

# EINFACH NUTZEN – WAS MACHT DIE PRIVATE DATENWIRTSCHAFT ANDERS?

Berlin, 29. Juni 2016

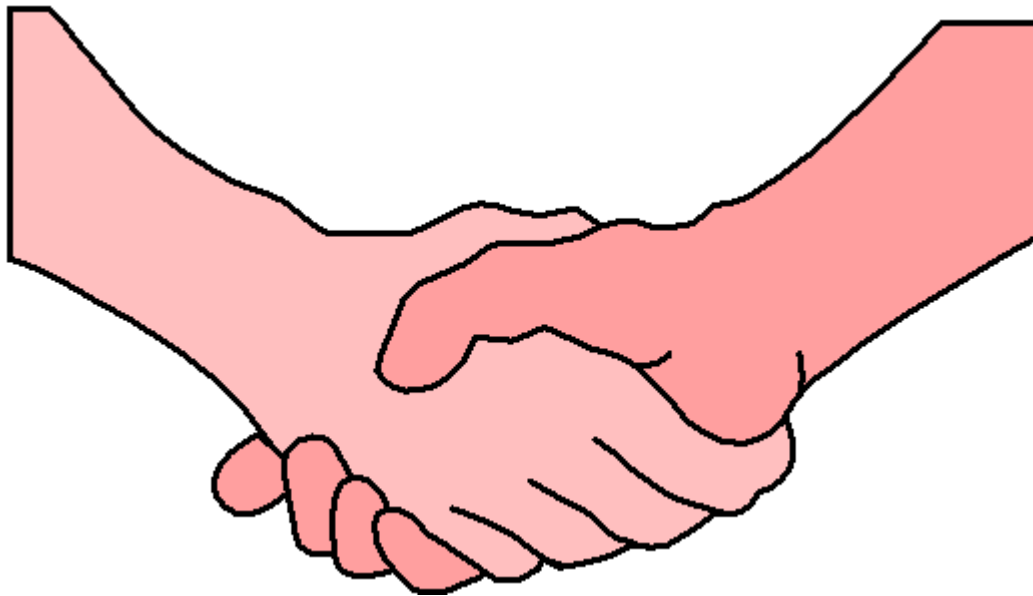


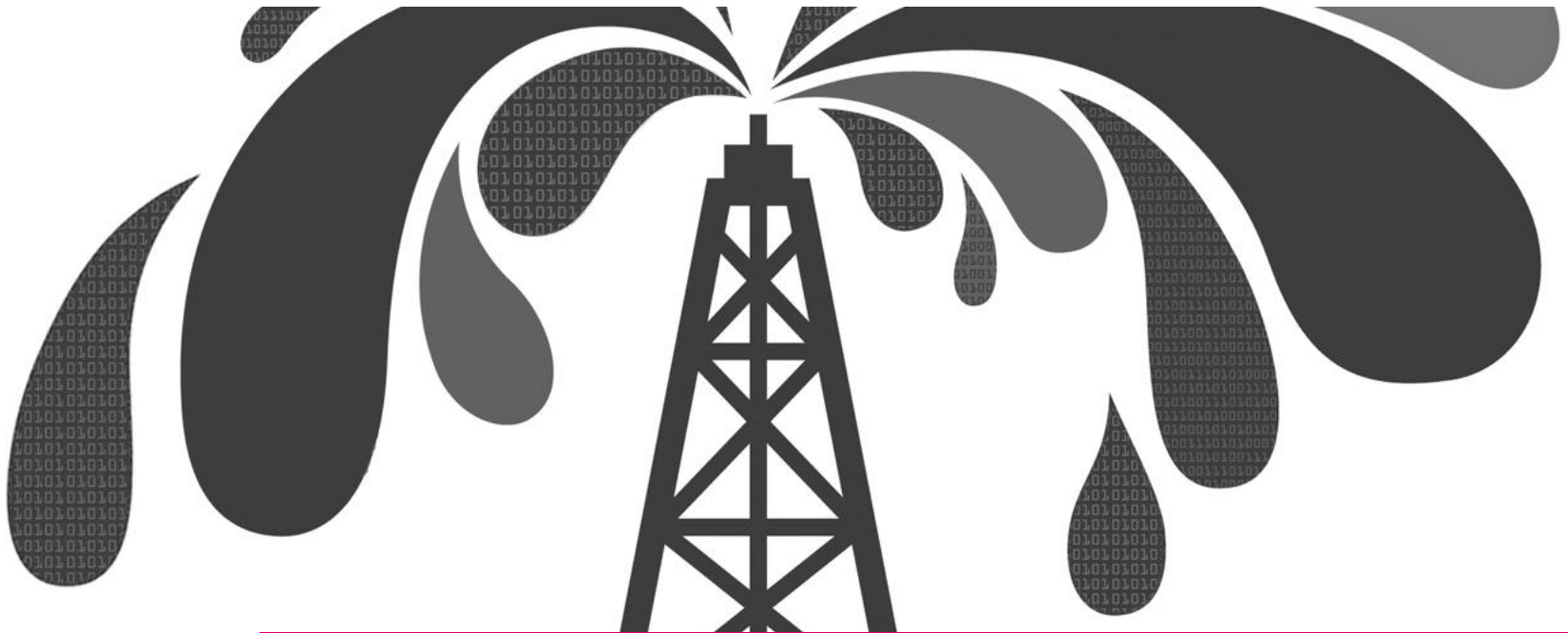
HEALTHCARE SOLUTIONS

# DIE ANTWORT VORNEWEG

Es gibt nur geringe Unterschiede zwischen privater und öffentlicher Datenwirtschaft

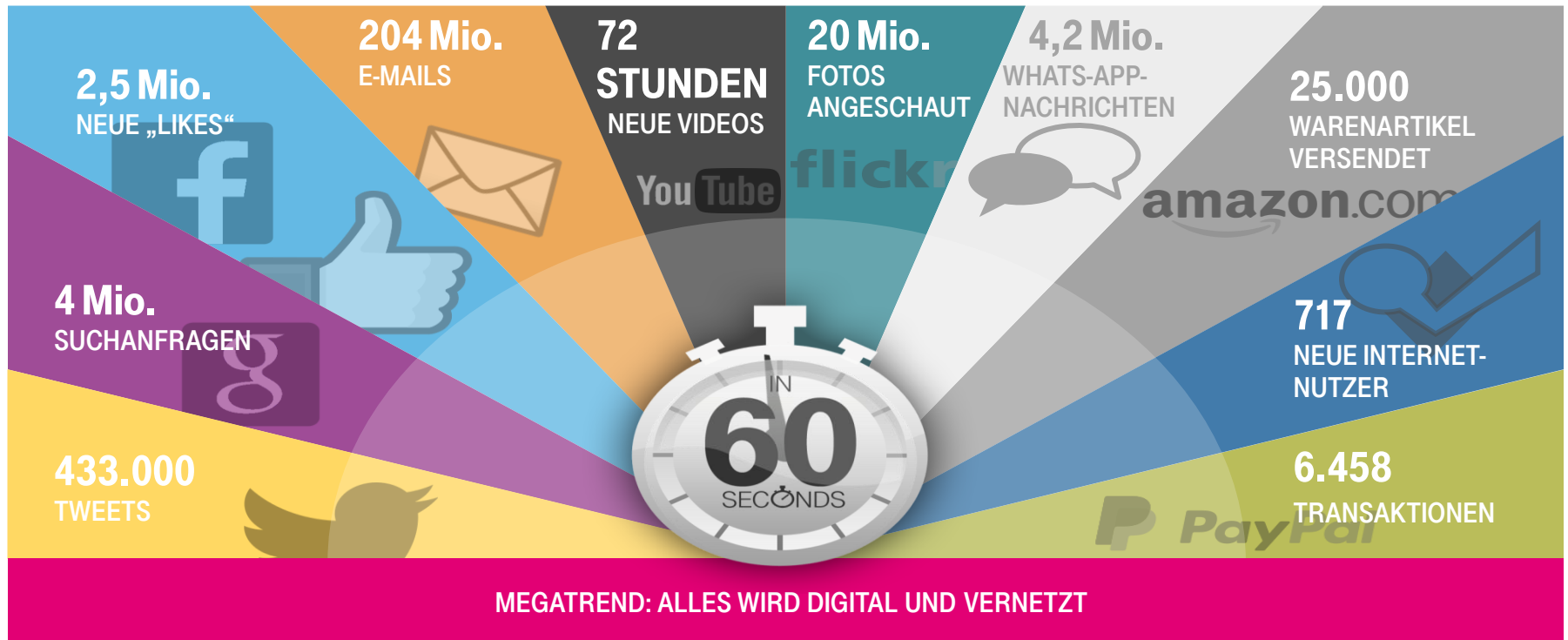
Private Datenwirtschaft und Betroffener wollen Hand in Hand partnerschaftlich und vertrauensvoll zusammen!





DIE REALITÄT HEUTE: DATEN SIND DER NEUE ROHSTOFF FÜR  
UNTERNEHMEN AUF DER GANZEN WELT

# 60 SEKUNDEN IM INTERNET



QUELLE: SocialTimes

<http://pennystocks.la/internet-in-real-time/>

# IN DEUTSCHLAND IST EIN SORGFÄLTIGER UMGANG MIT DATEN KRITISCH FÜR DEN GESCHÄFTSERFOLG

## Ängste, Sorgen von Betroffenen aufgreifen und als Chance erkennen

- Verbraucher / Betroffene in Deutschland weisen ein ausgeprägtes Bewusstsein für das Thema Datenschutz auf
- Datenskandale der Vergangenheit erschütterten das Vertrauen der Verbraucher
- Debatten zu diesen Skandalen trugen sicherlich zu Skepsis und Unsicherheit bei
- Folgerung
  - Zielsetzung: Vertrauen der Verbraucher gewinnen“
  - Dazu Datenschutz als Wettbewerbsvorteil begreifen
  - Hinweise von Betroffenen als Chance zur Verbesserung der eigenen Produkte begreifen:
    - Nur wer besser als die Konkurrenz ist wird mit dem Vertrauen der Verbraucher belohnt
    - Besser wird man nur durch einen Workflow der stetigen Verbesserung
    - Datenschutz muss integraler Bestandteil dieses Workflows sein

# VERTRAUEN & SENSIBILISIERUNG



# DATEN GEGEN MEHRWERT

## Betroffenen partizipieren lassen

- Wenn die Industrie an Daten verdient, muss auch der Betroffene „verdienen“
- Ggfs. Verständnis für den Mehrwert schaffen  
Darstellung der Gewinn-Möglichkeiten für den Betroffenen, z.B.
  - Prämienauszahlung
  - Reduzierung von regelmäßig anfallen Kosten  
(z.B. Versicherungsprämie bei Gesundheitsdaten, Kosten für Fernsehen, Telefon usw. bei Nutzung entsprechender Daten)
  - Upgrade von Leistungen  
(z.B. 1. Klasse Bahn statt 2. Klasse, Lounge für VIP-Kunden bei Kreuzfahrten)
  - Verbesserung von Leistungen  
(z.B. bessere Patientenversorgung durch Forschungsergebnisse, die u.a. durch die Daten des Betroffenen ermöglicht wurden)

# BETROFFENEN ABHOLEN UND MITNEHMEN

## Transparenz in der Verarbeitung

- Betroffene / Patient muss wissen, was mit seinen Daten geschieht
- Umfassende Information über das Produkt
- Aussagen zum Produkt und in die Datenverarbeitung müssen stimmen und vom Betroffenen überprüfbar sein
  - Werbematerialien, Gebrauchsanweisungen dürfen keine unwahren Aussagen beinhalten (Auch „Übertreibungen“ dürfen dem Anwender nie das Gefühl geben, er sei betrogen worden)
  - Die Überprüfbarkeit muss vorhanden sein
    - Nach Möglichkeit: Online-Zugriff des Betroffenen auf seine Daten inklusive Auskunft: wer hat wann auf meine Daten zugegriffen
    - Ggfs. externe Zertifizierungen
    - Ansprechpartner für Betroffene zu Geschäftszeiten (Kann Notfall eintreten: auch außerhalb Geschäftszeiten)



# BETROFFENEN "SELF-SERVICE" ANBIETEN

## Betroffenen als Partner in die Verarbeitung integrieren

- Dem Betroffenen ermöglicht, seine Daten zu sehen und zu verwalten
- Dies heißt auch: dem Betroffenen ermöglichen seine Opt-Ins selbst anzupassen:
  - Welche Werbung möchte ich als Betroffen bekommen?
  - Wem erlaube ich Zugriff auf meine Daten?
  - Welchen Auswertungen stimme ich zu?
- Transparenz bzgl. Datennutzung
  - Betroffener kann sehen, wann welche Daten wozu genutzt wurden
  - Betroffener sieht auch die Gegenleistung, denn...

# GELEBTER DATENSCHUTZ IM UNTERNEHMEN

## Gesetzliche Anforderungen nur Pflicht, nicht Kür

- Die gesetzlichen Anforderungen spiegeln die Mindestanforderungen an den Datenschutz
- Klar: man kann immer mehr tun, als der Gesetzgeber fordert
- Anspruch der Industrie im Gesundheitswesen
  - Bzgl. Datenschutz sind wir Enabler
  - Die Sicherheit von Gesundheitsdaten ist oberstes Ziel nach der bestmöglichen Patientenversorgung
  - Die gesetzlichen Anforderungen für Datenschutz sind für uns eine Selbstverständlichkeit, aber der Patient darf immer mehr erwarten

# AUSWERTUNGEN OHNE PERSONENBEZUG

## Frühzeitige Anonymisierung

- Häufig keine personenbezogenen Daten gebraucht, vielmehr Statistiken wie z.B.

Alter	Bevölkerung	Ischämische Herzkrankheiten		Pneumonie		Bösartige Neubildungen	
		Absolut Erkrankte	Proz. Erkrankte	Absolut Erkrankte	Proz. Erkrankte	Absolut Erkrankte	Proz. Erkrankte
< 10 Jahre	6.924.551	34	0,00%	42.864	0,62%	15.035	0,22%
10 - 20 Jahre	7.987.999	153	0,00%	5.013	0,06%	12.316	0,15%
20 - 40 Jahre	19.678.607	7.074	0,04%	10.799	0,05%	49.815	0,25%
40 - 60 Jahre	25.473.795	149.010	0,58%	33.879	0,13%	358.826	1,41%
60 - 80 Jahre	17.377.567	378.780	2,18%	111.430	0,64%	825.863	4,75%
> 80 Jahre	4.401.224	116.843	2,65%	103.062	2,34%	201.606	4,58%

Quelle: Statistisches Jahrbuch 2013, Statistisches Bundesamt, Wiesbaden, ISBN 978-3-8246-1007-5

# AUSWERTUNGEN MIT BESCHRÄNKTEM PERSONENBEZUG

## Frühzeitige Pseudonymisierung

- Wenn personenbezogene Daten benötigt werden, reichen in der Regel statistische Daten
  - Beispiel Tracking im Supermarkt:
    - Es ist völlig uninteressant, **wer** zum Einkaufen wiederkommt, wichtig ist, **dass** Kunden wiederkommen
    - Daher bei Boniprogrammen die exakte Identifikation der Person zwar nicht nötig, jedoch die Wiedererkennung zwingend notwendig → Pseudonymisierung
  - Beispiel Kundenzufriedenheit
    - Zur Messung der Kundenzufriedenheit benötige ich keine personenbezogenen Daten
    - Um im Einzelfall reagieren und auf Betroffenen zugehen zu können, muss ich diese Person identifizieren können → Pseudonymisierung

# BEISPIEL DATENSCHUTZ IM PRIVATEN UNTERNEHMEN

## DATENSCHUTZ MANAGEMENTPROZESSE BEI DER DEUTSCHEN TELEKOM

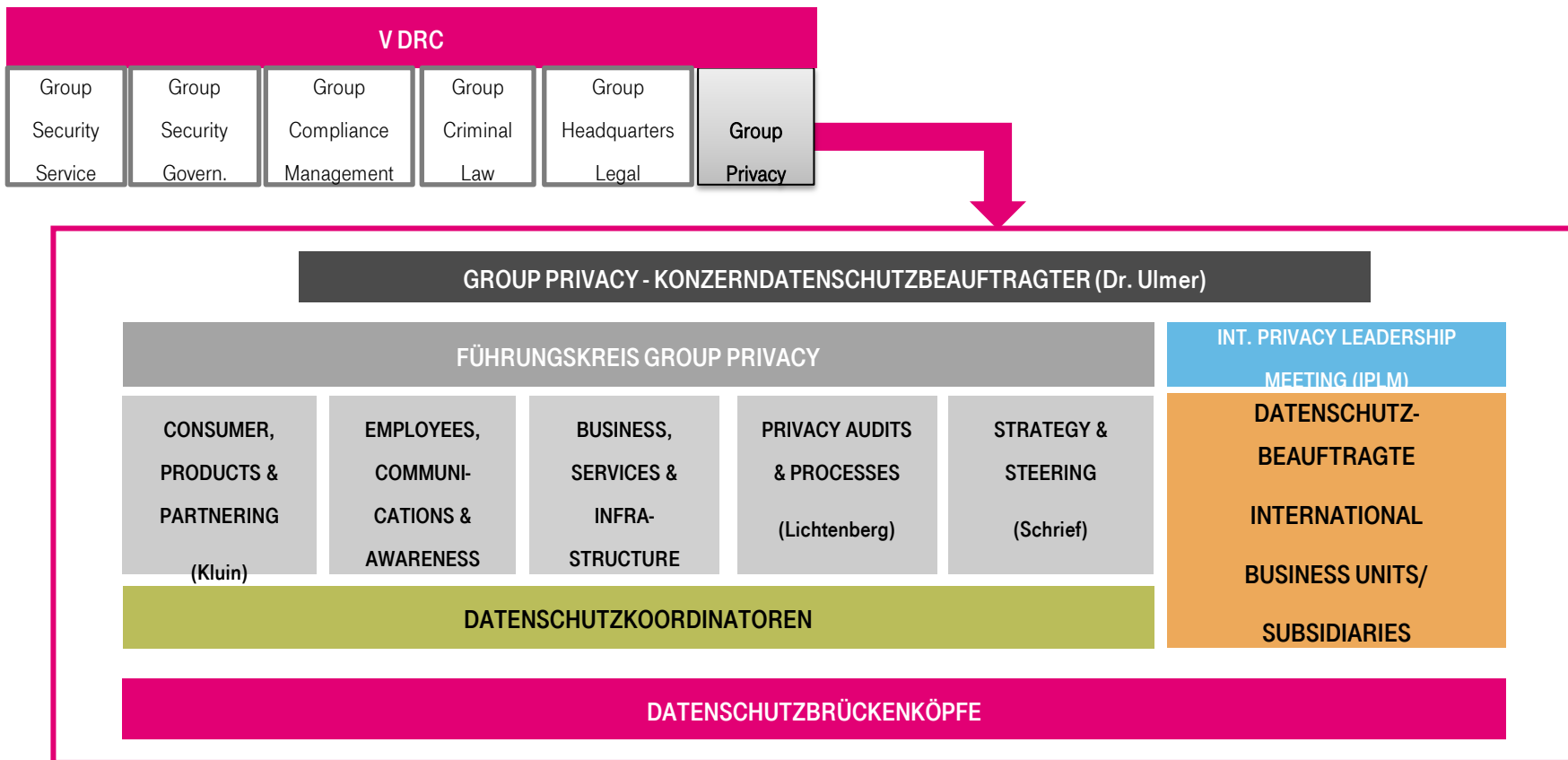


# GELEBTER DATENSCHUTZ IM UNTERNEHMEN

## Privacy Boy Design / Privacy Boy Default

- Privacy Boy Design
  - „Neue“ Anforderung der EU Datenschutz-Grundverordnung, in Industrie schon lange gelebte Praxis
  - Beispiel Telekom:
    - ✓ Datenschutz vor Beginn der Entwicklung in Projekt integriert,
    - ✓ Mittelfreigabe für Projekte erst nach Zustimmung Datenschutz
- Privacy Boy Default
  - Klare Vorgaben, wie Datenschutz im Produkt realisiert wird
  - Beschreibung für den Endanwender:
    - ✓ welche Daten werden warum erhoben und wie werden sie geschützt
  - Beispiel Telekom
    - ✓ Standardisiertes Datenschutz- und Sicherheitskonzept (SDSK):  
was technisch für den Datenschutz machbar ist, wird umgesetzt und geprüft

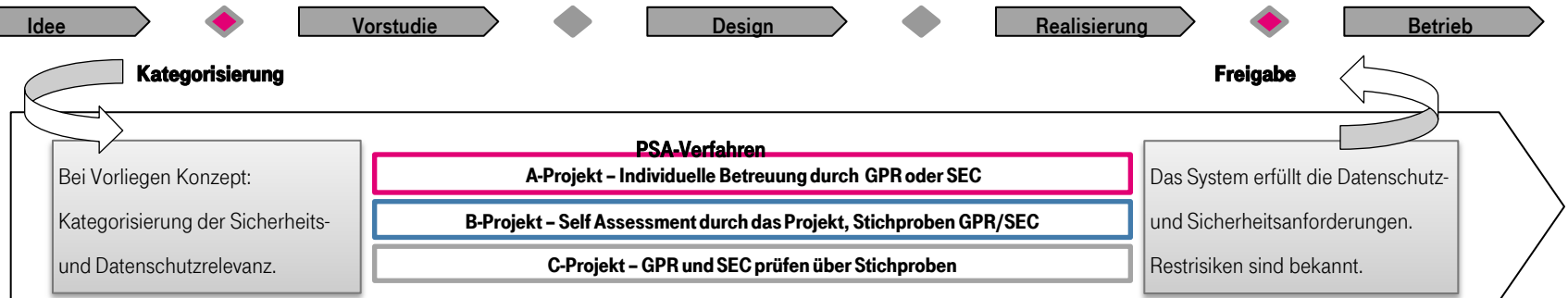
# DIE DATENSCHUTZORGANISATION DER DTAG



# EINBINDUNG DER PRIVACY & SECURITY IM KONZERN NEUENTWICKLUNGEN 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.



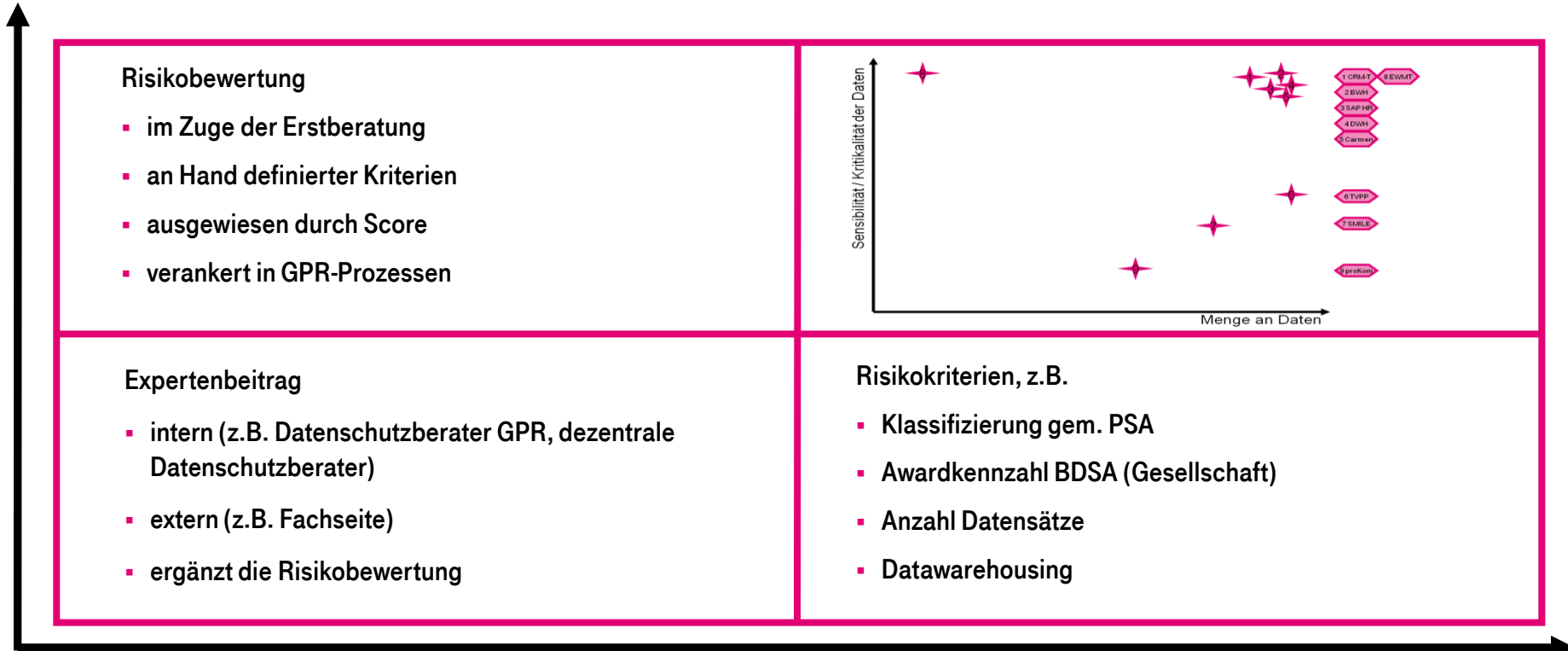
### Ziele

- 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



# RISIKOLANDKARTE DATA PRIVACY INSPECTIONS

## SYSTEMATISCHE DARSTELLUNG



# GROUP PRIVACY AUDITKONZEPT

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	<p>Self Assessment auf Mitarbeiterenebene national sowie international zu</p> <ul style="list-style-type: none"> <li>▪ Denken</li> <li>▪ Wissen</li> <li>▪ Handeln</li> </ul> <p>Zusätzlich international</p> <ul style="list-style-type: none"> <li>▪ Selbstauskunft der Data Privacy Officers (DPO) zur Umsetzung der Vorgaben des Privacy Code of Conduct (PCoC)</li> <li>▪ Verifikation über Stichproben</li> </ul>	<ul style="list-style-type: none"> <li>▪ Auditierung und Bewertung hinsichtlich der Rechtsgrundlagen aus einschlägigen Gesetzen (TKG, TMG, BDSG, PCoC), z.B. Zweckbindung, Datensparsamkeit</li> <li>▪ technische Prüfung auf Basis § 9 BDSG (nebst Anlage) der technischen und organisatorischen Maßnahmen</li> <li>▪ individualisierter Auditscope</li> </ul>	<ul style="list-style-type: none"> <li>▪ Auditierung und Bewertung hinsichtlich der Rechtsgrundlagen aus einschlägigen Gesetzen (TKG, TMG, BDSG, PCoC), z.B. Zweckbindung, Datensparsamkeit</li> <li>▪ technische Prüfung auf Basis § 9 BDSG (nebst Anlage) der technischen und organisatorischen Maßnahmen</li> <li>▪ individualisierter Auditscope</li> </ul>

# DER DATENSCHUTZBEIRAT DER TELEKOM

## ... UND ANDERE VERTRAUENSBLDENE MASSNAHMEN



- 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.
- und weitere Transparenzmaßnahmen:
  - **sicherdigital.de**
  - **Datenschutz und Datensicherheitsbericht**
  - **telekom.com/datenschutz**

# ÜBERPRÜFUNG VON DELOITTE NACH IDW PS 980: INSTITUT DER WIRTSCHAFTSPRÜFER PRÜFSTANDARD 980

## COMPLIANCE MANAGEMENT SYSTEM: PRÜFSTUFEN

Konzeption & Dokumentation

Angemessenheit &  
Implementierung

Wirksamkeitsprüfung

1. Stufe

Sind die Grundsätze und  
Maßnahmen des CMS\*  
zutreffend beschrieben?

2. Stufe

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

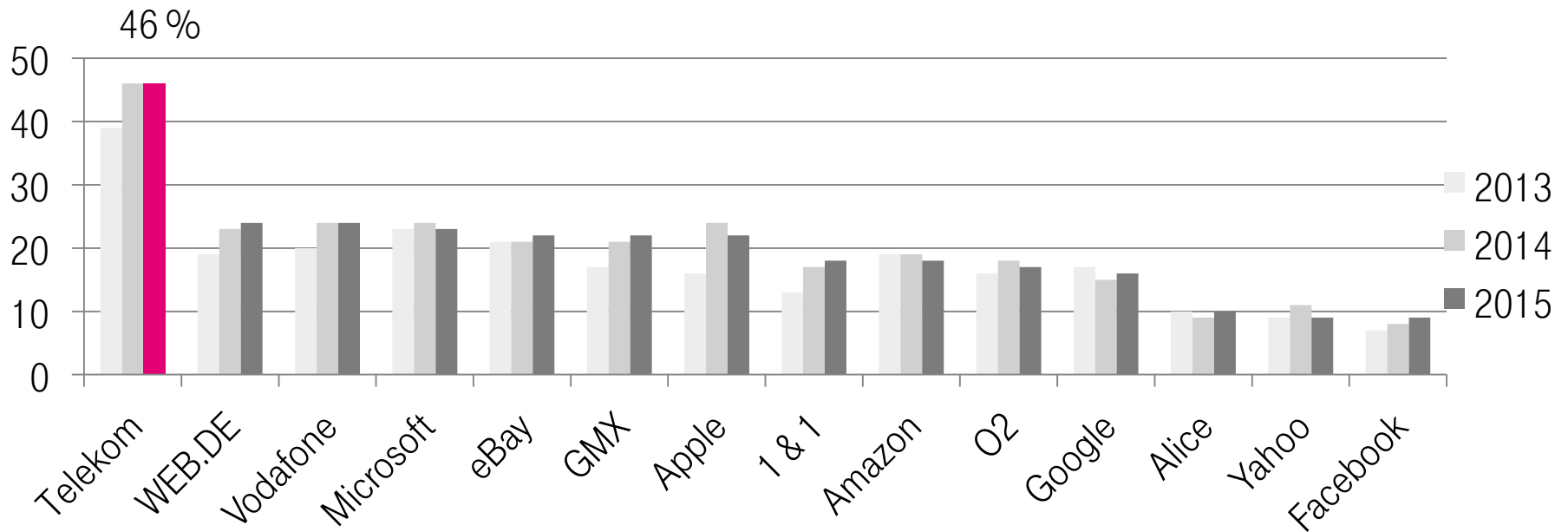
3. Stufe

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

\*Compliance Management System

# TELEKOM ALS VERTRAUENSWÜRDIGES UNTERNEHMEN

FRAGE: „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: Security Report INSTITUT FÜR DEMOSKOPIE ALLENSBACH, Juni 2015

**Vielen Dank für Ihre Aufmerksamkeit!**

[www.telekom.com/datenschutz](http://www.telekom.com/datenschutz)



**HEALTHCARE SOLUTIONS**