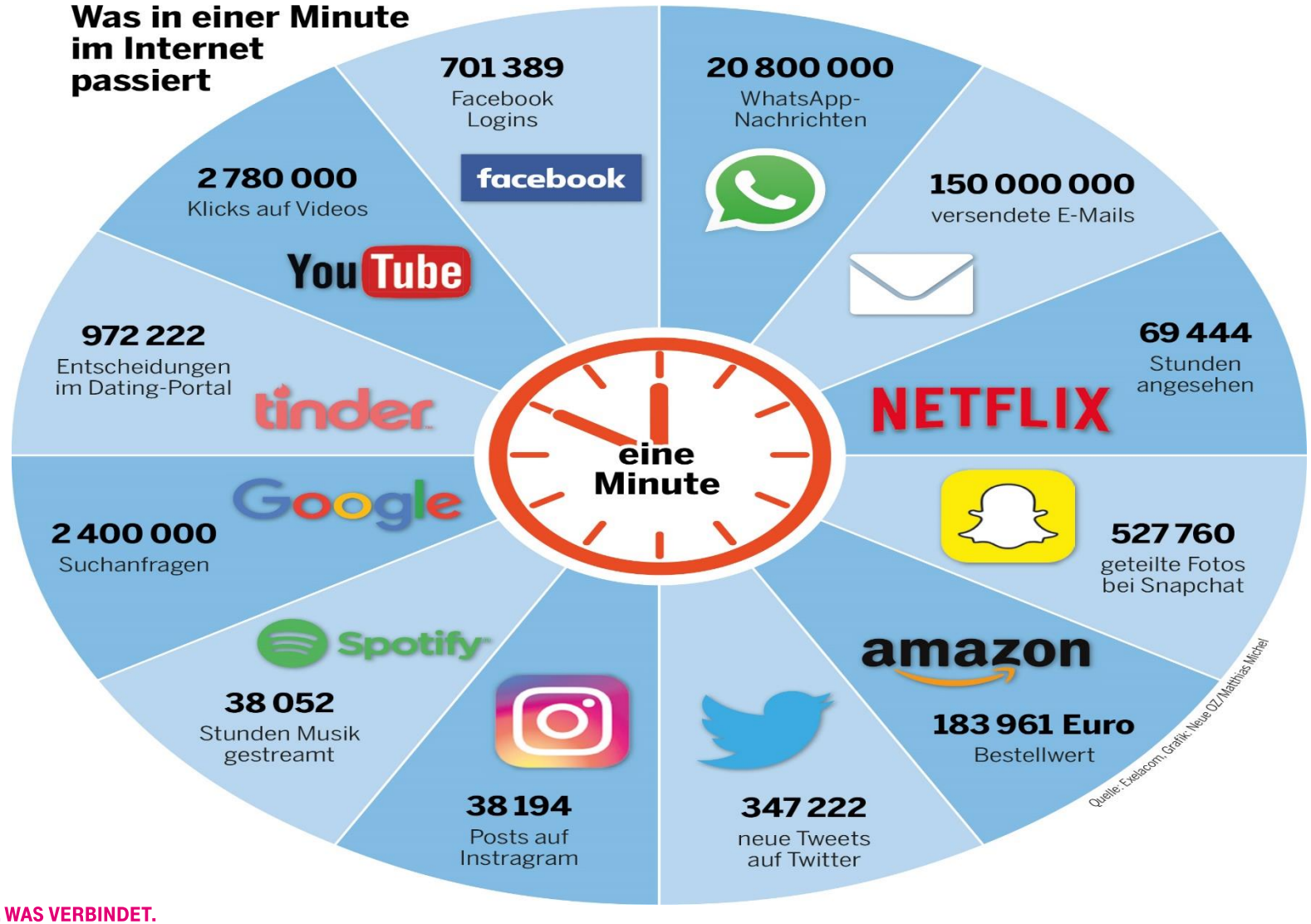
SAARBRÜCKEN
19. JULI 2017

ERLEBEN, WAS VERBINDET.

DIE DIGITALISIERUNG

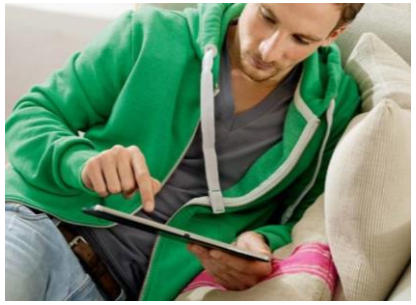
IHRE AUSWIRKUNG AUF GESCHÄFTSMODELLE UND DEN DATENSCHUTZ

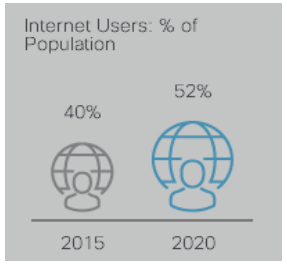
60 SEKUNDEN IM INTERNET

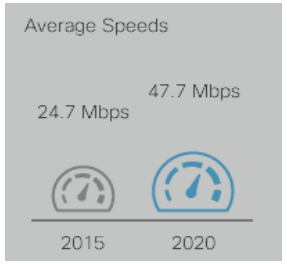


AUSTAUSCH, VERARBEITUNG UND ANALYSE VON DATEN NEHMEN IMMER MEHR ZU

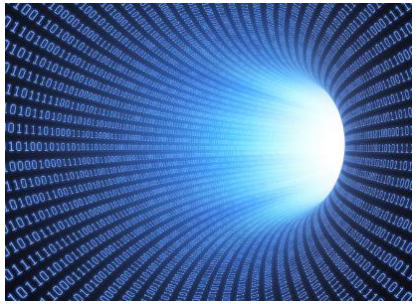
Umfangreiche Verarbeitung von personenbezogenen Daten

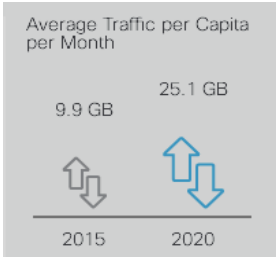




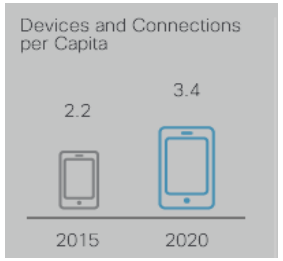


Steigende Komplexität durch weltweite Datenflüsse





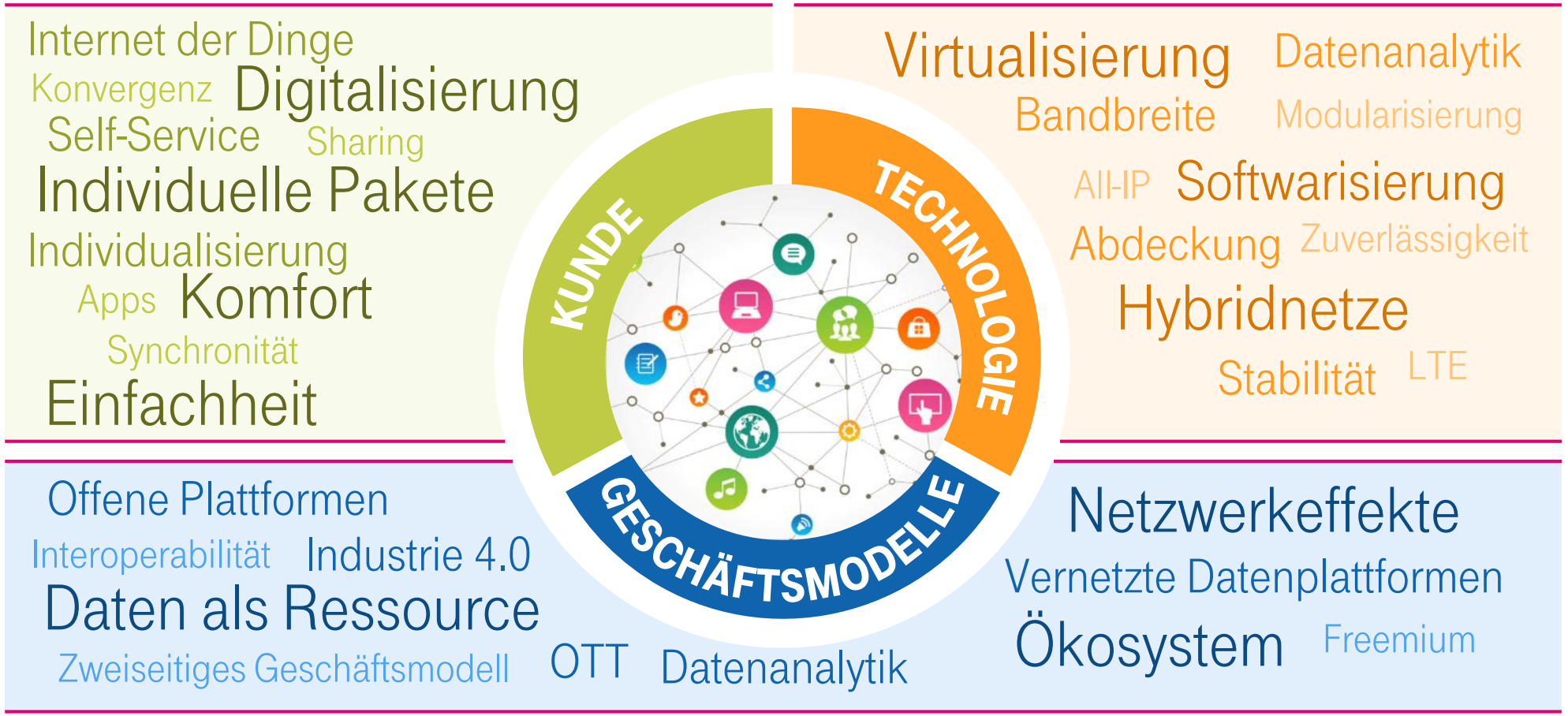
Umfassende Vernetzung von Endgeräten und Alltagsgegenständen



... die digitale Gesellschaft braucht Daten für ihre zukunftsfähige Entwicklung.

Source: CISCO, VNI Complete Forecast Highlights Tool, 2016

WANDEL DER BRANCHENPARADIGMEN



SKEPSIS DER BEVÖLKERUNG UND MANGELNDES VERTRAUEN GEFÄHRDEN DIE DIGITALEN GESCHÄFTSMODELLE

CERES-Studie „Digitale Selbstbestimmung“*

91 % der Deutschen glauben, dass im Internet unbemerkt auf die persönlichen Daten der Nutzer zugegriffen wird.

82 % denken, dass die meisten Unternehmen die Daten ihrer Kunden auch an andere Unternehmen weitergeben.

85 % meinen, dass man nicht herausfinden kann, welche privaten Unternehmen oder staatlichen Stellen persönliche Daten von ihren Kunden speichern.

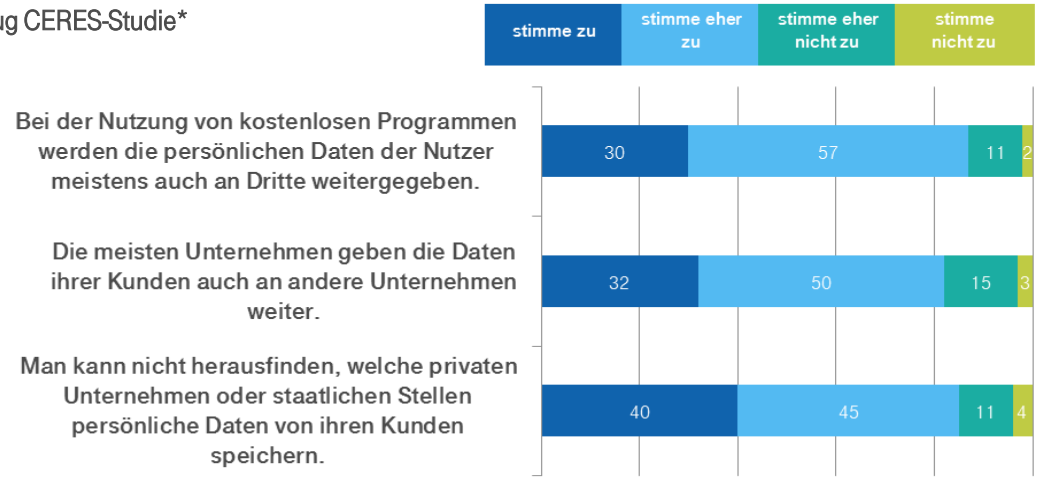
Dimap Studie „EU und Digitalisierung“**

80 % der 18-24 jährigen Deutschen wollen, dass sich die Politik „um die Stärkung des Datenschutzes besonders kümmern“ soll.

NTIA Umfrage – USA***

45 % von 41.000 befragten amerikanischen Haushalten gaben an, die Internet-Nutzung wegen Datenschutz-Bedenken einzuschränken.

Beispiel Auszug CERES-Studie*



* Quelle: Studie „Digitale Selbstbestimmung“; CERES im Auftrag der Telekom 2016
** Quelle: Studie „Europäische Union und Digitalisierung“, Dimap im Auftrag des Presse- und Informationsamts der Bundesregierung, April 2016
***Quelle: Studie National Telecommunications and Information Administration (NTIA) Mai 2016

WAS ERWARTEN DIE KUNDEN VON UNTERNEHMEN? - AUS: CERES-STUDIE - „DIGITALE SELBSTBESTIMMUNG“*

91% der Befragten wollen wissen, welche Daten über sie online vorliegen.

88 % wünschen sich eine persönliche Einflussnahme auf die Weiterverarbeitung ihrer Daten im Netz.

95% wollen über die Weiternutzung ihrer Daten informiert werden.

* Quelle: Studie „Digitale Selbstbestimmung“; CERES im Auftrag der Telekom 2016

DIE REGULATORISCHEN RAHMEN-BEDINGUNGEN

DIE DATENSCHUTZ-GRUNDVERORDNUNG UND IHRE ZIELE

HARMONISIERUNG – EINHEITLICH HOHES DATENSCHUTZNIVEAU IN DER EUROPÄISCHEN UNION

“LEVEL PLAYING FIELD” – GILT FÜR ALLE UNTERNEHMEN, DIE IHRE LEISTUNGEN EU-BÜRGERN ANBIETEN

VERLÄSSLICHKEIT – SCHAFFUNG VON RECHTSSICHERHEIT FÜR INDUSTRIE UND BÜRGER

EFFEKTIVITÄT – UMSETZUNG VON VORSCHRIFTEN (PRIVACY BY DESIGN, RISIKO ASSESSMENT, BÜRGERRECHTE)

DATENSCHUTZ-GRUNDVERORDNUNG
AUSWIRKUNGEN AUF GESCHÄFTSMODELLE

Chancen

Positive Auswirkungen auf Geschäftsmodelle

- **Cloud Business**, Zertifizierung erleichtert den Nachweis der Compliance z.B. für Cloud -Anbieter und kann damit erheblich administrative Aufwände reduzieren.
- **Big Data**, erweiterter Anwendungsbereich für Big Data Auswertungen unter Verwendung pseudonymer Daten, die Kunden haben ein Widerspruchsrecht (z.B. Internet of Things, Nutzerpofile bei Connected Car). Bislang nur in Ausnahmefällen möglich.
- **EU-Geschäftsmodelle und Lösungen**, verbesserte Voraussetzungen für europäische Projekte durch eine zentral zuständige Aufsichtsbehörde in Europa.
- **Level Playing Field**, soziale Netzwerke und OTTs müssen bei der Verarbeitung von Daten, die in Europa erhoben werden, das europäische Datenschutzrecht anwenden.

Risiken

Deutlich erhöhter Sanktionsrahmen: Bußgelder **für Unternehmen von bis zu 4 % des** weltweiten Jahres-umsatzes bei erheblichen Verstößen

WEITERE AKTIVITÄTEN IM REGULATORISCHEN UMFELD

Datenschutz-Grundverordnung – abgeschlossen

Umsetzungsgesetze in den Ländern? ...

Überarbeitung ePrivacy Richtlinie - läuft

Beschäftigtendatenschutz? ...

Leitfäden der Aufsichtsbehörden ...

DATENSCHUTZ-GRUNDVERORDNUNG
AUSWIRKUNGEN AUF GESCHÄFTSMODELLE

Chancen

Positive Auswirkungen auf Geschäftsmodelle

- **Cloud Business**, Zertifizierung erleichtert den Nachweis der Compliance z.B. für Cloud -Anbieter und kann damit erheblich administrative Aufwände reduzieren.
- **Big Data**, erweiterter Anwendungsbereich für Big Data Auswertungen unter Verwendung pseudonymer Daten, die Kunden haben ein Widerspruchsrecht (z.B. Internet of Things, Nutzerpofile bei Connected Car). Bislang nur in Ausnahmefällen möglich.
- **EU-Geschäftsmodelle und Lösungen**, verbesserte Voraussetzungen für europäische Projekte durch eine zentral zuständige Aufsichtsbehörde in Europa.
- **Level Playing Field**, soziale Netzwerke und OTTs müssen bei der Verarbeitung von Daten, die in Europa erhoben werden, das europäische Datenschutzrecht anwenden.

Risiken

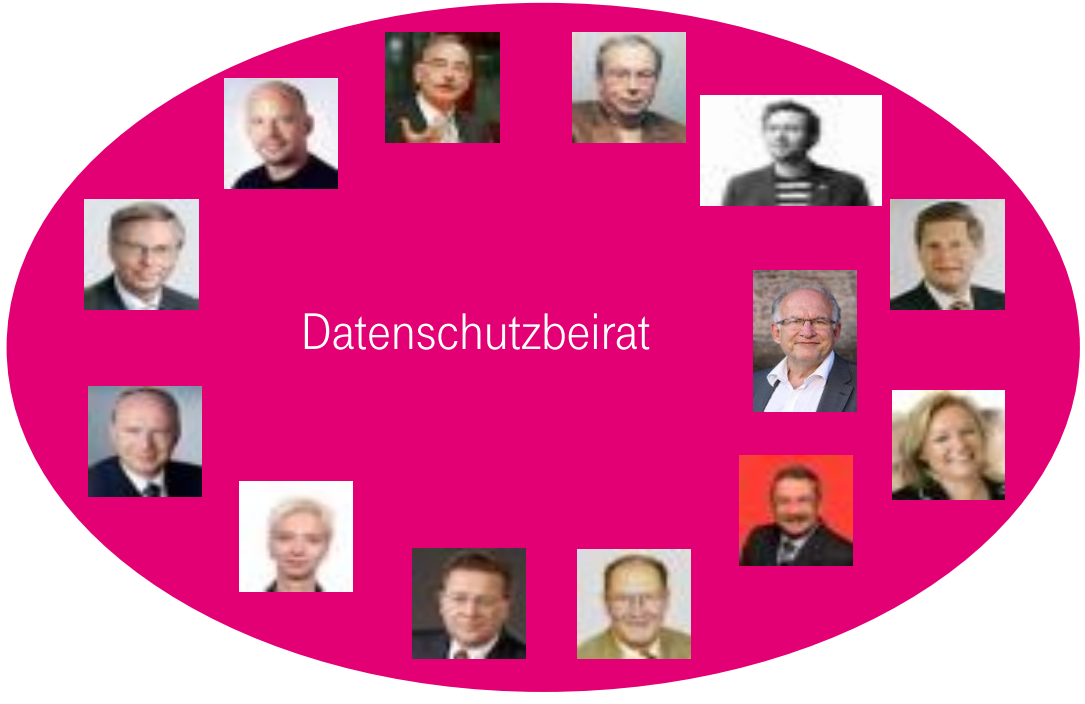
Deutlich erhöhter Sanktionsrahmen: Bußgelder **für Unternehmen von bis zu 4 % des** weltweiten Jahres-umsatzes bei erheblichen Verstößen

Zusätzlich:

- Nicht koordinierte gesetzgeberische und aufsichtsbehördliche Aktivitäten gefährden die Harmonisierung in Europa

WAS MACHT DIE DEUTSCHE TELEKOM IM DATENSCHUTZ?

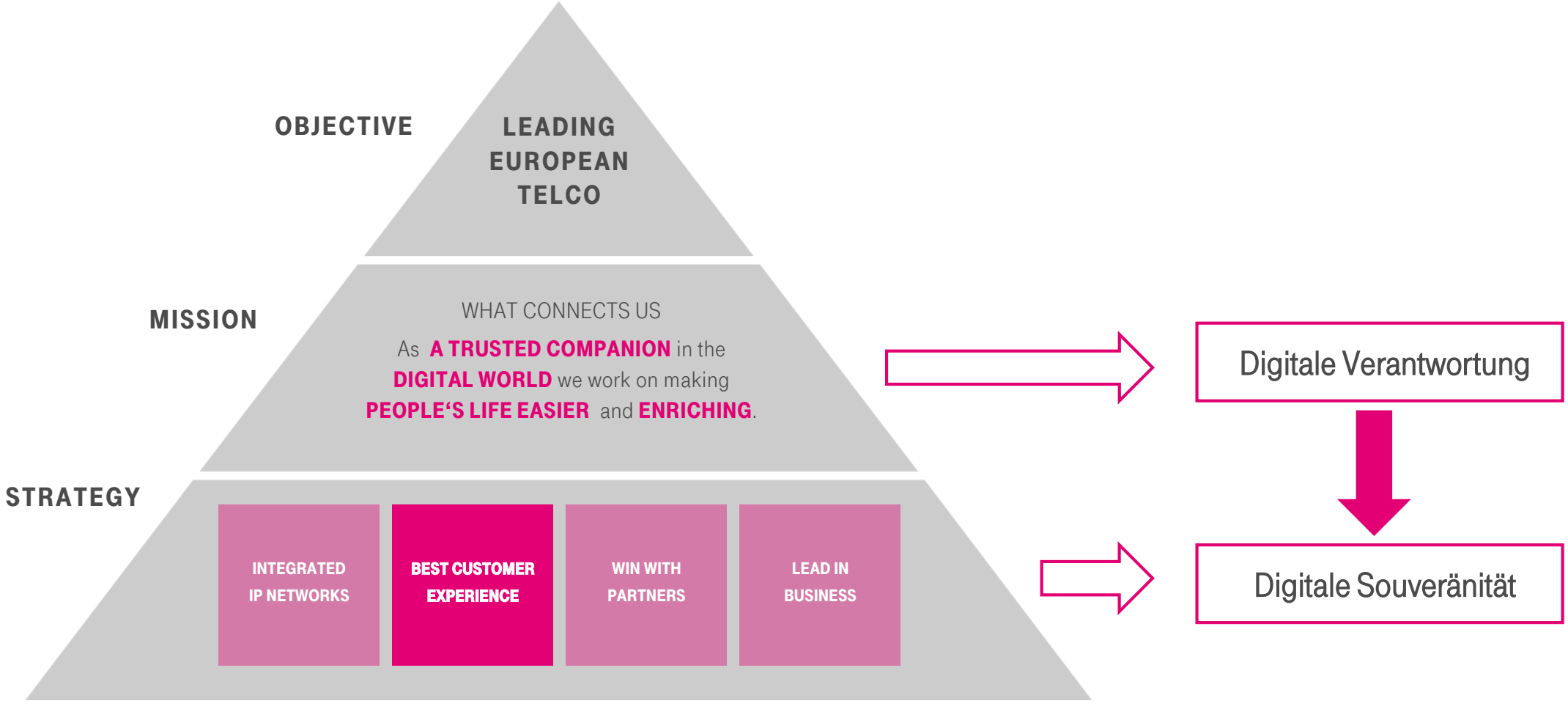
DER DATENSCHUTZBEIRAT DER DEUTSCHEN TELEKOM



Der Datenschutzbeirat ist ein unabhängiges Beratungsgremium des Vorstands der Deutschen Telekom AG. Er dient dem konstruktiven Austausch mit führenden Datenschutzexperten und Persönlichkeiten aus Politik, Lehre, Wirtschaft und unabhängigen Organisationen und berät zu wichtigen datenschutzrelevanten Themen.

KONZERNSTRATEGIE DEUTSCHE TELEKOM

VERTRAUEN IST EIN WICHTIGER BESTANDTEIL



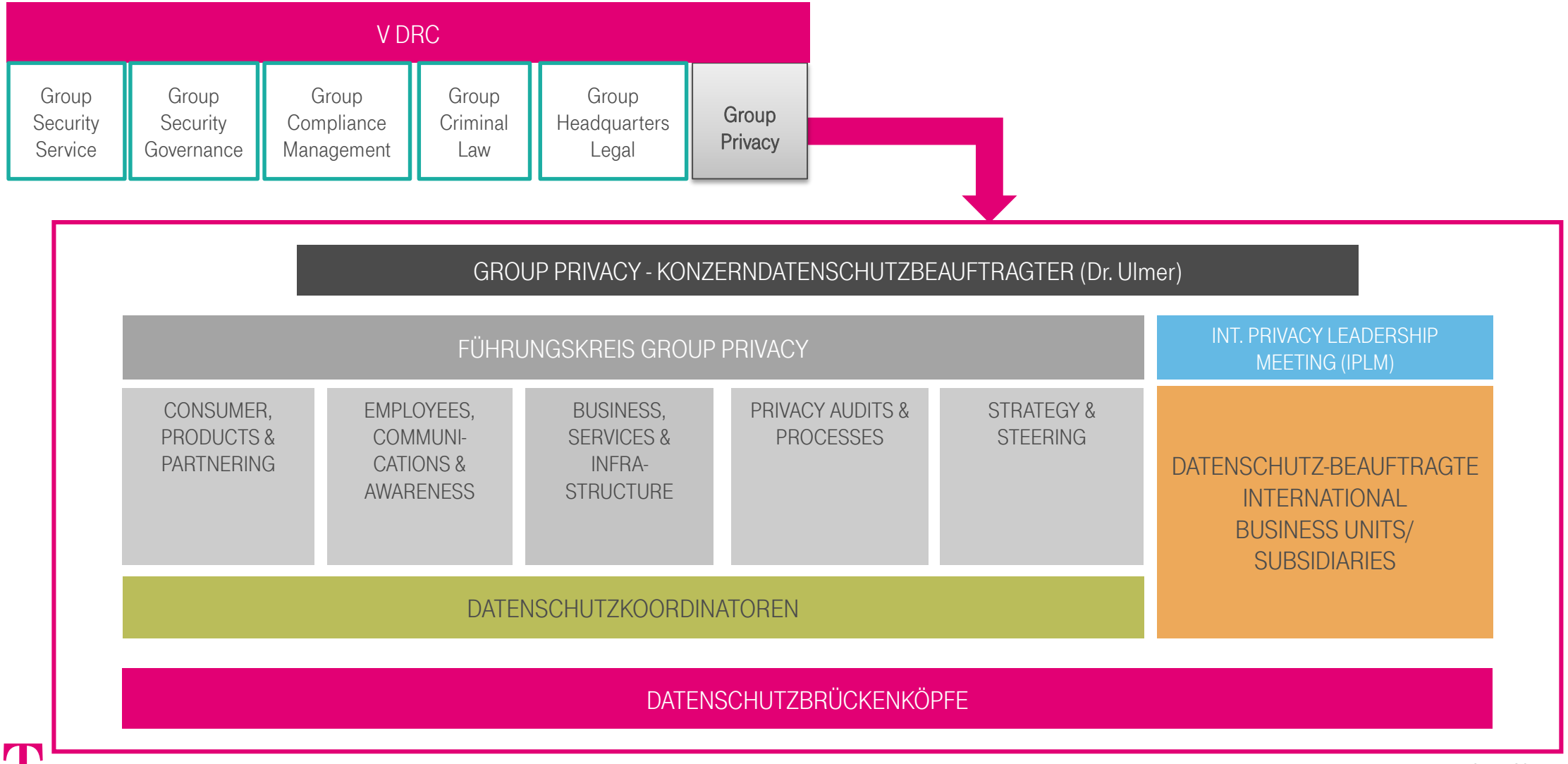
DIE DEUTSCHE TELEKOM NIMMT IHRE VERANTWORTUNG WAHR

„Die Deutsche Telekom sieht sich in der Verantwortung, das **Vertrauen der Menschen** in den Umgang mit ihren Daten nachhaltig zu stärken. Nur so können digitale Geschäfts- und Verarbeitungsmodelle zum **Wohle der Gesellschaft** und des Einzelnen **erfolgreich** weiter entwickelt werden.

Die digitale Souveränität der Menschen steht dabei im Vordergrund. Sie wird gewährleistet durch ein hohes Maß an **Transparenz, Entscheidungsfreiheit** und **die Entwicklung von datenschutzfreundlichen Lösungen**. Dafür müssen Datenschutzexperten **von Anfang an** in die Entwicklung neuer Produkte und Dienste einbezogen werden, in denen personenbezogene Daten verarbeitet werden.“

(Auszug aus DT Whitepaper „Datenschutz in der digitalen Welt“)

DIE DATENSCHUTZORGANISATION DER DTAG



ZERTIFIZIERTES MANAGEMENTSYSTEM

INSTITUT DER WIRTSCHAFTSPRÜFER PRÜFSTANDARD 980

COMPLIANCE MANAGEMENT SYSTEM: PRÜFSTUFEN

1. Stufe

Sind die Grundsätze und Maßnahmen des CMS* zutreffend beschrieben?

2. Stufe

... und auch 2. angemessen und zu einem bestimmten Zeitpunkt implementiert?

3. Stufe

... und auch 3. zu einem bestimmten Zeitpunkt wirksam?

*Compliance Management System

PRÜFUNGSERGEBNIS

FESTSTELLUNGEN UND EMPFEHLUNGEN

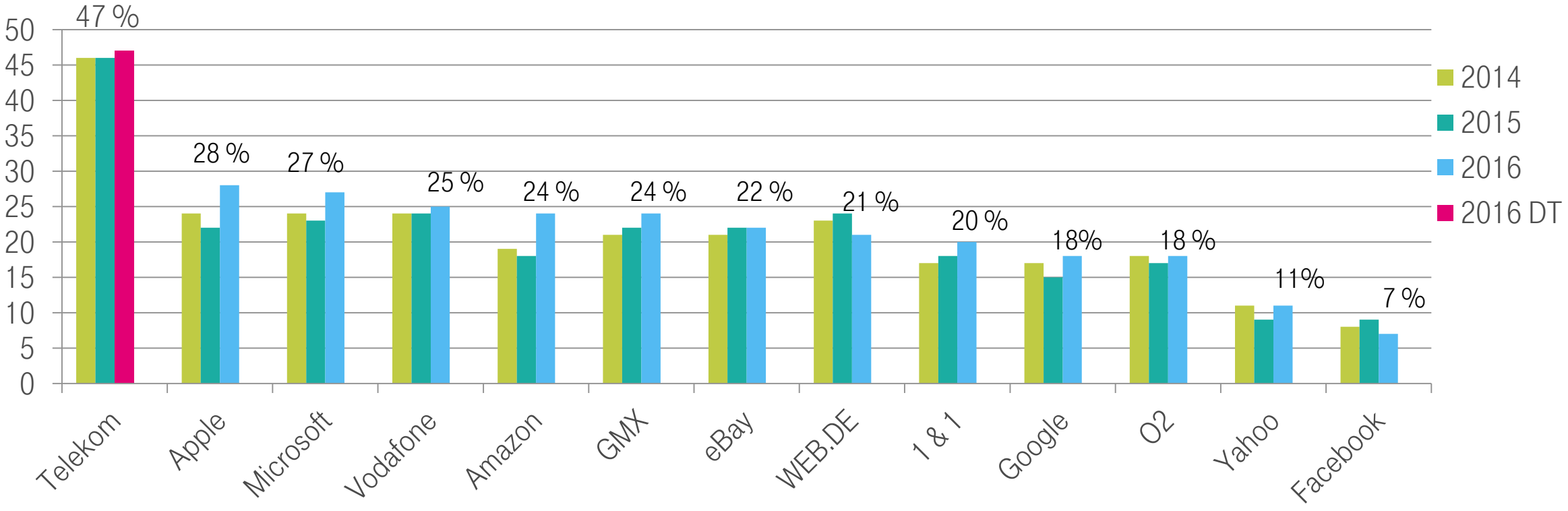
Die Wirksamkeitsprüfung gemäß Prüfungsstandard 980 (PS 980) des Instituts deutscher Wirtschaftsprüfer (IDW) ergab **keinerlei Feststellungen.**

ZERTIFIZIERUNG ERFOLGREICH

Die Zertifizierung der datenschutzbezogenen Compliance-Organisation der Deutschen Telekom AG (mit Wirkung für die Telekom Deutschland GmbH und deren Mehrheitsbeteiligungen sowie die T-Systems International GmbH und deren Mehrheitsbeteiligungen) wurde am **30. September 2014** erteilt.

VERTRAUENSWÜRDIGSTES UNTERNEHMEN IN DER INTERNET UND MOBILFUNK-BRANCHE*

Wenn Sie einmal danach gehen, was Sie wissen oder vermuten: Welche Unternehmen halten Sie für vertrauenswürdig, wenn es um den Umgang mit persönlichen Daten geht?



*Quelle: Institut für Demoskopie Allensbach, Allensbach Studie 2016

TOP-BEWERTUNGEN BEI NACHHALTIGKEITS-FONDS

ROBECOSAM
Sustainability Investing
(Dow Jones Sustainability Index)

✓ **Privacy Policy 100%, Best in Class**

✓ Data protection and information security: A+
- Policy on data protection A
- Information security management system A+

oekom research

SUSTAINALYTICS

✓ Data Privacy and Security
- Data Privacy & Security Program 100%
- Data Request Management 100%

"Further Development of Data Privacy Principles for the "Internet of Things" and "Industry 4.0" is worth the effort in investing in IoT and M2M."

DIE AUFGABEN DES DATENSCHUTZ-BEAUFTRAGTEN

KONZERNBEAUFTRAGTER FÜR DEN DATENSCHUTZ – FUNKTION – BEISPIEL TELEKOM

DATENSCHUTZBEAUFTRAGTER IN DEUTSCHLAND
STRATEGISCHE VORGABE UND KONTROLLINSTANZ FÜR DEN GESAMTKONZERN

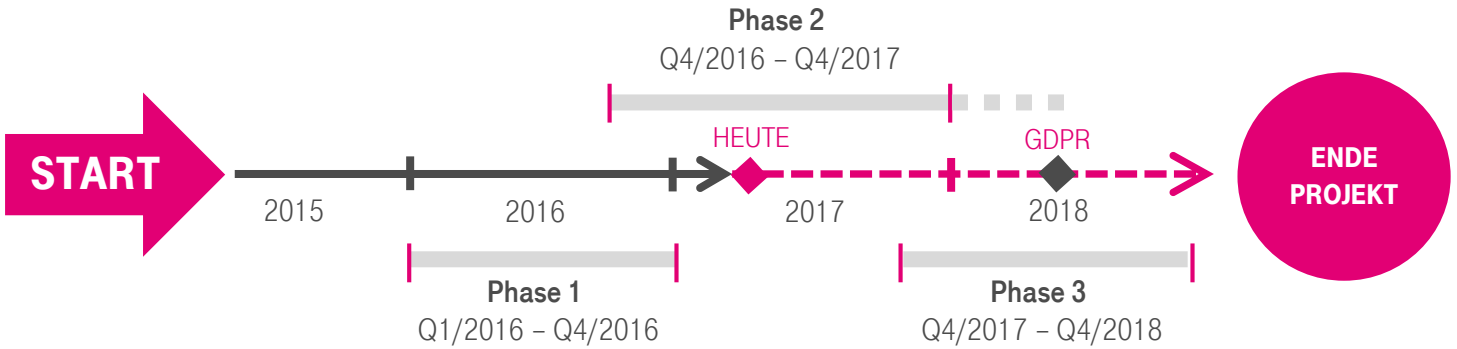
STEUERUNG UND KOORDINIERUNG DER DATENSCHUTZORGANISATIONEN UND UMSETZUNGSFUNKTIONEN IM KONZERN WELTWEIT

TREIBER UND IDEENGEBER FÜR KUNDEN- UND MARKTORIENTIERTE DATENSCHUTZLÖSUNGEN

GROSSE PROJEKTE INITIIEREN UND VORANTREIBEN

UMSETZUNGSPROJEKT DATENSCHUTZ-GRUNDVERORDNUNG

- **Phase 1** Entwicklung regulatorischer Rahmen (BI) ✓
- **Phase 2** Implementierung der Anforderungen
- **Phase 3** Compliance Check



Next Steps

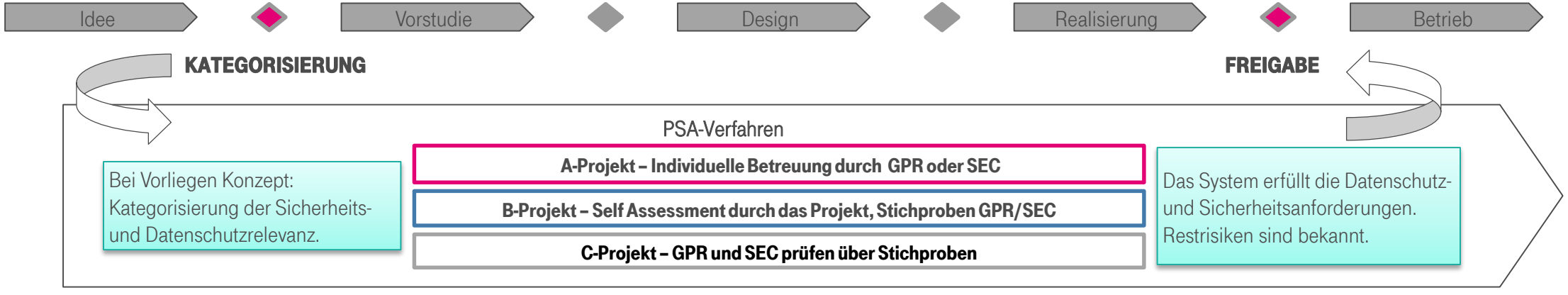
- Priorisierung der Implementierung wird von allen Segmenten vorgenommen, DSB unterstützt
- Fortführung IT- und Prozessanpassungen innerhalb des Konzerns
- Regelmäßig Monitoring und Beratung des DSB für alle Angelegenheiten zum Datenschutz
- Alle relevanten Aspekte wurden identifiziert und implementiert
- Implementierung läuft planmäßig

UNTERNEHMENSPROZESSE GESTALTEN

NEUE ENTWICKLUNGEN UNTERSTÜTZEN

Privacy & Security Assessment Verfahren

Das **Privacy & Security Assessment (PSA)** ist das zentrale Verfahren, um Sicherheits- und Datenschutzanforderungen in mehr als zweitausend IT-/NT-Entwicklungsprojekten pro Jahr sicherzustellen.



Ziele

- Integration von Sicherheit und Datenschutz in Produkt- und Systementwicklung
- Fokussierung wertvoller Ressourcen auf die größten Risiken
- Privacy/Security by Design – bedarfsgerechte Beratung prozessbegleitend von Projektbeginn bis zur Erstellung der Compliance Dokumentation
- komplexe Sachverhalte zielgerichtet und einheitlich betreuen durch dedizierte Anforderungskataloge

AUDITKONZEPT ENTWICKELN

BEISPIEL DEUTSCHE TELEKOM: AUDITJAHRESPROGRAMM, BASISDATENSCHUTZAUDIT SOWIE ABNAHME- UND ANLASSAUDITS

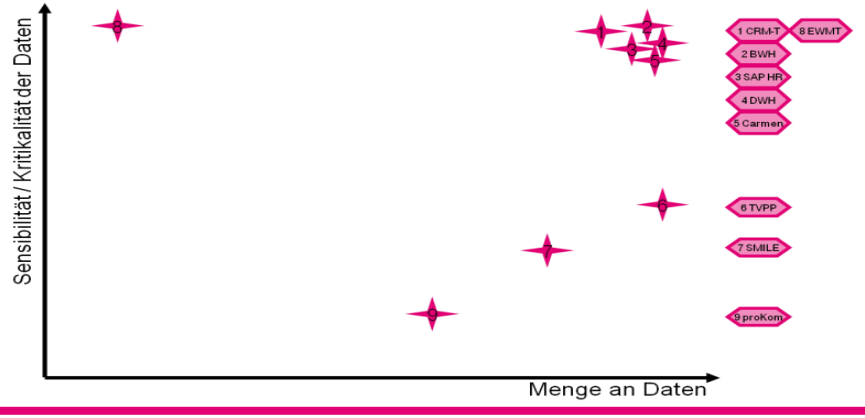
	Privacy Inspections		
	Konzerndatenschutzaudit	Inspectionprogramm	Abnahme-/Anlassaudits
Zielgruppe	Alle Mitarbeiter DTAG National/International	TOP-Systeme/-Plattformen Ausgewählte Zielgruppen und Arbeitsprozesse (z.B. Vertrieb/Partner) Internationale Audits	IT-Systeme/Plattformen vor Wirkbetrieb Entsprechende Zielgruppen/ Arbeitsprozesse
Frequenz	1x jährlich	Risikobasierte Jahresauditplanung	Anlassbezogen, z. B. durch Vorfall
Inhalte	Self Assessment auf Mitarbeiterebene national sowie international zu ▪ Denken ▪ Wissen ▪ Handeln Zusätzlich international ▪ Selbstauskunft der Data Privacy Officers (DPO) zur Umsetzung der Vorgaben des Privacy Code of Conduct (PCoC) ▪ Verifikation über Stichproben	▪ Auditierung und Bewertung hinsichtlich der Rechtsgrundlagen aus einschlägigen Gesetzen (TKG, TMG, BDSG, PCoC), z.B. Zweckbindung, Datensparsamkeit ▪ technische Prüfung auf Basis § 9 BDSG (nebst Anlage) der technischen und organisatorischen Maßnahmen ▪ individualisierter Auditscope	▪ Auditierung und Bewertung hinsichtlich der Rechtsgrundlagen aus einschlägigen Gesetzen (TKG, TMG, BDSG, PCoC), z.B. Zweckbindung, Datensparsamkeit ▪ technische Prüfung auf Basis § 9 BDSG (nebst Anlage) der technischen und organisatorischen Maßnahmen ▪ individualisierter Auditscope

KRITIKALITÄTEN NACH RISIKOLANDKARTE

SYSTEMATISCHE DARSTELLUNG

Risikobewertung

- im Zuge der Beratung durch den Datenschutz
- an Hand definierter Kriterien
- ausgewiesen durch Score
- verankert in GPR-Prozessen



Expertenbeitrag

- intern (z.B. Datenschutzberater, dezentrale Datenschutzberater)
- extern (z.B. Fachseite)
- ergänzt die Risikobewertung

Risikokriterien, z.B.

- Klassifizierung gem. Prüfverfahren für Systeme
- Awardkennzahl aus Konzernaudit (Gesellschaft)
- Anzahl Datensätze
- Datawarehousing

STRATEGIEN FÜR DAS UNTERNEHMEN ENTWICKELN

Beispiel Telekom

Mission

VERTRAUENS-RÄUME SCHAFFEN!

Was

Unsere Ziele:

- **Compliance** – auch mit der bevorstehenden Europäischen Gesetzgebung – Entwickeln, Implementieren und Monitoren von Anforderungen
- **Stärkung kundenorientierter** Geschäftsmodelle - transparente und einfache Kundeninformationen und -einwilligungen
- Nachhaltige **Geschäftskundenlösungen** - "Privacy by design" Lösungen, wie zum Beispiel Pseudonymisierung und Anonymisierung.
- **Einen zukunftsfähigen Rechtsrahmen mitgestalten -** Beteiligung an Expertenrunden und politischen Diskussionen.

Wie

Jede Datenschutzlösung baut auf den Kernprinzipien auf:

Einfach

Kundenorientiert

Rechtssicher

Dynamisch

DER DATENSCHUTZBEAUFTRAGTE

Heute

Vom Vorgaben- und Kontrollorgan ...

Morgen

... zum Impulsgeber im Unternehmen.

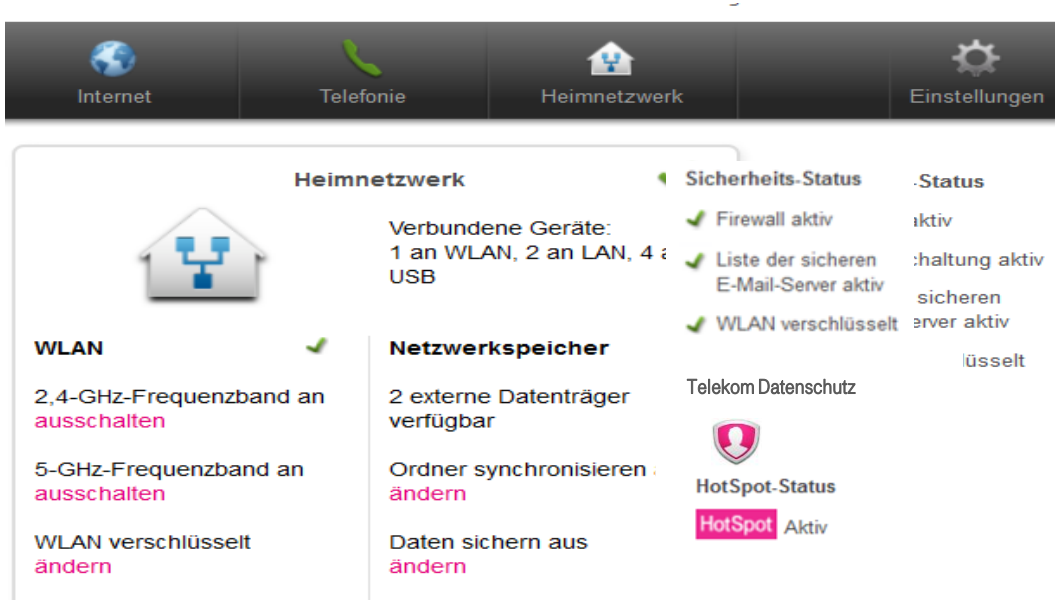
DATENSCHUTZ IN PRODUKTEN

PRIVACY BY DESIGN

BEISPIEL: PRIVACY ICON

IPv6 - PRIVACY BUTTON IM SPEEDPORT ROUTER

ICON



Erläuterung

- Privacy Icon als Privacy Button
- Über den Privacy Button wird der IP Adressenwechsel in allen zukünftigen Speedport – Routern gesteuert

BEISPIEL: BEGLEITUNG DES BUSINESS MARKETPLACE DER DEUTSCHEN TELEKOM

TRANSPARENZ DURCH ICONS

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 Informationen 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)

INFORMATIONSTIEFE

BEISPIEL: BEGLEITUNG DES BUSINESS MARKETPLACE DER DEUTSCHEN TELEKOM

TRANSPARENZ DURCH ICONS

Hosting-Standort

D — Datenspeicherung in Deutschland

EU — Datenspeicherung in der EU

CH — Datenspeicherung in der Schweiz

Datenspeicherung außerhalb EU & Schweiz

Applikationsbetrieb

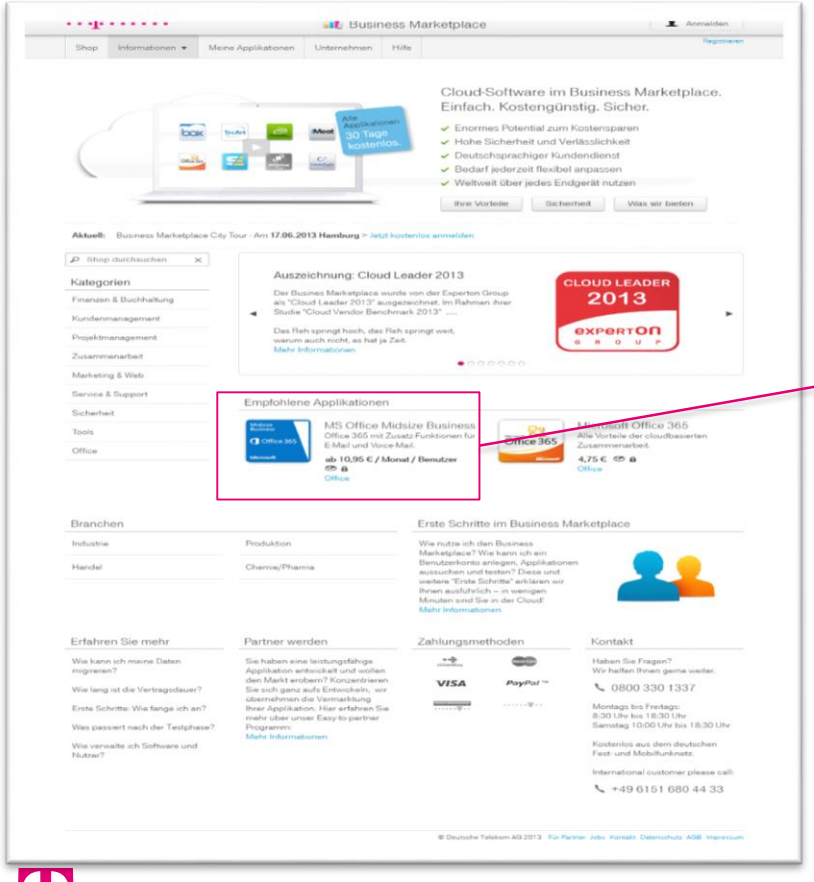
Der Betrieb erfolgt durch die Deutsche Telekom. Es kommen die hohen Sicherheitsstandards der Deutschen Telekom zur Anwendung.

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.

BEISPIEL: BEGLEITUNG DES BUSINESS MARKETPLACE DER DEUTSCHEN TELEKOM

TRANSPARENZ DURCH ICONS

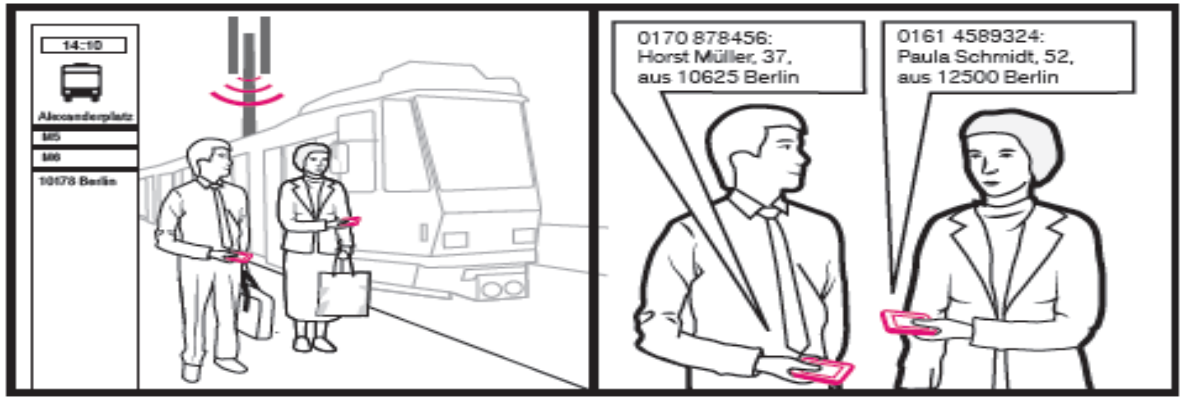


Mouseover

Office 365 wird durch unseren Partner betrieben.

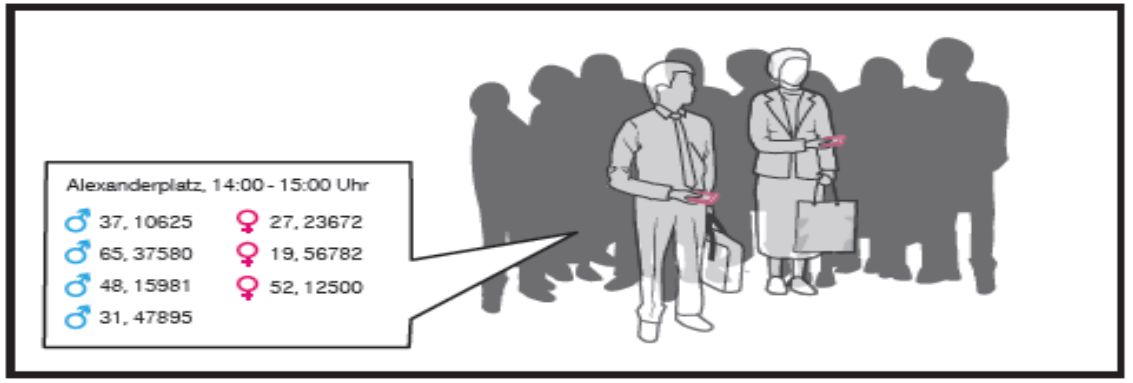
Datenspeicherung außerhalb EU & Schweiz

BEISPIEL: MOTIONLOGIC - ANONYMISIERUNGSLOGIK

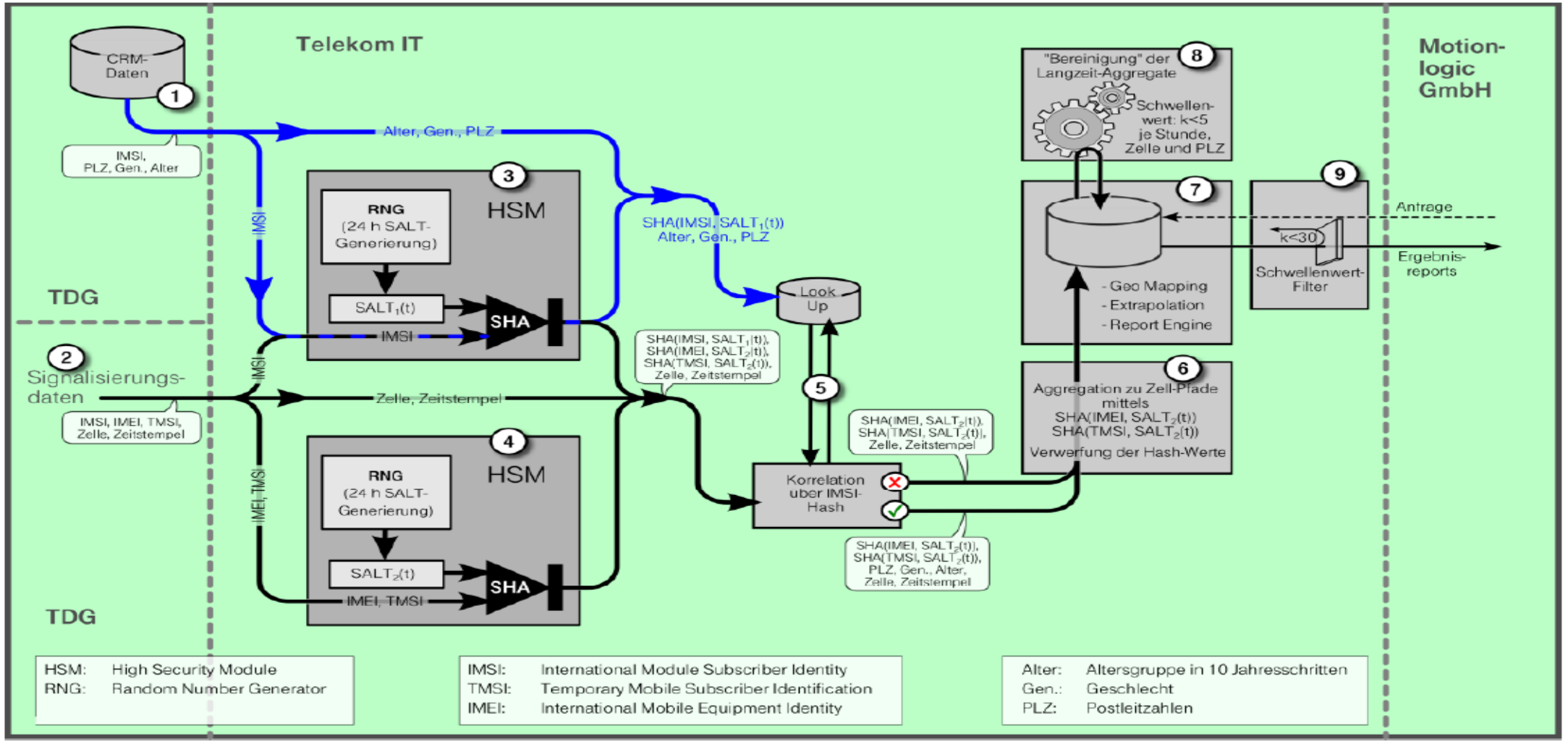


~~0170878456:~~
~~Horst Müller,~~ 37,
aus 10625

~~0161 4589324:~~
~~Paula Schmidt,~~ 52,
aus 12500



BEISPIEL: MOTIONLOGIC ANONYMISIERUNG-UMSETZUNG



BEISPIEL: FAHRTENMANAGER MOBILITY CAR

Wesentliche Merkmale

Nutzungs- & Laufleistungsabgrenzung

- Nutzungsabgrenzung für geschäftliche vs. private Fahrten
- Auswertungen über KM-Laufleistungen & Anzahl Geschäftsreisetage

Nutzungsvereinbarung

- Der Fahrer schließt eine Zusatzvereinbarung über die Nutzung eines Mobility Car ab
  ➔ beidseitige Freiwilligkeit

Geringer Aufwand für Fahrer

- Vorschlags-Algorythmus mit Erkennung von bereits hinterlegten wiederkehrenden Reisezielen oder ganzer Fahrten

Datenschutz und Datensicherheit

- Datensparsamkeit in der Erhebung von Daten
- Privatmodus-Schalter im Fahrzeug für absolute Diskretion bei Privatfahrten

➔

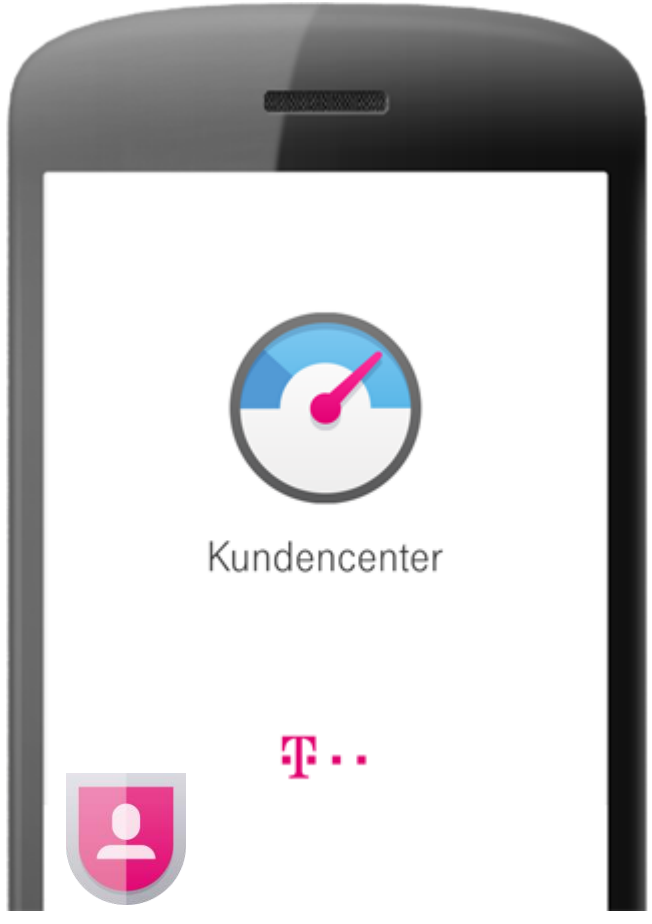
DATENSCHUTZ IN DER ZUKUNFT

BEISPIEL KUNDENERWARTUNG: DESIGN THINKING ANALYSE

POTENTIAL FÜR ALLGEMEINE VERBESSERUNGEN*

Datenschutz-Maßnahmen zurückhaltend, aber aktiv sichtbar machen

- Maßnahmen von Providern zum Schutz der Daten sind den Nutzern in der Regel **nicht bewusst**.
- Datenschutz oft an Stellen erklärt, die Nutzer **nicht aufsuchen.**
- Es fehlt an einer einfach verständlichen, für Nutzer **relevanten und attraktiven/illustrierten** Darstellung.
- Lösungsansätze:
  - Kommunikation in **die Produkte integriert**, durch Botschaften und Hinweise, z.B. in Login-Bereichen.
  - Mittelfristig kann Datenschutz auch zu einem **Produkt-Feature** ausgebaut werden.



*Abgeleitet von Ergebnissen der Nutzerstudie durch Agentur IXDS

KUNDENORIENTIERTE DATENSCHUTZ-LÖSUNGEN

ONE PAGER

verständliche Zusammenfassung der Datenschutz-Hinweise auf einer Seite.

DATA COCKPIT

zentrale Zusammenfassung und Steuerung der Daten des Kunden durch den Kunden an einer Stelle.

PRIVACY BOT

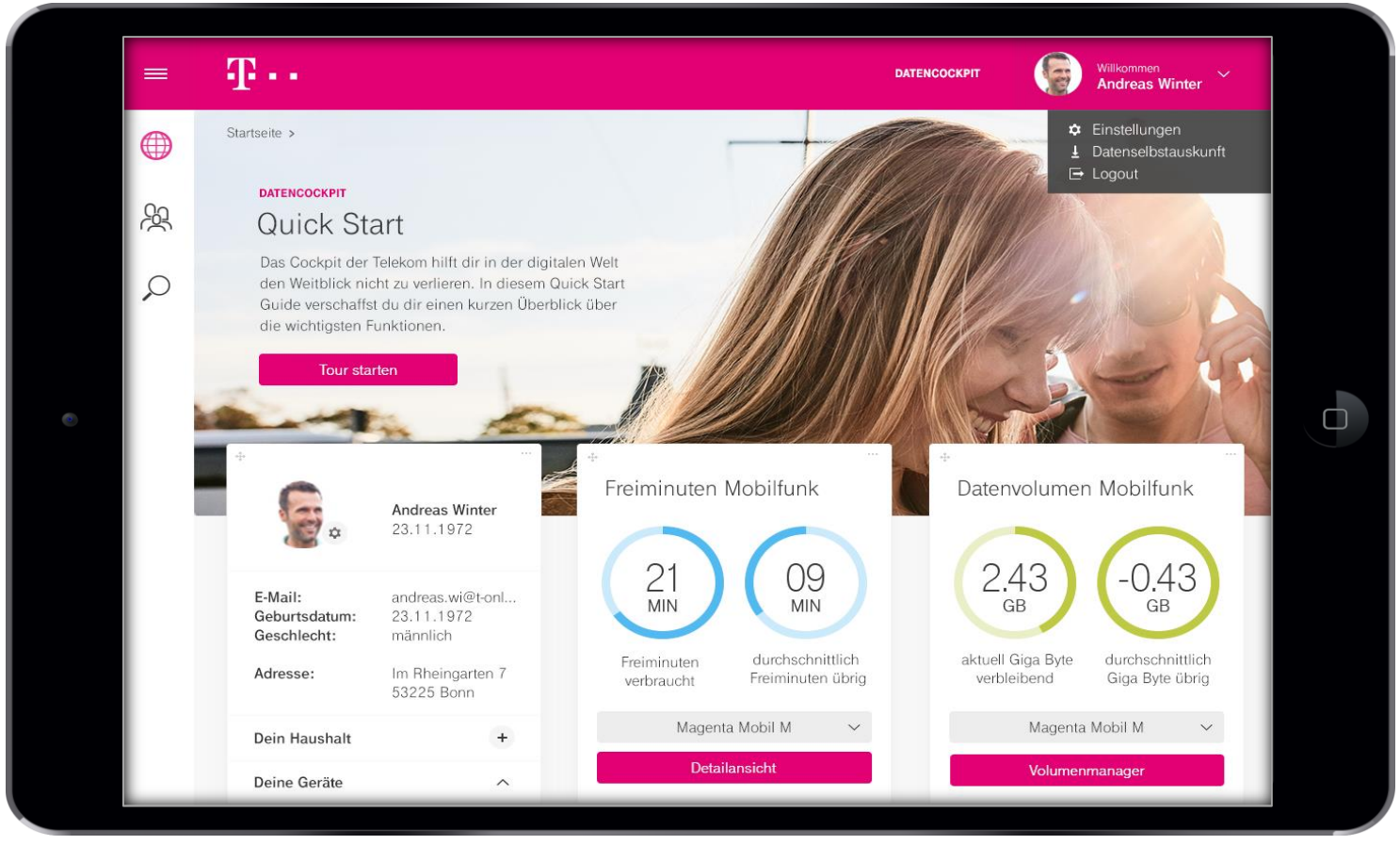
Mein Datenschutz-Vertreter in der digitalen Welt.

SCHAFFEN EIN „LEVEL PLAYING FIELD“ UND DAMIT AKZEPTANZ …

DEUTSCHE TELEKOM DATA COCKPIT

DER KUNDE KANN DAS DATA COCKPIT FÜR SEIN UMFASSENDES DATEN-MANAGEMENT VERWENDERN

- ✓ **Opt-in generator** für Abgabe und Widerruf von Einwilligungen
- ✓ **Übersicht** über die gespeicherten und verarbeiteten Daten
- ✓ Einfache Funktion, Daten herunterzuladen (“Datenportabilität”)



VIELEN DANK!

WWW.TELEKOM.COM/DATENSCHUTZ

WWW.TELEKOM.COM/PRIVACY