IT-Sicherheitsrechtstag 2019

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Berlin, 14.11.2019

"Data Protection by Design / by Default"

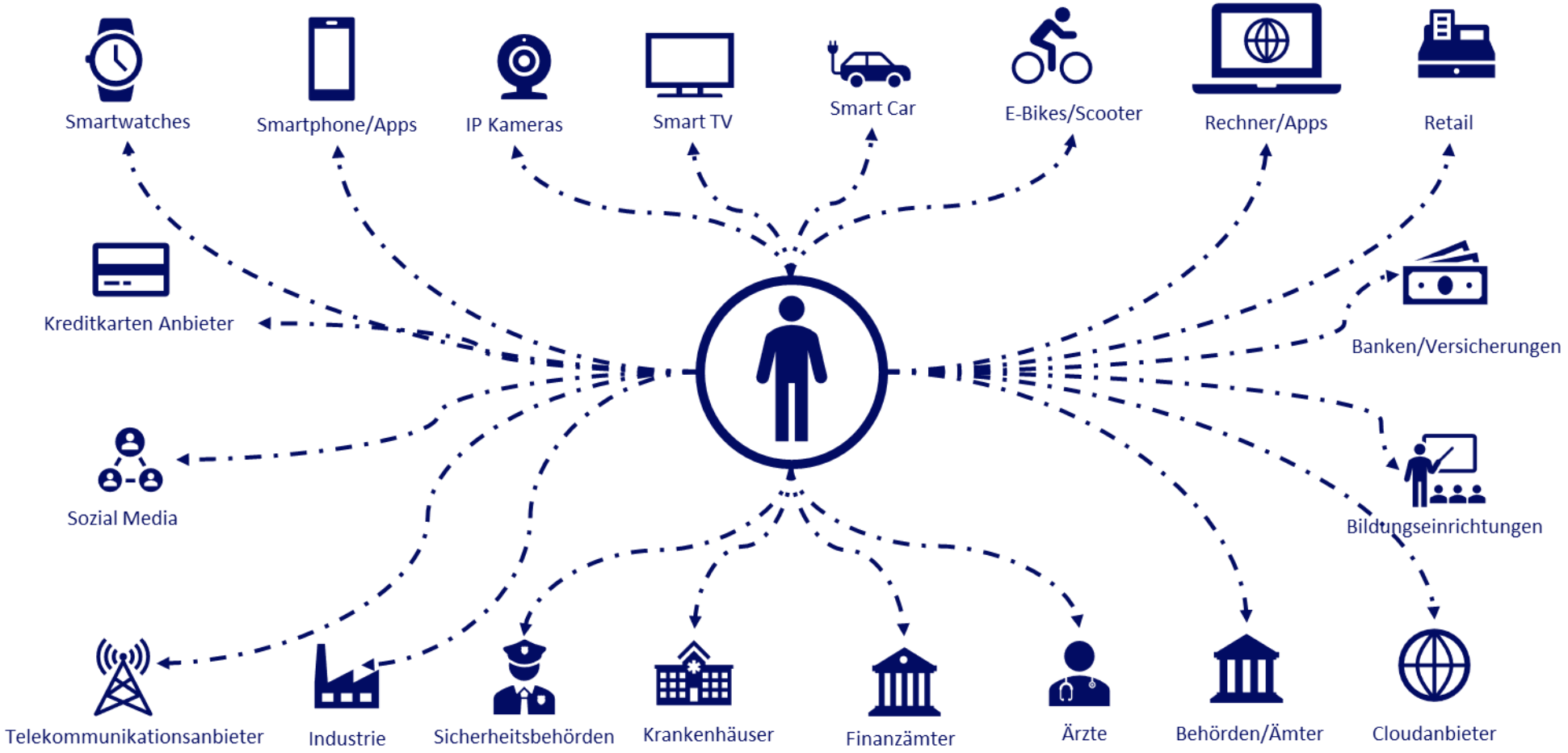
Rolf Blunk, Otaris

"Data Protection by Design / by Default"

- Definition und Bedeutung
- Voraussetzungen und Abhängigkeiten
- Anforderungen
- Best Practise Lösungen/Projekterfahrungen
- Fazit und Ausblick

"Data Protection by Design / by Default" - Worum geht es?
Mögliches Gesamt-Szenario:

Umgang mit personenbezogenen Daten durch verschiedenste Instanzen



Beispiele für den Umgang mit Daten im gesamten Lebenszyklus (von A – Z)

Quelle: Merentis DataSec GmbH

Jede Verwendung personenbezogener Daten, z.B. zur Korrespondenz mit dem Betroffenen, Duplizieren, Kopieren, Auswertungen, zur Information des Betroffenen über das Vorhandensein der Daten

Definition und Bedeutung

- Privacy by Design (= Privatsphäre durch Gestaltung)
- Privacy by Default

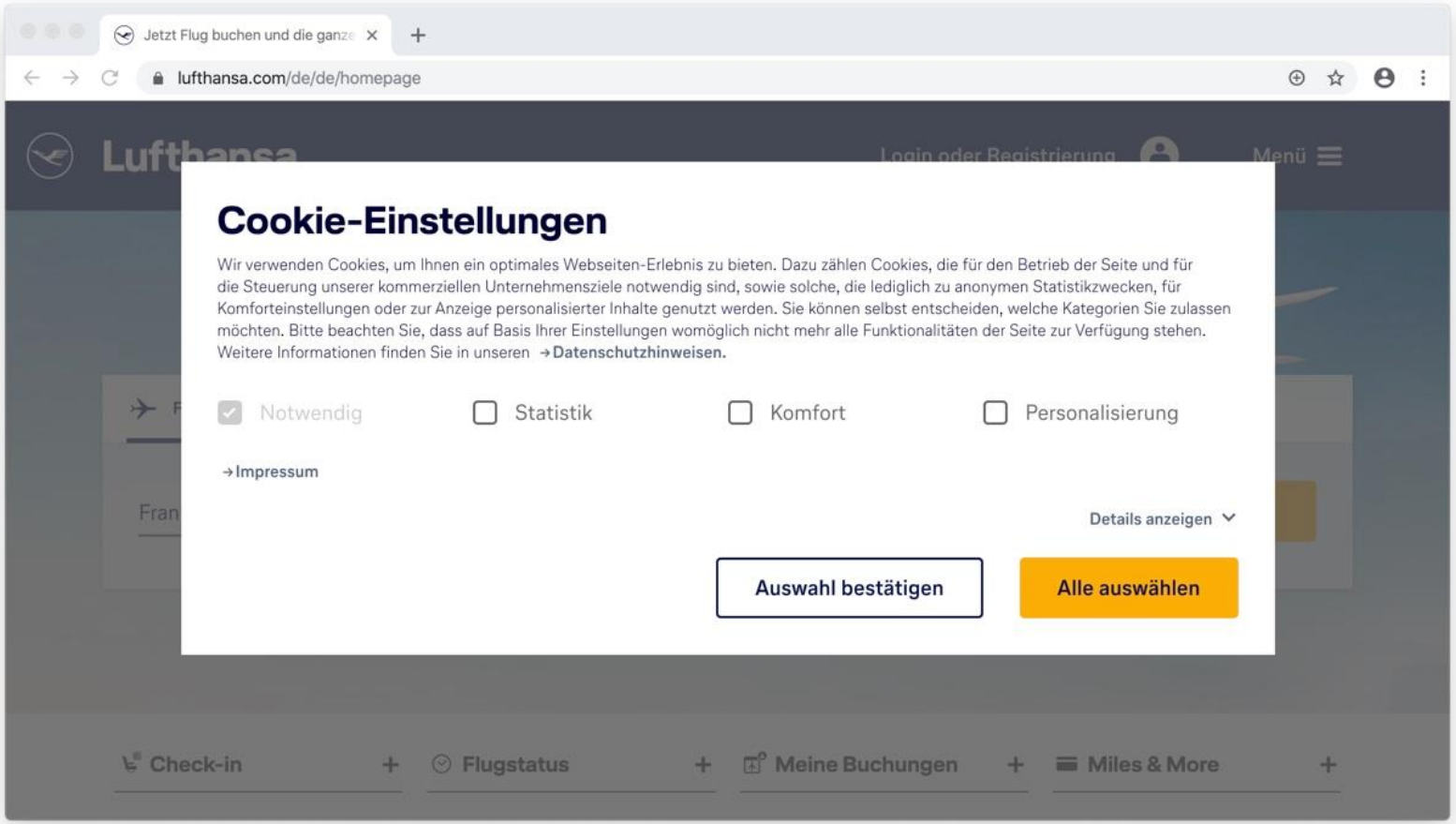
Ziel: Gestaltung von Systemen + Diensten
von Anfang an über den gesamten Lebenszyklus
a) datenminimierend
b) mit möglichst datenschutzfreundlichen Voreinstellungen

Quelle: Marit Hansen (ULD)

Beispiel zu "Privacy by Default"
Setzen von Cookies erfordert eine aktive Einwilligung des Internetnutzers

EuGH Urteils vom 01.10.2019 (Rechtssache: C-637/17; Bundesverband der Verbraucher-zentralen vs. Planet 49 GmbH)

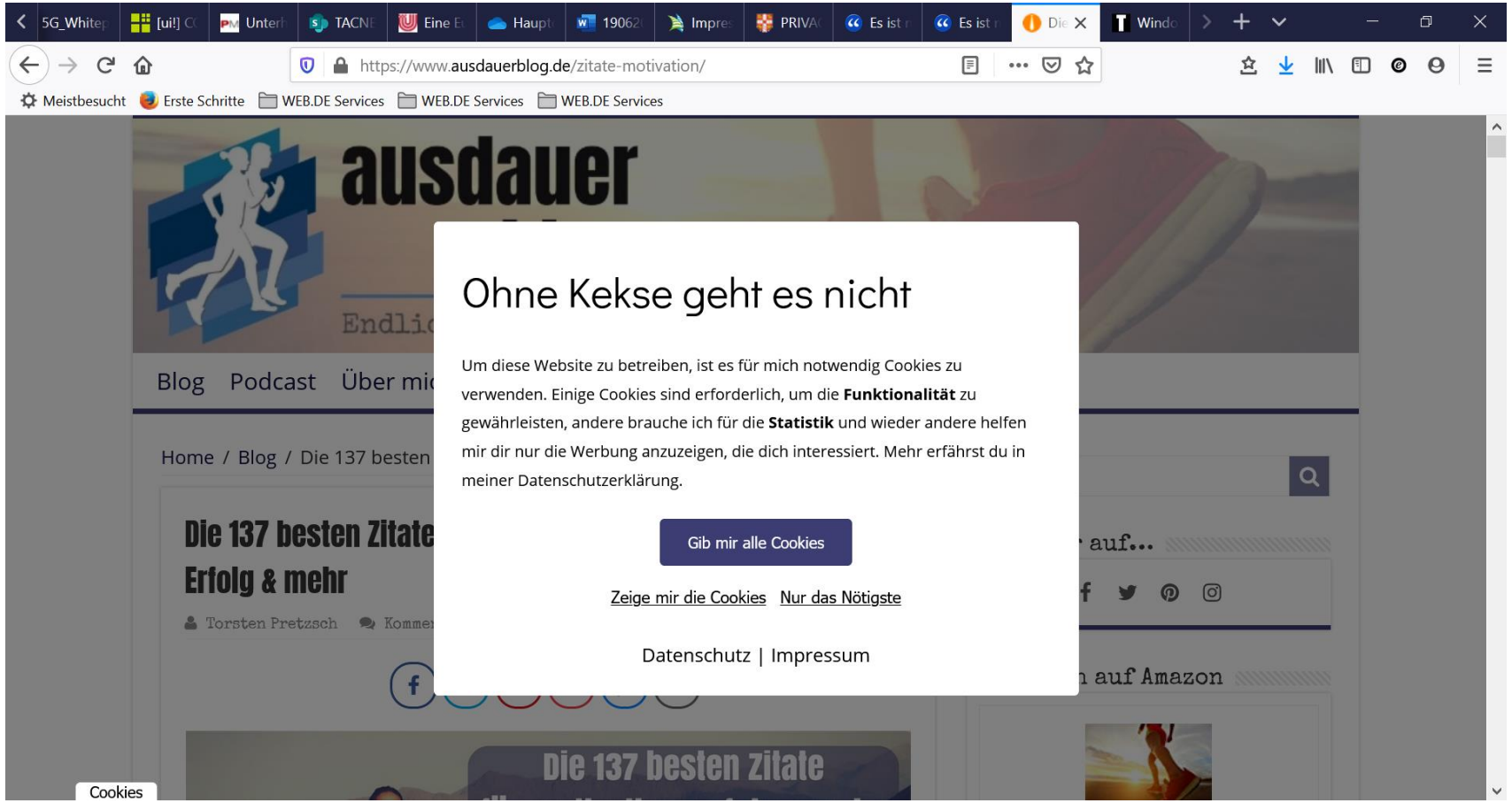
Ein voreingestelltes Ankreuzkästchen genügt nicht



Beispiel zu "Privacy by Default"
Setzen von Cookies erfordert eine aktive Einwilligung des Internetnutzers

EuGH Urteils vom 01.10.2019 (Rechtssache: C-637/17 ;Bundesverband der Verbraucherzentrale vs. Planet49 GmbH)

Ein voreingestelltes Ankreuzkästchen genügt nicht



Definition und Bedeutung

- Privacy by Design
- Privacy by Default

Artikel 25 […] durch datenschutzfreundliche Voreinstellungen

(2) Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit.

Quelle: Marit Hansen (ULD)

Definition und Bedeutung

- Privacy by Design
- Privacy by Default

Artikel 25 […] durch datenschutzfreundliche Voreinstellungen
(2) ff …Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

Quelle: Marit Hansen (ULD)

Voraussetzungen und Abhängigkeiten

Zwei Seiten einer Medaille:

Datenschutz by Design/Default

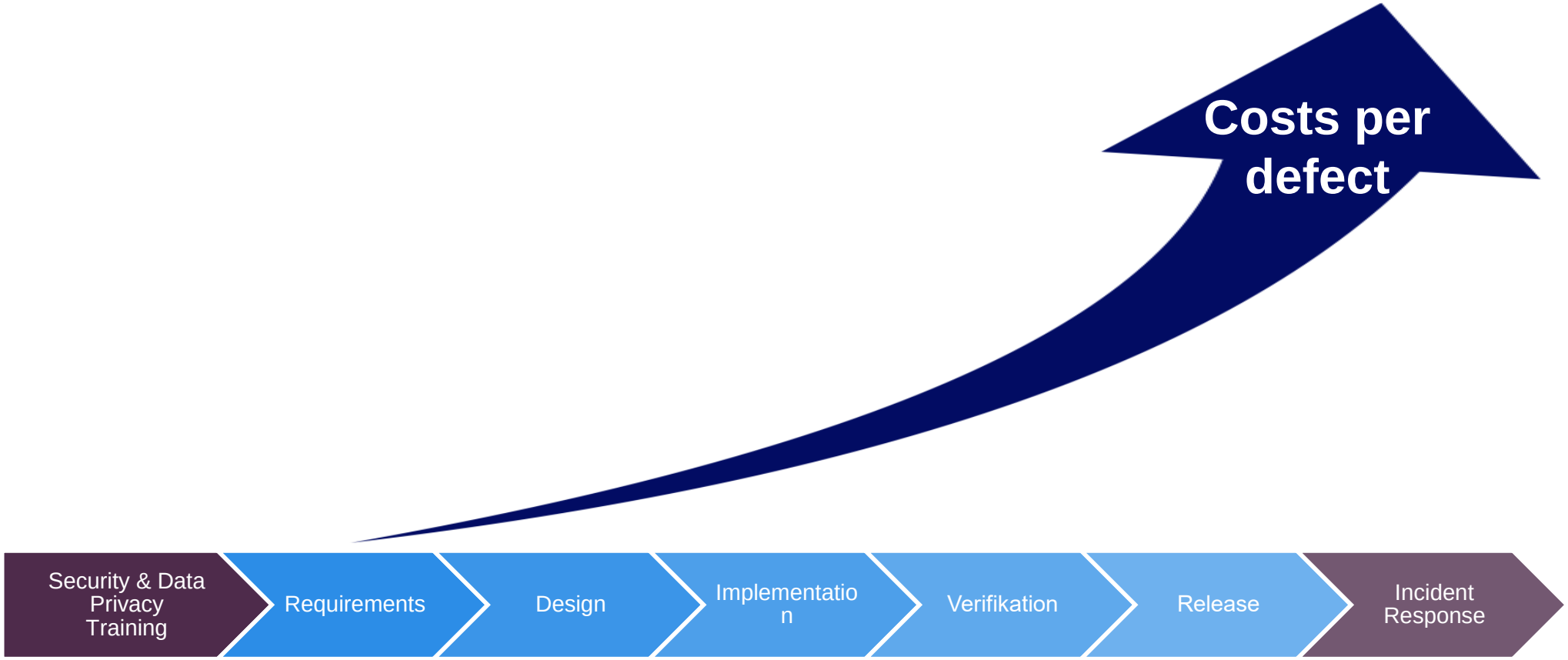
IT-Sicherheit by Design

"Datenschutz by Design"
= Datenschutz durch technische IT-Sicherheit

(entscheidender Erfolgsfaktor:

Vertrauensvolle interdisziplinäre Zusammenarbeit zwischen allen relevanten Stakeholdern von A – Z!)

Security & Privacy by Design



Secure Development LifeCycle (SDL)

Datenschutz Anforderungen

Grundlagen des Datenschutzes

Worum geht es?
Welche **Anforderungen** sind zu erfüllen?

Grundlagen des Datenschutzes

Jeder Mensch soll grundsätzlich **selbst** über die Preisgabe und Verwendung seiner persönlichen Daten **bestimmen.**

Volkszählungsurteil, 1983

Datenschutz ist ein Grundrechtsschutz

In der EU

•Art. 8 der EU-Grundrechtecharta: "Schutz personenbezogener Daten"

In Deutschland

•Recht auf informationelle Selbstbestimmung

Grundlagen des Datenschutzes

DER UMGANG MIT PERSONENBEZOGENEN DATEN WIRD DURCH DAS DATENSCHUTZRECHT GEREGELT

- Es kommt zur Anwendung, wenn Sie Daten bearbeiten, die **einem Menschen zugeordnet** (natürliche Person) werden können.

- Daten von **juristischen Personen**, wie Vereinen, Verbänden, AGs, GmbHs etc. sind durch das Datenschutzrecht nicht geschützt.

Grundlagen des Datenschutzes

DAS DATENSCHUTZRECHT verbietet grundsätzlich den Umgang mit personenbezogenen Daten, erlaubt diese aber unter bestimmten Voraussetzungen (**Verbot mit Erlaubnisvorbehalt**).

- **DATENUMGANG ist nur zulässig, wenn er ... durch das Datenschutzrecht selbst ...**
  Beispiel: Zur Durchführung eines Vertrages
- **oder durch eine besondere Rechtsvorschrift ...**
  Beispiel: Steuern, Abgaben
  ... erlaubt und dem Betroffenen transparent gemacht wird.
- **oder durch die Einwilligung des Betroffenen ...**
- Beispiel: Einverständniserklärung zur Datennutzung

Personenbezogene Daten

Was ist damit gemeint?

Personenbezogene Daten

PERSONENBEZOGENE DATEN sind alle Angaben, die sich auf eine identifizierte oder aber auch nur identifizierbare Person beziehen.

Beispiele

ADRESSE	VERMÖGEN	ARBEITSVERHALTEN	BENUTZERKENNUNG
GEBURTSDATUM	BESITZ	PERSONALNUMMER	MASCHINENBEZOGENE
TELEFONNUMMER	GEHALT	ARBEITSERGEBNISSE	NUTZUNGSZEITEN
	FOTO		

Quelle: Merentis DataSec GmbH

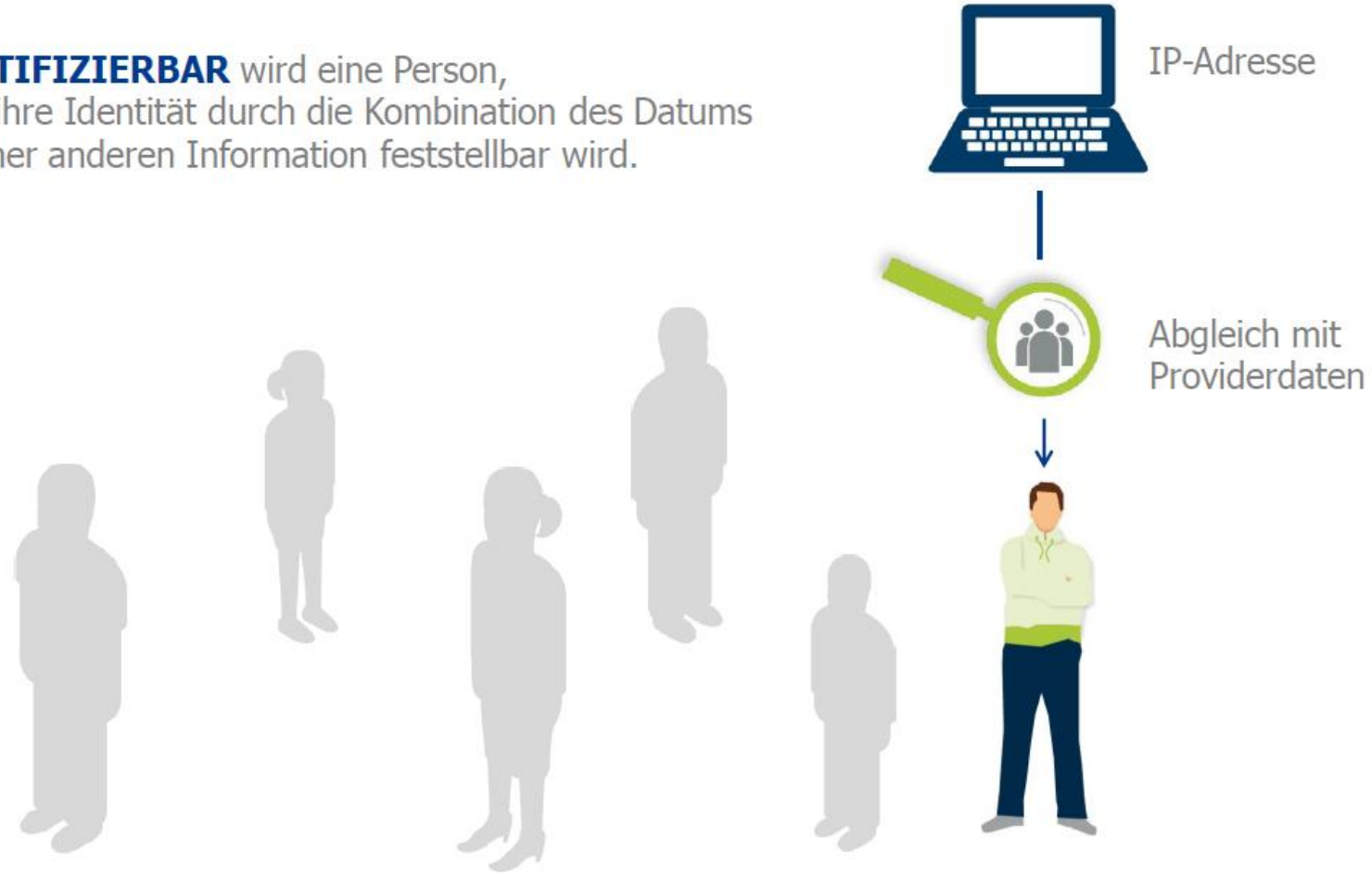
Personenbezogene Daten

IDENTIFIZIERT ist eine Person, wenn sich ihre Identität direkt aus dem Datum selbst ergibt.

Quelle: Merentis DataSec GmbH

Personenbezogene Daten

IDENTIFIZIERBAR wird eine Person,
wenn ihre Identität durch die Kombination des Datums
mit einer anderen Information feststellbar wird.



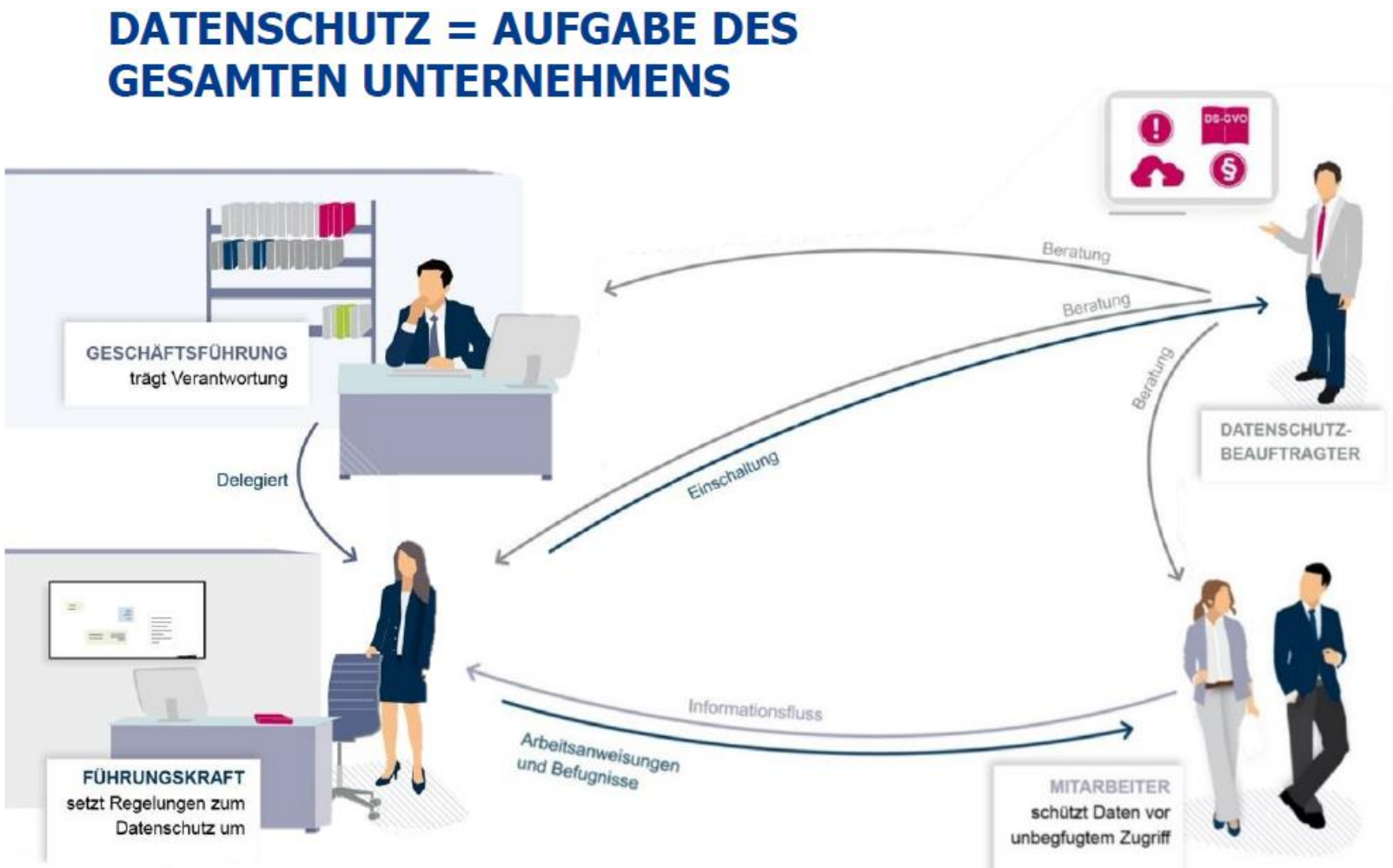
Quelle: Merentis DataSec GmbH

Personenbezogene Daten

Weitaus strengere Regeln gibt es für den Umgang mit sogenannten **besonderen Kategorien personenbezogener Daten,** da diese besonders schützenswert sind.

Quelle: Merentis DataSec GmbH

Pflichten



Quelle: Merentis DataSec GmbH

Technisch-Organisatorische Maßnahmen (TOMs)

- Technisch-Organisatorische Maßnahmen haben das Ziel, den Schutz der Verarbeitung zu garantieren und damit den Rechten der Betroffenen Person zu dienen
- Sie werden vom Verantwortlichen implementiert und sind regelmäßig nach ihrem Schutzniveau zu beurteilen
- Technische Maßnahmen sind beispielsweise die Pseudonymisierung von Daten, ein ausdifferenziertes Berechtigungskonzept oder auch die getrennte Speicherung von Daten, welche zu unterschiedlichen Zwecken erhoben werden
- Organisatorische Maßnahmen sind dagegen eher physischer Natur, wie Alarmanlagen, die Gliederung in verschiedene Sicherheitszonen oder Transponder Schließsysteme

Anforderungen an die Sicherheit (nach Art. 32 DSGVO)

Sicherstellung der Integrität der Systeme und Dienste

- Weitergabekontrolle (verschlüsselte Übertragung, VPNs, elektronische Signatur…);
- Eingabekontrolle (Protokollierung von Systemaktivitäten, Dokumentenmanagement…);
- Zugriffskontrolle (Berechtigungskonzepte, Protokollierung von Zugriffen…);

Verfügbarkeit und Belastbarkeit der Systeme und Dienste

- Verfügbarkeitskontrolle (Backup-Strategie, USV, Virenschutz, Firewall, Notfallpläne…);
- Maßnahmen zur Gewährleistung der raschen Wiederherstellbarkeit der Verfügbarkeit der personenbezogenen Daten und des Zugangs zu ihnen bei einem physischen oder technischen Zwischenfall

Quelle: Merentis DataSec GmbH

Rechte des Betroffenen

TRANSPARENZPFLICHTEN DES UNTERNEHMENS

INFORMATIONSPFLICHTEN
Bereits bei der Datenerhebung muss das Unternehmen die betroffene Person über die Verarbeitung und alle ihre Rechte Informieren.

BENACHRICHTIGUNG
Bei Datenanforderung über die betroffene Person durch Dritte.

AUSKUNFT
Verpflichtung zur Auskunft über die gespeicherten Daten, deren Herkunft und Empfänger.

Quelle: Merentis DataSec GmbH

Rechte des Betroffenen

Inhalt insbesondere:

- Daten/-kategorien
- Zwecke und Rechtsgrundlage
- Berechtigte Interessen im Falle einer Interessenabwägung
- Empfänger, falls Daten übermittelt werden
- Übermittlung in Drittländer
- Dauer der Speicherung
- Betroffenenrechte
- Kontaktdaten

Beachten Sie, wenn Betroffene ihre Rechte geltend machen:

- Nehmen Sie den Wunsch auf.
- Versuchen Sie zu ergründen, was der Betroffene tatsächlich möchte.
- Geben Sie den Wunsch unverzüglich an die betrieblich zur Bearbeitung vorgesehenen Stellen weiter.

Quelle: Merentis DataSec GmbH

Rechte des Betroffenen

Quelle: Merentis DataSec GmbH

Sanktionen

SANKTIONEN

Womit müssen Sie rechnen, wenn Sie gegen Vorgaben des Datenschutzes verstoßen?

Quelle: Merentis DataSec GmbH

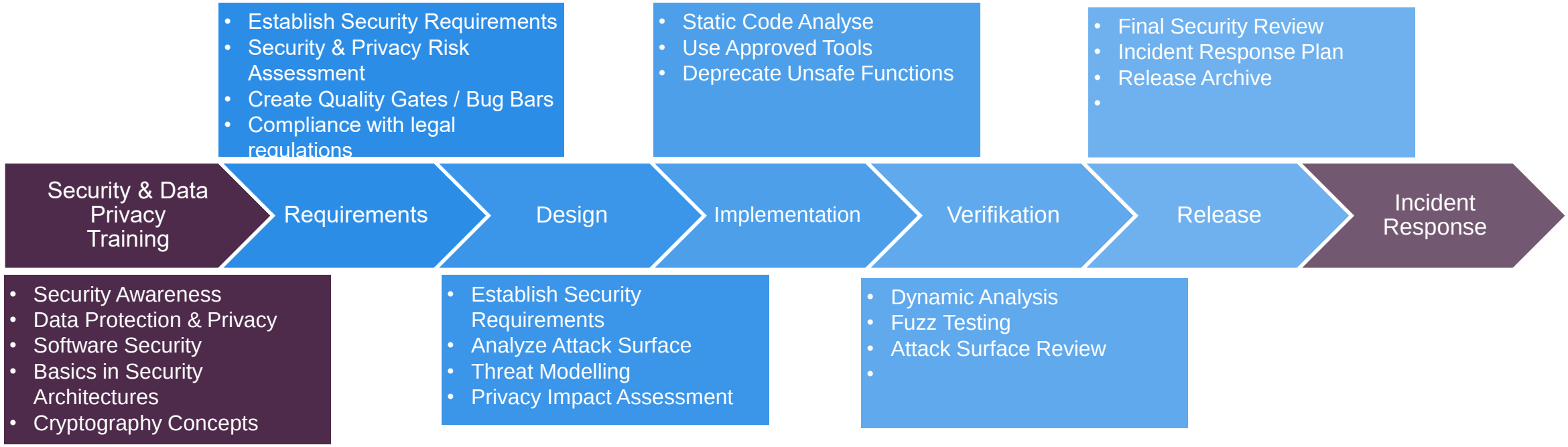
Sanktionen

Quelle: Merentis DataSec GmbH

"Sicherheit von Anfang bis Ende" – erfolgreich zukünftig nur noch mit "Security und Privacy by Design" (Projekterfahrungen – mit 5G)

- Ob bei der **Entwicklung neuer Hardware- und Software-Komponenten** oder bei der **Planung und Etablierung zukünftiger Unternehmensprozesse oder Dienstleistungen für die Kunden –** mit der sich rasant entwickelnden Digitalisierung und exponentiell zunehmenden Vernetzung zwischen Menschen und Maschinen müssen alle erfolgreichen Anbieter am Markt **adäquate Sicherheit über den gesamten Lebenszyklus gewährleisten**!
- **Wichtigste Voraussetzungen** hierfür sind **Engagement und Leadership im Management** ("Sicherheit ist Chefsache") sowie Sensibilisierung und Kompetenzaufbau bei allen Mitarbeitern (nicht nur in der IT) und vertrauensvolle Zusammenarbeit aller beteiligten Mitarbeiter und Partner (relevante Stakeholder)
- **Von Anfang an** müssen zu den geplanten Funktionen, Komponenten und Datenflüssen **mögliche Bedrohungen und Schutzbedarfe (inkl. Privacy) identifiziert und bewertet werden**. **Angemessene Sicherheitsanforderungen und Lösungen** sind in allen weiteren Lebensphasen kontinuierlich weiter zu überprüfen und zu optimieren

Security Development LifeCycle / Anwendungserfahrungen in Projekten



- Microsoft SDL conforms to ISO/IEC 27034-1:2011 (Application Security)
- General Data Protection Regulation (GDPR)

Der Datenschutzbeauftragte…

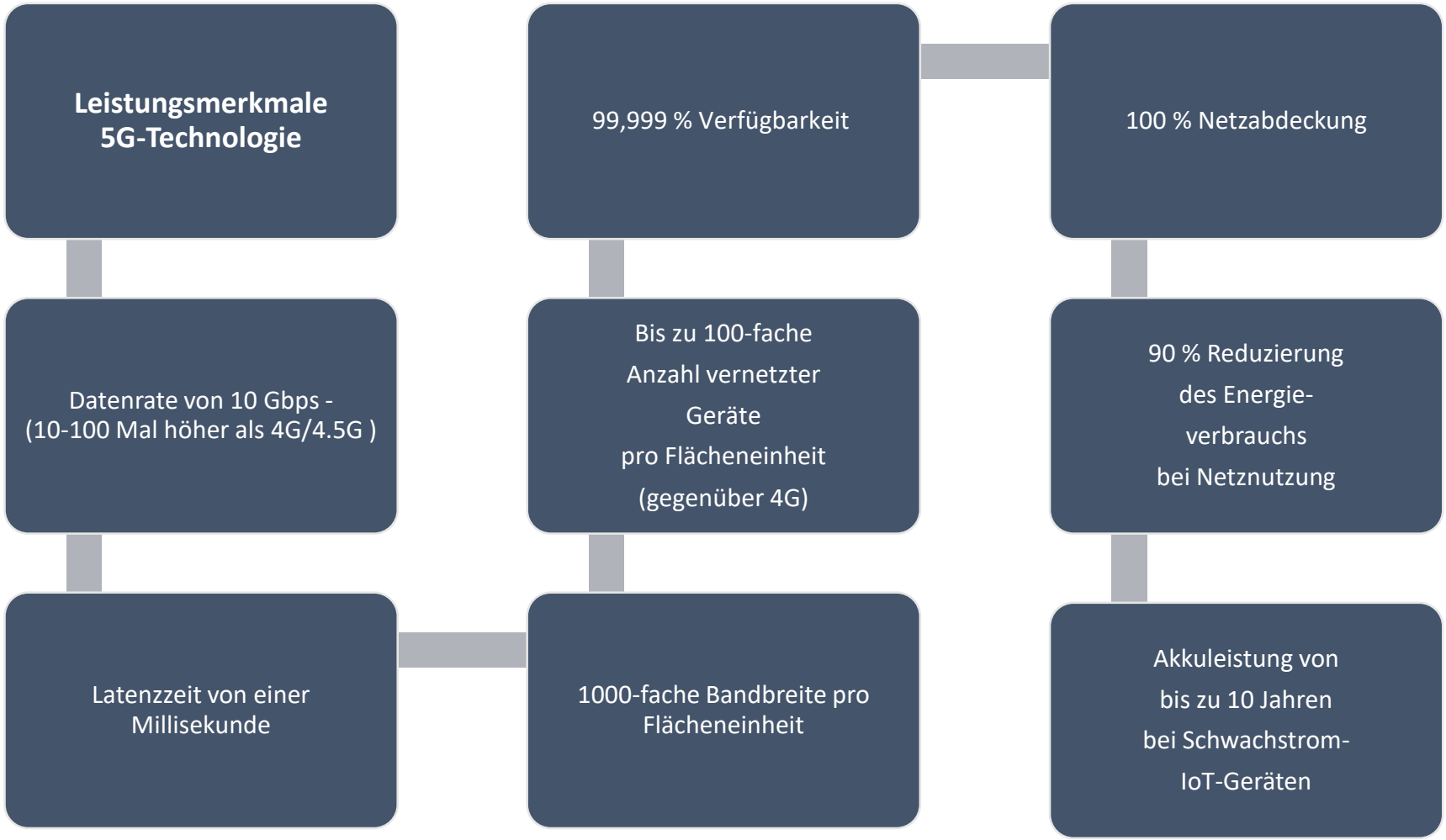
- überwacht die Einhaltung des Datenschutzrechts
- berät und unterrichtet Geschäftsführung und Mitarbeiter bei Fragen, die den Datenschutz betreffen
- unterliegt der Verschwiegenheitspflicht
- hat das Recht, sich in Zweifelsfällen an die Aufsichtsbehörde zu wenden

"Sicherheit von Anfang bis Ende" – erfolgreich zukünftig nur noch mit "Security und Privacy by Design" (5G Projekterfahrungen)

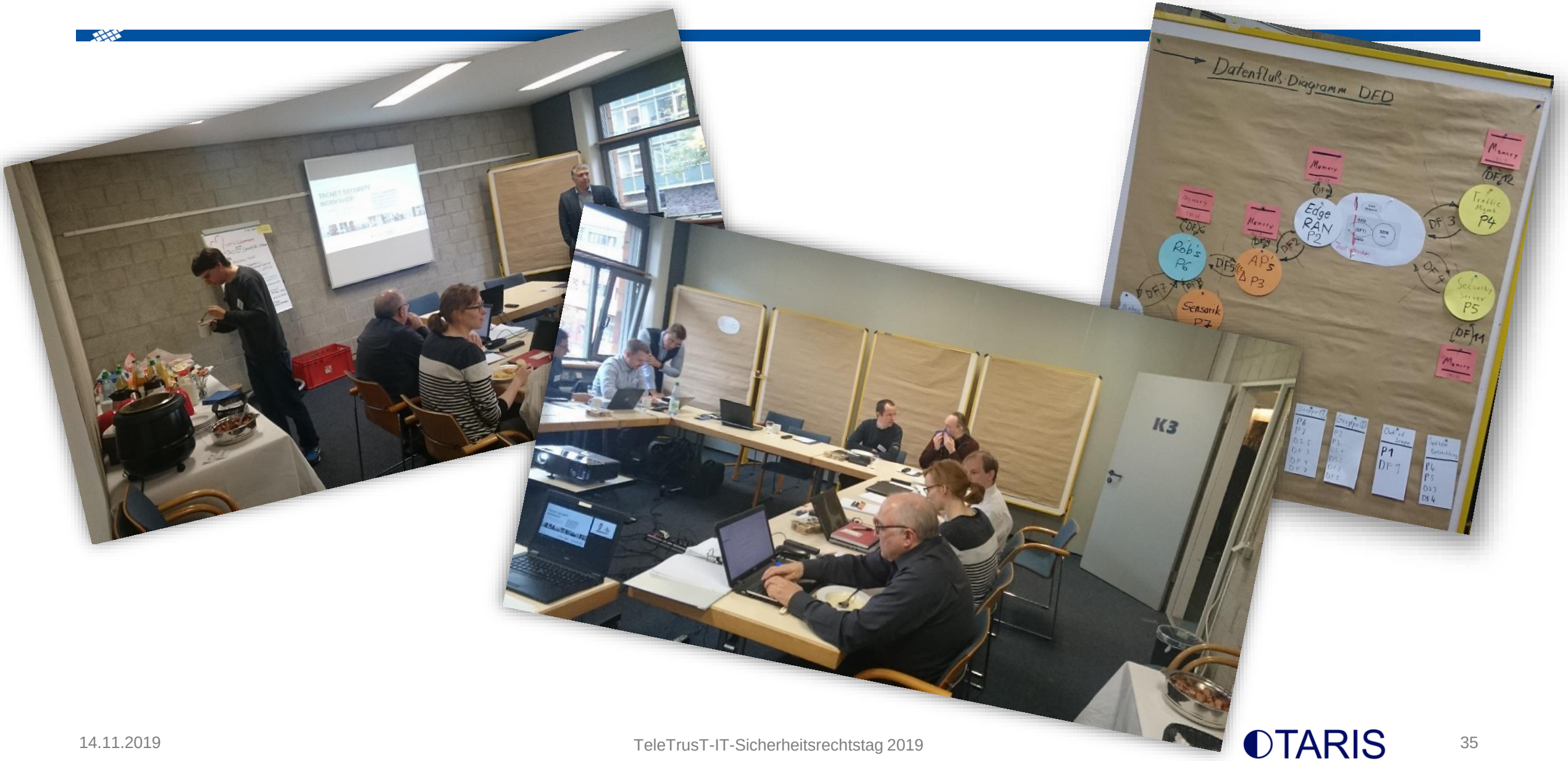
- Die bisherigen Erfahrungen und Erkenntnisse aus Standardisierungs-Prozessen und Forschungsprojekten im Umfeld von 5G- (5. Generation Funktechnologien) und vergleichbaren Zukunftstechnologien sowie den damit verbundenen Industrie 4.0 / IoT-(Internet of Things) Möglichkeiten der nächsten Jahre machen deutlich:

- **Gegenwärtig übliche IT-Security-Standard-Konzepte in Unternehmen reichen keinesfalls aus, um etwa den nachfolgend beispielhaft aufgeführten 5G-Leistungsmerkmalen als Treiber für eine neue Generation von Anforderungen an Security- und Privacy-Management und Produktiv-Betrieb im internationalen Wettbewerb gerecht zu werden!**

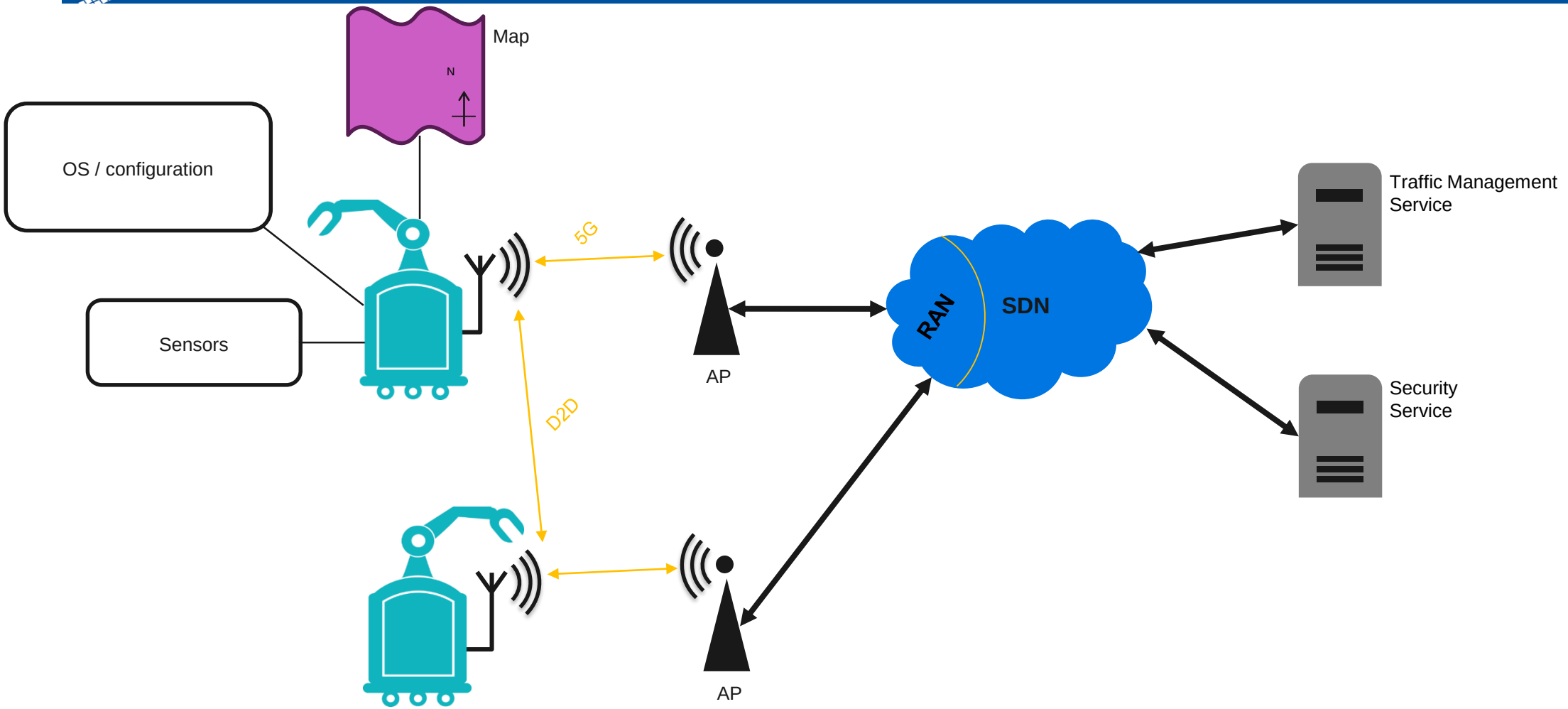
5G-Leistungsmerkmale als Treiber für eine neue Generation von Anforderungen an Security- und Privacy-Management und Produktiv-Betrieb



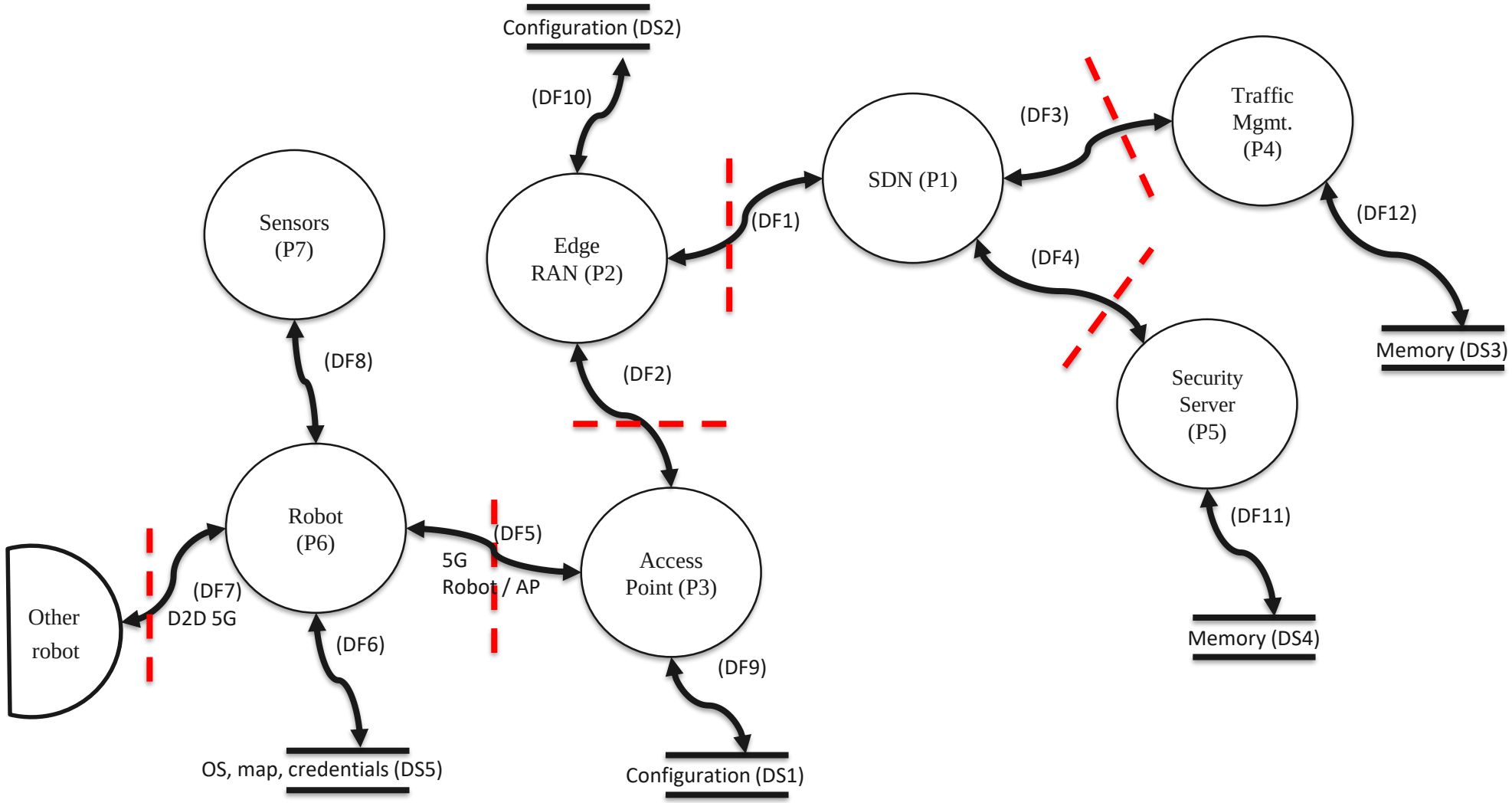
THREAT Modeling Workshop Impressions – 5G-Use Cases



Identifizierung der "schützenswerten" Assets und Daten in Roboter-unterstützten Fertigungsprozessen und Systemen mit 5G



Data Flow Diagram (DFD) - in Roboter-unterstützten Fertigungsprozessen und Systemen mit 5G



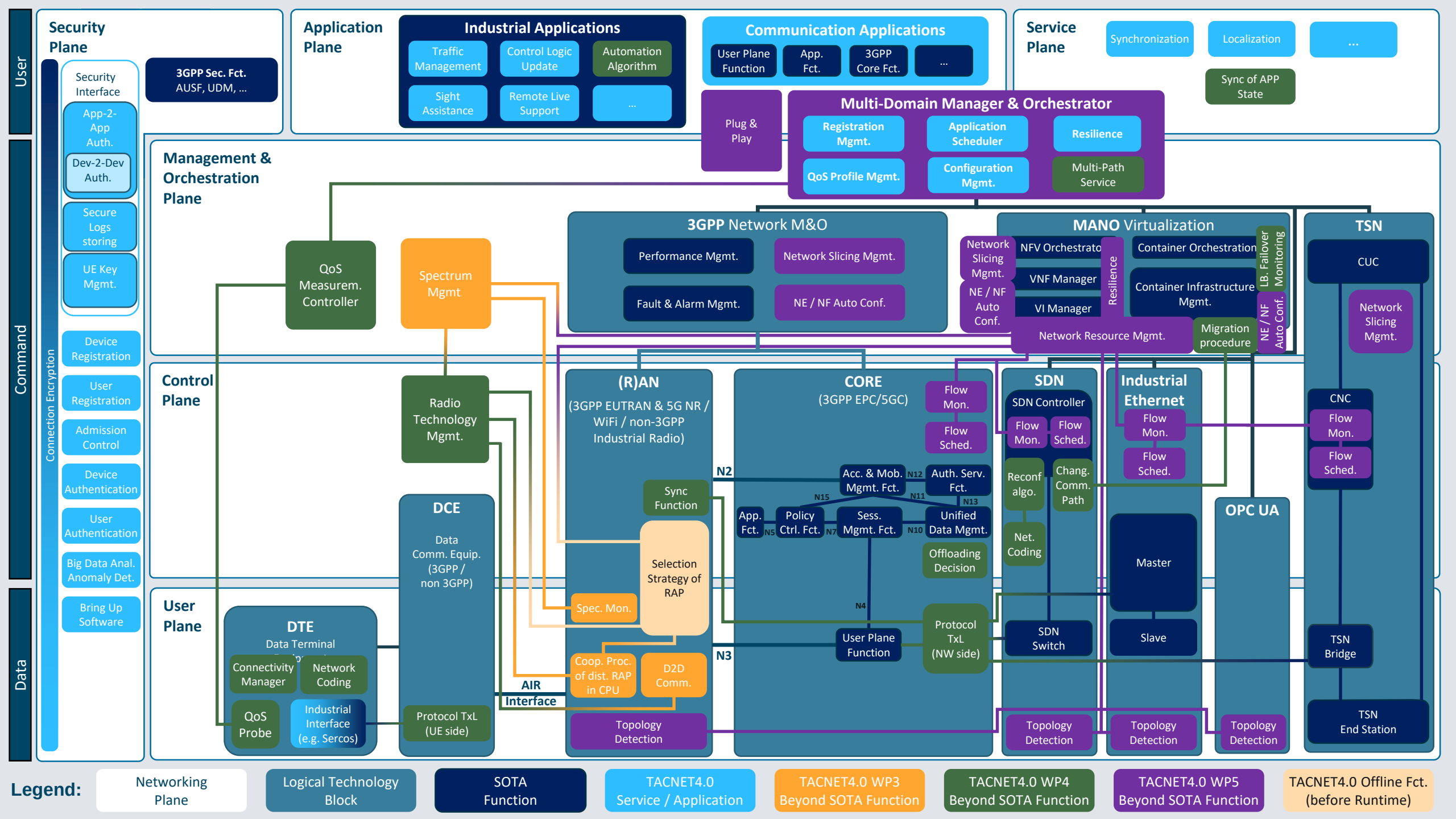
Architekturelle Risikoanalyse von Software und IT-Systemen

Microsoft **STRIDE** Methode zur Klassifizierung von Bedrohungen

Threats / Bedrohung	Protection Goals / Schutzziele	Example/Beispiel
Spoofing Identity *Identitätsfälschung*	Authenticity *Authentizität*	An attacker fakes a false identity. *Ein Angreifer täuscht eine falsche Identität vor*
Tampering with Data *Manipulation von Daten*	Integrity *Integrität*	An attacker manipulates data. *Ein Angreifer manipuliert Daten*
Repudiation *Abstreiten von Handlungen*	Non-repudiability *Nichtabstreitbarkeit / Verbindlichkeit*	An attacker performs an action and the victim can not prove it to him *Ein Angreifer führt eine Aktion durch, und das Opfer kann es ihm nicht beweisen*
Information Disclosure *Offenlegung*	Confidentiality *Vertraulichkeit*	An attacker sees data that he should not see. *Ein Angreifer sieht Daten, die er nicht sehen soll*
Denial of Service *Serviceverweigerung*	Availability *Verfügbarkeit*	An attacker interferes with the availability of an application *Ein Angreifer stört die Verfügbarkeit einer Anwendung*
Elevation of Privilege *Erhöhung der Zugriffsrechte*	Authorization *Autorisierung*	An attacker finds a way to increase his privileges *Ein Angreifer findet einen Weg seine Berechtigungen zu erhöhen*

Quelle: Microsoft (MSDN)

Overall Architecture 5G Project


User
Command
Data
Security Plane
Security Interface
App-2-App Auth.
Dev-2-Dev Auth.
Secure Logs storing
UE Key Mgmt.
3GPP Sec. Fct.
AUSF, UDM, ...
Application Plane
Industrial Applications
Traffic Management
Control Logic Update
Automation Algorithm
Sight Assistance
Remote Live Support
...
Communication Applications
User Plane Function
App. Fct.
3GPP Core Fct.
...
Service Plane
Synchronization
Localization
...
Sync of APP State
Plug & Play
Multi-Domain Manager & Orchestrator
Registration Mgmt.
Application Scheduler
Resilience
QoS Profile Mgmt.
Configuration Mgmt.
Multi-Path Service
Management & Orchestration Plane
QoS Measurem. Controller
Spectrum Mgmt
3GPP Network M&O
Performance Mgmt.
Network Slicing Mgmt.
Fault & Alarm Mgmt.
NE / NF Auto Conf.
MANO Virtualization
Network Slicing Mgmt.
NFV Orchestrator
VNF Manager
VI Manager
NE / NF Auto Conf.
Resilience
Container Orchestration
Container Infrastructure Mgmt.
LB. Failover Monitoring
NE / NF Auto Conf.
Network Resource Mgmt.
Migration procedure
TSN
CUC
Network Slicing Mgmt.
Control Plane
Radio Technology Mgmt.
(R)AN
(3GPP EUTRAN & 5G NR / WiFi / non-3GPP Industrial Radio)
CORE
(3GPP EPC/5GC)
Flow Mon.
Flow Sched.
Acc. & Mob. Mgmt. Fct.
Auth. Serv. Fct.
App. Fct.
Policy Ctrl. Fct.
Sess. Mgmt. Fct.
Unified Data Mgmt.
Offloading Decision
N2
N3
N4
N5
N7
N10
N11
N12
N13
N15
Sync Function
Selection Strategy of RAP
SDN
SDN Controller
Flow Mon.
Flow Sched.
Reconf algo.
Chang. Comm. Path
Net. Coding
SDN Switch
Industrial Ethernet
Flow Mon.
Flow Sched.
Master
Slave
OPC UA
CNC
Flow Mon.
Flow Sched.
TSN Bridge
TSN End Station
User Plane
DTE
Data Terminal
Connectivity Manager
Network Coding
QoS Probe
Industrial Interface (e.g. Sercos)
DCE
Data Comm. Equip. (3GPP / non 3GPP)
Protocol TxL (UE side)
AIR Interface
Spec. Mon.
Coop. Proc. of dist. RAP in CPU
D2D Comm.
Topology Detection
User Plane Function
Protocol TxL (NW side)
Topology Detection
Topology Detection
Topology Detection
Connection Encryption
Device Registration
User Registration
Admission Control
Device Authentication
User Authentication
Big Data Anal. Anomaly Det.
Bring Up Software
Legend:
Networking Plane
Logical Technology Block
SOTA Function
TACNET4.0 Service / Application
TACNET4.0 WP3 Beyond SOTA Function
TACNET4.0 WP4 Beyond SOTA Function
TACNET4.0 WP5 Beyond SOTA Function
TACNET4.0 Offline Fct. (before Runtime)

"Fazit" – Ausblick – aktuelle Tätigkeitsschwerpunkte

- IT-Sicherheit by Design wird in den letzten 2 – 3 Jahren zunehmend und systematisch angewandt – vorwiegend in der Software-Entwicklung!
- "Datenschutz by Design" erfolgt während der frühen Design-Phasen bestenfalls sporadisch; Ermittlung und Vorgabe konkreter und spezifischer DSGVO Anforderungen zu Beginn des Lebenszyklus sind eher die Ausnahme – ebenso die Einbeziehung der Datenschutz-Stakeholder!!!

Ausblick - Aktuelle Maßnahmen und Aktivitäten:

- Austausch und gemeinsame Weiterentwicklung/Integration der Datenschutz Aspekte in angewandten IT-Sicherheit by Design Prozessen u.a. mit SAP
- Kompetenzaufbau / Trainings zu Datenschutz-Anforderungen und Datenschutz by Design Methodiken in allen laufenden Beratungsprojekten;
- TeleTrusT Handreichung V1.0 zu Security/Privacy by Design" in Q1 2020;

"Privacy by Design / by Default" – Alltags-Erkenntnis:

Es ist nicht genug zu wissen, man muß es auch anwenden; es ist nicht genug zu wollen, man muß es auch tun.

Wilhelm Meisters Wanderjahre III, aus Makariens Archiv

Vielen Dank für Ihre Aufmerksamkeit

Quelle: Johann Wolfgang von Goethe
deutscher Dichter
* 28.08.1749, † 22.03.1832

Kontakt

OTARIS Interactive Services GmbH

Fahrenheitstraße 7

28359 Bremen

Tel +49 421 685 111 00

Fax +49 421 685 111 99

Rolf Blunk

blunk@otaris.de