Datenschutz im Betrieb regeln
14. Jänner 2020

Technikgestaltung und Datenschutz

Thomas Riesenecker-Caba

Forschungs- und Beratungsstelle Arbeitswelt (FORBA)

Datenschutz – Datensicherheit – Informations-schutz

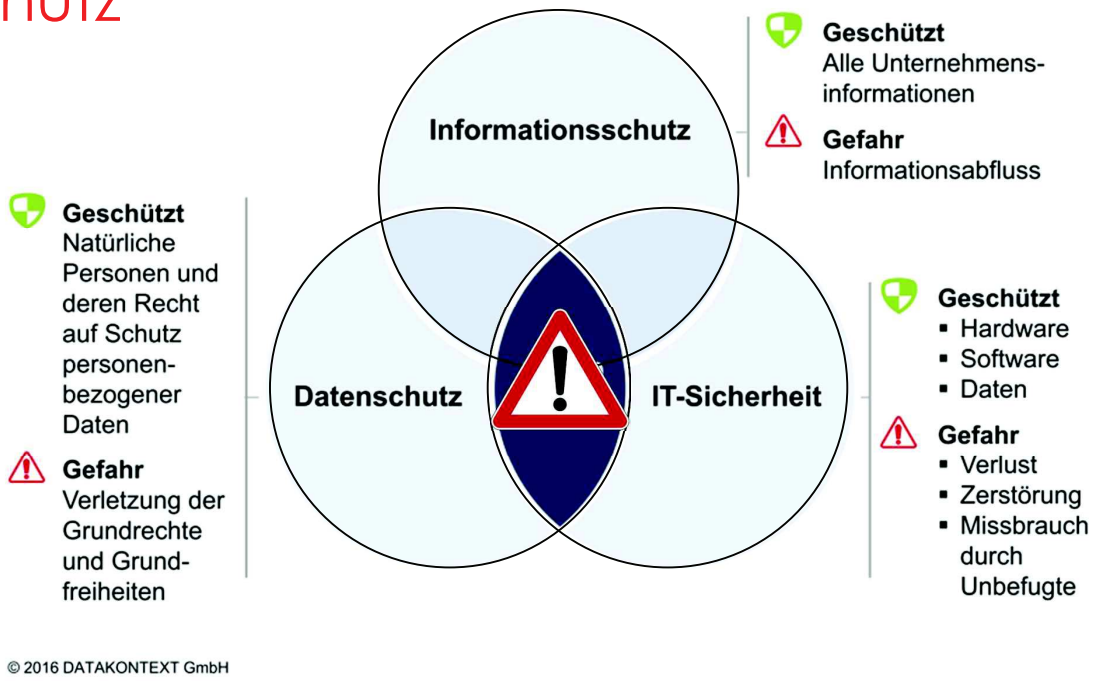


Abbildung aus: Gola et. al (2017): Datenschutz-Grundverordnung im Überblick, DATAKONTEXT (adaptiert)

Neue Herausforderungen an Datenschutz (1/2)

- Durchdringung aller betrieblichen Bereiche mit Informationstechnik und dadurch vermehrte Speicherung personenbezogener MitarbeiterInnendaten.
- Lokale und globale Zusammenführung von personenbezogenen MitarbeiterInnendaten aus unterschiedlichen Systemen.
- Daten mobiler Services (mobiler Endgeräte) werden in betriebliche Systeme und Prozesse integriert -> App Industrie.

Neue Herausforderungen an Datenschutz (2/2)

- Auslagerung von Diensten (z.B. externes Rechenzentrum, Cloud Computing, virtuelle Arbeitsplätze).
- Servicegedanken steht bei IKT-Einsatz im Vordergrund, immer neuere Produkte (Namen):
  z.B. RFID-Multifunktionskarten, M2M (automatisierter Informationsaustausch zwischen Endgeräten), Internet der Dinge , Big Data, Wearables (SmartWatch)
- Social Web liefert Software für Unternehmen (workplace by Facebook, Yammer, MS Teams, SAP JAM, Skype for Business)

➔ ES WIRD KOMPLEXER!!

RFID = radio-frequency identification / **M2M** = Machine to Machine – Kommunikation

Vernetzung 4.0

- Internet(technologie) brachte überbetriebliche Vernetzung („Cloud“)
- Big Data (neue Formen der Analyse strukturierter und NICHT strukturierter Daten, wie Mail, Dokumente, Bilder, Sprache)
- Vernetzung aller betrieblichen Ebenen (IT/OT*) und Dinge (IoT), Sensoren, Aktuatoren**, Standards wie RAMI4.0
- Künstliche Intelligenz (KI/AI) wird „wiederbelebt“ - kognitive Systeme
- Lernende Maschinen ohne menschlichen Programmier-aufwand

* OT = Operational Technology/Betriebstechnologie
**Aktuatoren setzen elektrische Signale in mechanische Bewegung oder andere physikalische Größen um

… führt zu

- Digitalisierung der Gesellschaft
- (vernetzte) Informations- und Kommunikationstechnik in allen Lebens- und Arbeitsbereichen, Integration alter und neuer Systeme (es wird *smart*)
- „dank“ Internet jederzeitige Verfügbarkeit von Information („dezentrale Zustandsüberwachung“)
- Schaffung automatisierter Marktplätze / Optimierung der Wertschöpfungsketten / neue Geschäftsmodelle
- technikgesteuertes Arbeiten: Crowd-/Micro-Work und Arbeiten 4.0 vs. Robotic Process Automation (RPA)

Internet der Dinge nur mit IPv6

IPv4 aufgrund Gestaltung Adressformat mit 2^{32} => ca. 4,3 Milliarden Adressen

IPv6 aufgrund Änderung Adressformat nun 2^{128} => ca. 340 Sextillionen Adressen

4.300.000.000

340.000.000.000.000.000.000.000.000.000.000.000

	Internet Protocol version 4 (IPv4)	Internet Protocol version 6 (IPv6)
Deployed	1981	1999
Address Size	32-bit number	128-bit number
Address Format	Dotted Decimal Notation: 192.149.252.76	Hexadecimal Notation: 3FFE:F200:0234:AB00:0123:4567:8901:ABCD
Prefix Notation	192.149.0.0/24	3FFE:F200:0234::/48
Number of Addresses	2^{32} = ~4,294,967,296	2^{128} = ~340,282,366,920,938,463,463,374,607,431,768,211,456

Quelle: www.linkedin.com

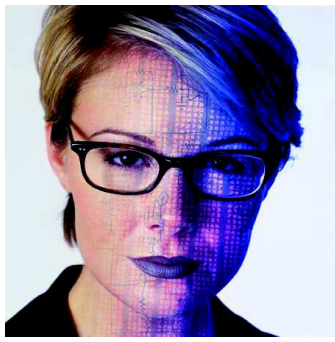
Was sind personenbezogene Daten ?

Personenbezogenen Daten (Art. 4 DS-GVO)

alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen

als identifizierbar wird eine Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen bestimmt werden kann, die Ausdruck ihrer physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind

Arten personenbezogener Daten



- Zeichen (Eingabe von Buchstaben und Ziffern in bestehende Datenmasken – z.B. Name, SV-Nummer, Kostenstelle)
- Bilder (Videoerfassung, Screen-Shot des Bildschirms, Einträge in sozialen Netzwerken [z.B. Profilbild])
- Texte (Bewerbungsschreiben, elektronischer Personalakt)
- Zeitpunkte (An-/Abmeldung PC, Signale Microsoft 365, Statusmeldung Skype for Business oder WhatsApp, Bedienen Kopierer oder Laborgeräte)
- Geodaten (GPS Daten von smarten Endgeräten, Fahrzeugen)
- Sprache (Voice-Recording, VoIP [Voice over Internet Protocol] - Datenpaket)
- Muster (Barcode, Fingerprint, Handvenenscan)

Empfehlung Datenschutzkommission
(jetzt Datenschutzbehörde)

Wenn zu einer Gruppen mehr als fünf Personen zu zählen sind, gewährleistet dies, dass ein Rückschluss auf bestimmte Arbeitnehmer/innen nicht möglich ist.

http://tinyurl.com/K213-180 und http://tinyurl.com/DSB-D215-611

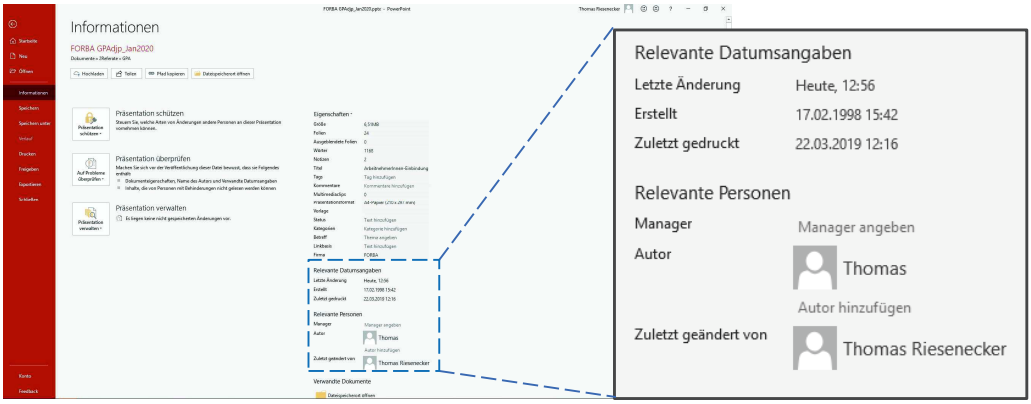
-> bei online-Befragung/Fragebögen, Auswertungen zu Team, … von Bedeutung

Personenbezogene Daten werden vor allem in drei großen Bereichen verwendet, aber …

1. Technische Systeme im Bereich der **Personalverwaltung** (Teil von ERP-Systemen): zur Entgeltberechnung oder zur Zeitwirtschaft. Wird immer mehr zu (globalen) HCM-Systemen ausgebaut. Integration von Daten zur Weiterbildung (e-learning), BewerberInnenverwaltung, digitale Personalakte
2. Systeme zur **Leistungserfassung und -kontrolle** (Verhaltenskontrolle): vom betrieblichen Controlling, der Produktionsplanung und –steuerung sowie Qualitätssicherung in hoch technisierten Produktionsstraßen („MES“ Manufacturing Execution System), zur Bewältigung von KundInnen-anfragen in Call-Center bis hin zur Videoüberwachung.
3. **Kommunikations-/Kollaborationssysteme**: Telefon (Nebenstellenanlagen, VoIP, CTI [Computer Telephony Integration]), Handy oder E-Mail.

aber …
nicht zu vergessen

4. **Verwaltungssoftware**: Ticket-Systeme/Fernwartung, MDM (Mobile Device Management), Verwaltung und Steuerung von Druck-, Kopier- und Scanvorgänge (follow me)
5. **Embedded Systems** (eingebettete Systeme), **M2M**, **Internet der Dinge**
6. **Metadaten**:



Überblick Systeme

* **Personalverwaltung**: Personalverrechnung, Zeitwirtschaft, Personalentwicklung (MitarbeiterInnen-Gespräche, Self-assessment), e-Learning, digitaler Personalakt	* **ERP-Systeme** (abseits HCM/HR): Enterprise Resource Planning (Finanzwesen, Lagerverwaltung, Einkauf, Vertrieb, …)
* **Kommunikationssysteme**: Telefon (Festnetz, VoIP), mobile Kommunikation (inkl. Apps), E-Mail, Internet, Intranet	* **Kollaborationssysteme**: soziale Medien (Workplace von Facebook, MS Teams, Yammer, Skype for Business, SAP JAM), Messenger
* **Verwaltungssoftware**: Multifunktions-Chip, MDM (Mobile Device Management), Multifunktionsgeräte, HelpDesk, BenutzerInnenverwaltung (AD = Active Directory)	* **Branchenspezifische Lösungen**: Produktion (MES: MDE, BDE, …), Call Center, Außendienst (Flottenmanagement, GPS), Ausgabeautomaten
* **Kontrollsysteme**: Zutritt, Video	* **Datenbank-Lösungen**: Business Intelligence, Data Warehouse, Big Data (SAP HANA)
* **IT-Sicherheit**: Firewall, SIEM (Security Information and Event Management), UBA/UEBA (User and Entity Behavior Analytics), ISMS (Information Security Management System)	* **embedded systems** (eingebettete Systeme): M2M (machine to machine), Borddaten (in Fahrzeugen)
* **Cloud Anwendungen**: Microsoft 365 (Office 365, EMS, Windows 10), z.B. mit Sharepoint	* **Hinweisgebersystem (whistle blowing)**
* **online-Befragungstools**	* ***MitarbeiterIn in anderer Rolle*** : als **KundIn** in betriebsinternem CRM oder Kunden-/Klientenverwaltung, vor Eintritt in das Unternehmen als **BewerberIn**

© FORBA 08/2019

Was tun?

- Iststand (möglichen Sollstand) hinterfragen -> Infopflicht nach § 91 ArbVG, Verzeichnis Verarbeitungstätigkeiten, Rechenschaftspflicht nach DSGVO
- Unterstützung bei der Analyse der Veränderungen (technisch, organisatorisch, rechtlich) suchen
- Betriebsvereinbarung abschließen nach § 96 oder § 96a ArbVG
- Kontrolle des laufenden Betriebes organisieren (Regelungen Datenschutzgesetz beachten)

Klassifizierung von Daten/Information

Datenschutz	Datensicherheit
A: Allgemeine Daten zur Person	öffentlich
B: Daten zur Person, die verpflichtend aus Gesetz, Normen der kollektiven Rechtsgestaltung oder Arbeitsvertrag für einen eindeutigen und berechtigten Zweck verarbeitet werden müssen.	intern
C: Schutzwürdige Daten der Beschäftigten sowie Daten, für die keine der Datenschutzklasse B entsprechende Rechtsgrundlage besteht.	vertraulich
D: besondere Kategorien von Daten (sensible Daten).	geheim

Ist-Stand erheben -> FRAGEN STELLEN!

- Welche Systeme (inkl. Module) sind im Einsatz und wer ist Zuständiger (Owner)?
- Zu welchen Zwecken wird IT eingesetzt? Grundsätze Verarbeitung personenbezogener Daten (Rechenschaftspflicht! Art. 5 DS-GVO) und Beschreibung Verarbeitungstätigkeiten (Art. 30 DS-GVO)?
- Welche Unterlagen (Systembeschreibungen) sind vorhanden?
- Welche Daten werden in den Systemen erfasst?
- Welche Auswertungen sind vorgesehen?
- Wer hat Zugriff auf Daten und Auswertungen?
- Welche Daten werden zwischen den Systemen ausgetauscht (Schnittstellen) und/oder an andere Unternehmensstandorte übermittelt (bzw. in globalen Systemen gearbeitet)?
- Maßnahmen zur >> *IT-Datensicherheit*! (Protokolle, Datengeheimnis)
- Gibt es externe Auftragsverarbeiter? -> Vertrag!

Landkarte: IT/OT + Informationssicherheit

Access management	GRC software	Security analytics
Advanced threats and deep packet inspection	Identity and access management	Security orchestration and/or automation
Application security	Identity and access management as a service (IDaaS)	SIEM
Cloud access security broker (CASB)	Identity governance solution	Single sign-on (SSO)
Cloud security services	Internet of things (IoT) security	Software security (source code and architecture review, code scanning, etc.)
Container security	Managed detection & response (MDR)	Threat detection/management (IDS – Intrusion Detection System/IDP - Intrusion Detection and Prevention, sandboxing, etc.)
Data loss prevention	Managed security services	Threat intelligence (platforms or feeds)
Deception technologies	Mobile device security (incl. enterprise mobility management, unified endpoint management)	User provisioning
DevSecOps (integration of security into DevOps application development process; as a security initiative)	Monitoring software (incl. AIOps, APM, cloud, DevOps, log, metrics)	Virtualization security (protection of a virtualization infrastructure/environment)
DNS (Domain Name System) management	Multifactor authentification	Visibility or auditing tools for cloud based enviroments
DNS security and DDoS (Distributed-Denial-of-Services) defense	Network traffic analytics	VPN/NAC (network access control, as a security initiative)
Email security	Next-generation firewalls	Vulnerability management (patch/configuration management)
Encryption	Privileged identity or privileged account management solution	Web security
Endpoint detection & response (EDR)	Secure point-of-sale devices (incl. chip-capable card readers)	
Endpoint security (antimalware, endpoint suites, etc.)	Secure web gateway	
End-user security tracking		
Forensic capabilities (digital forensics)		
Fraud detection systems		

© TechTarget 2018

Zum Weiterlesen

Beschäftigtendatenschutz: Handbuch für die betriebliche Praxis
Hrsg.: Haslinger Susanne, Krisch Andreas, Riesenecker-Caba Thomas
ÖGB-Verlag

Betriebsrat und Information
Autoren: Felten Elias, Goricnik Wolfgang, Riesenecker-Caba Thomas
Verlag: Manz

DANKE FÜR DAS INTERESSE!

Thomas Riesenecker-Caba

Forschungs- und Beratungsstelle Arbeitswelt (FORBA)

riesenecker@forba.at

http://www.forba.at