Verfasser: Gerald Kortschak

Thema: DSGVO/DSG (Was – Wie – bitte konkret)

Dipl.-Ing. Gerald Kortschak, BSc, CMC

- Selbständig seit 2001
- IT-Systeme & Unternehmensberatung
- Zertifizierungen: CMC, CDISE, CDC, geprüfter Datenschutzexperte
- IT-Security ExpertGroup, Spr. Ö
- FH-Lektor: FH St. Pölten
- DSGVO-Vorträge & Workshops
- DSGVO-Begleitung (0-2400 MA)

FAKTEN

Die DSGVO gilt für alle EU-Mitgliedstaaten. Alle Unternehmen sind von den umfangreichen Neuerungen betroffen – von Ein-Personen-Unternehmen bis zum Großbetrieb.

Die DSGVO enthält zahlreiche Öffnungsklauseln und lässt den nationalen Gesetzgebern Spielräume. In Österreich wurde daher am 29. Juni 2017 das Datenschutz-Anpassungsgesetz 2018 vom Nationalrat beschlossen. Dieses tritt am 25. Mai 2018 in Kraft.

Tun Sie das nicht, drohen merklich höhere Strafen als bisher: Bis zu 20 Millionen Euro oder bis zu 4 Prozent des weltweiten Jahresumsatzes Ihres Unternehmens sind im Extremfall möglich.

Die neue Datenschutz-Grundverordnung (DSGVO) der EU regelt künftig den Umgang mit personenbezogenen Daten. Es wird darin u.a. vorgegeben, unter welchen Voraussetzungen Ihr Unternehmen diese Daten (z.B. Daten Ihrer Kunden) verarbeiten darf.

Quelle: WKÖ Informationsfolder Juni 2017

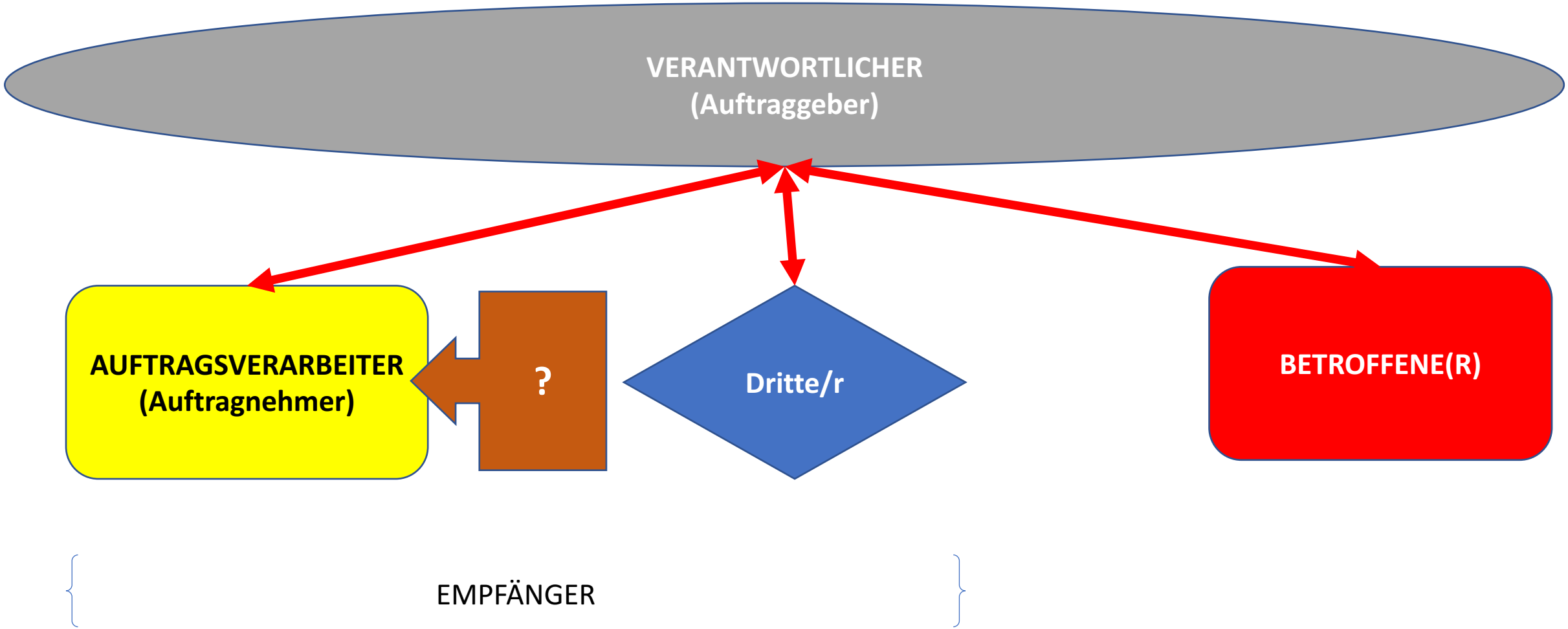
Welche Teile sind betroffen?

Quelle: https://www.wko.at/branchen/information-consulting/unternehmensberatung-buchhaltung-informationstechnologie/it-dienstleistung/it-dienstleister-als-datenschutzbeauftragter.html

Anleitung VdV – Die 8 Ws!

WER	• (wer als Verantwortlicher benannt wird)
WAS	• (welche Daten-Kategorien erfasst werden)
WO	• (Daten gespeichert und verarbeitet werden – betroffene Systeme,)
WARUM	• (was ist der Rechtsgrund der zur Anwendung kommt)
WOZU	• (Zweck der jeweiligen Datenverarbeitung)
WOHIN	• (wenn Daten weitergegeben werden - an wen werden die Daten übergeben, auch ob innerhalb der EU oder Drittland)
WIE LANGE	• (werden Daten gespeichert – welche Löschfristen kommen zur Anwendung)
WIE SICHER	• (welche Datensicherheitsmaßnahmen werden ergriffen).

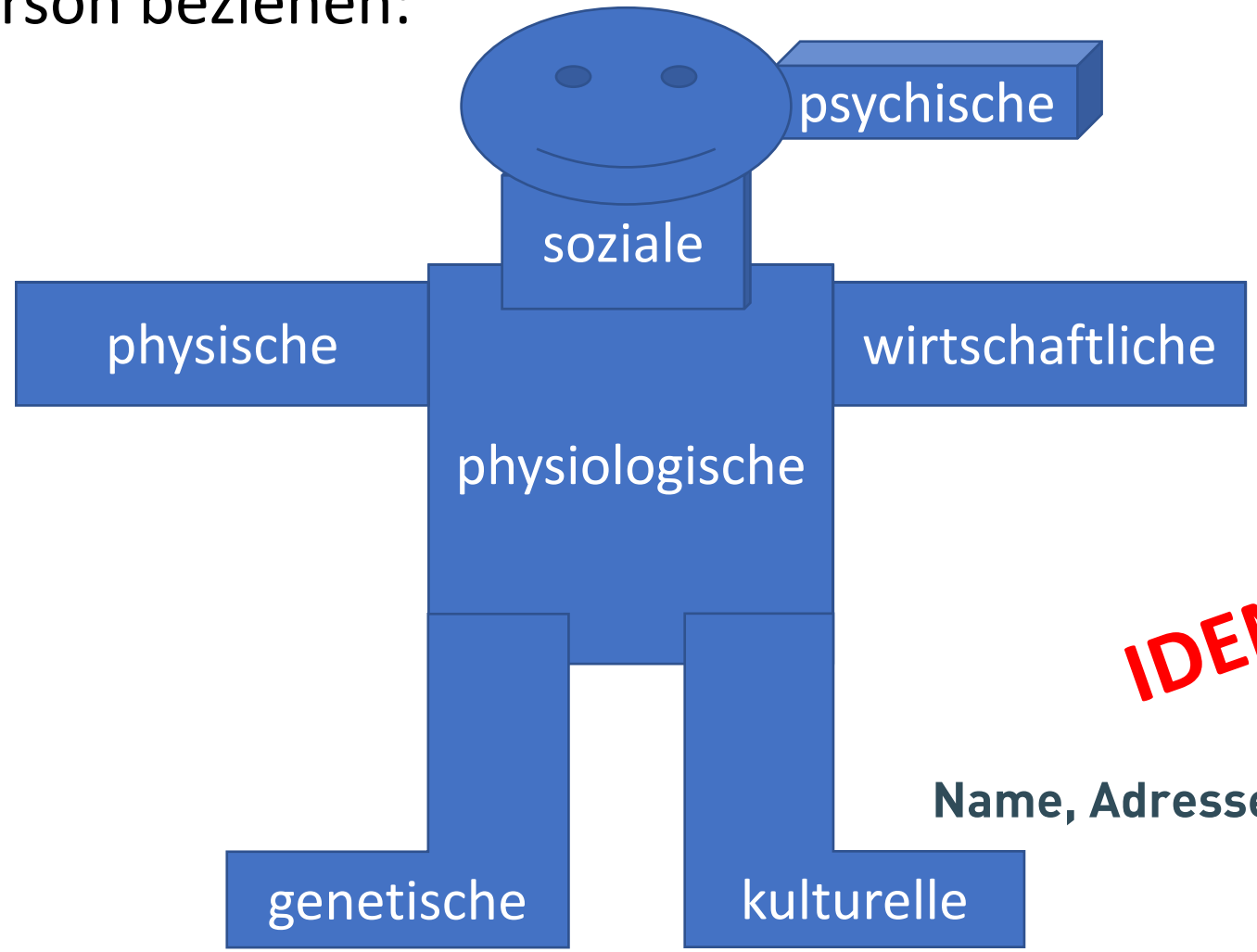
Rollen in der DSGVO



Um welche Daten geht es überhaupt?

Um welche Daten geht es?

alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen:



IDENTITÄT

Name, Adresse, Geburtsdatum, Bankdaten, et

SENSITIVE DATA

- rassische Herkunft
- Religion
- ethnische Herkunft
- politische Meinung
- sexuelle Orientierung
- Gewerkschafts -zugehörigkeit
- Weltanschauung

„genetische Daten“ personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden.

„biometrische Daten“

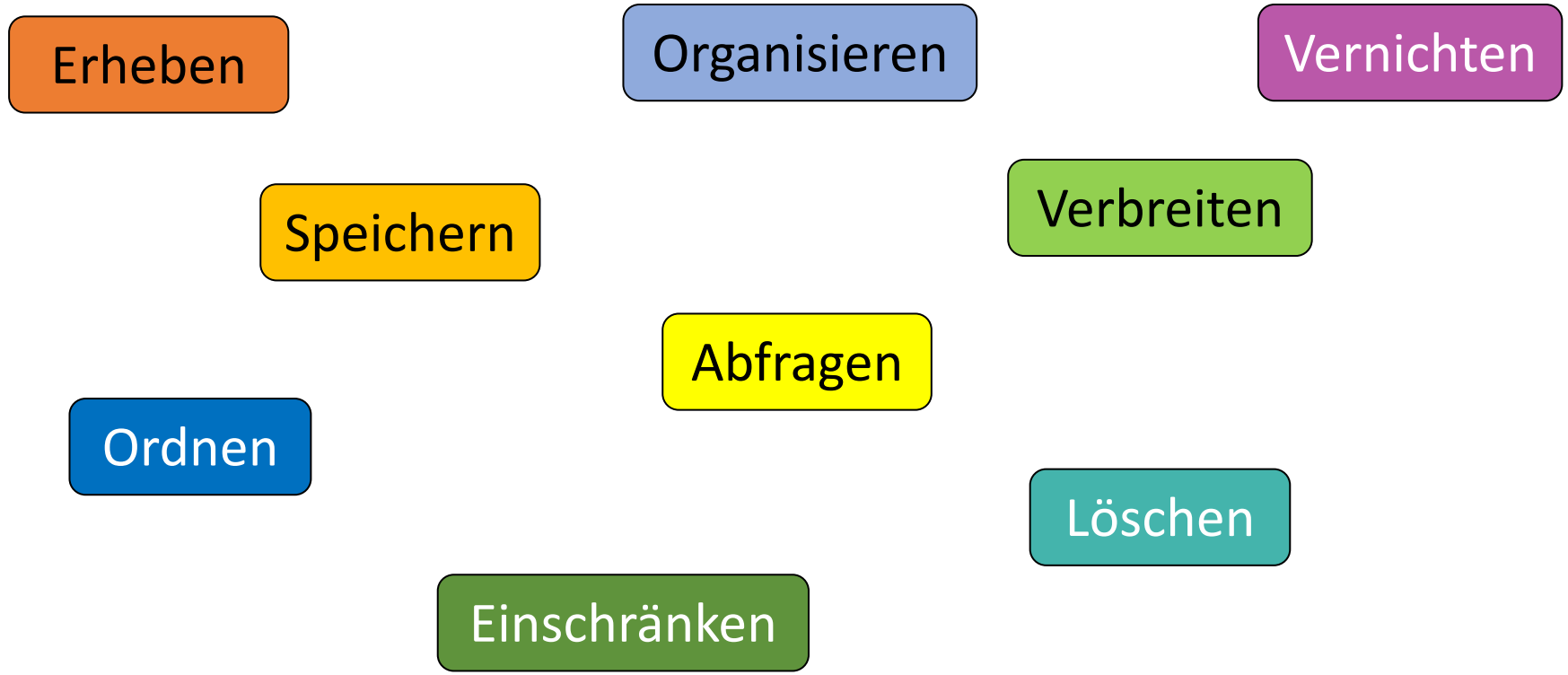
mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten.

„Gesundheitsdaten“

personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.

Was bedeutet Datenverarbeitung?

jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang im Zusammenhang mit personenbezogenen Daten



!

Auch **manuelle Daten** unterliegen der DSGVO, wenn sie in einem Dateisystem gespeichert sind und einer gewissen Ordnung unterliegen.

DIE DSGVO

UNTERSAGT

DIE

VERARBEITUNG

außer ...

Rechtmäßigkeit der Verarbeitung 1/2

Generell Verbotsgesetz, außer:

Verarbeitung für Erfüllung eines Vertrages notwendig

z.B.: Online-Bestellung → Lieferadresse	Angebotslegung, Auftragserfüllung, ...

Erfüllung rechtlicher Verpflichtung, z.B.:

Rechnungslegung (Finanzrecht)	Mitarbeiter-Abrechnung (Sozialversicherungsnummer)

lebenswichtiges Interesse des Betroffenen

z.B.: Medizinischer Bereich

Rechtmäßigkeit der Verarbeitung 2/2

Generell Verbotsgesetz, außer:

Wahrung eines berechtigten Interesses des Verantwortlichen

- Betrugsverhinderung (ErwG: 47)
- Direktwerbung (ErwG: 47)

Anonymisierte Verarbeitung

- Keine Identifizierung der betroffenen Person möglich

Einwilligung seitens des Betroffenen liegt vor

- Bedingungen für Einwilligung erfüllen!
- Achtung: Eigene Bedingungen für Einwilligung eines Kindes

Zustimmungserklärung wie?

Welche Datenarten (Name, Geburtsdatum, ...) werden

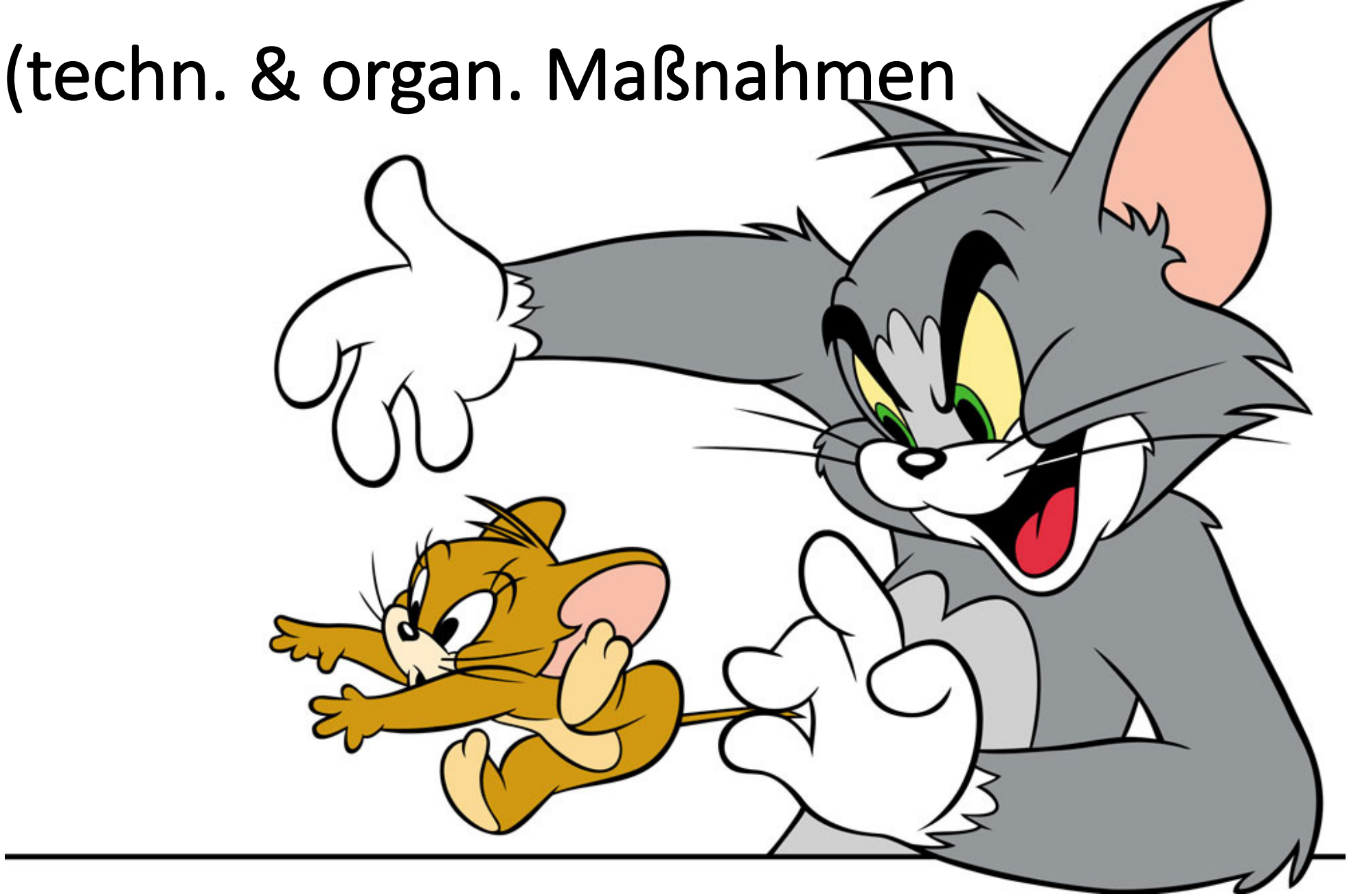
zu welchem Zweck (zB Newsletter) gespeichert und/oder

an wen übermittelt? (Firma, Land, Zweck)

Widerrufsbelehrung

schriftlich empfohlen!

TOMs (techn. & organ. Maßnahmen



“geeignete“ TOM – techn. und org. Maßnahmen

- die **Pseudonymisierung** und **Verschlüsselung** personenbezogener Daten;
- die Fähigkeit, die **Vertraulichkeit, Integrität, Verfügbarkeit** und **Belastbarkeit** der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- die Fähigkeit, die **Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen** bei einem physischen oder technischen Zwischenfall **rasch wiederherzustellen**;
- ein Verfahren zur **regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit** der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

DAHER:
Backup-Konzept erstellen!

Datensicherheitsmaßnahmen (§54 DSG [für Behörden])

Risikobewertung → Maßnahme

STAND DER TECHNIK

- Zugangskontrolle
- Datenträgerkontrolle
- Speicherkontrolle
- Benutzerkontrolle
- Zugriffskontrolle
- Übertragungskontrolle
- Eingabekontrolle
- Transportkontrolle
- Wiederherstellung
- stabiles System: Zuverlässigkeit / Datenintegrität

TOMS

- **Beispiel**
  Kundenkartei in Papierform
  Notebook, Tablet, Smartphone
  USB-Sticks
  …
- **Bei IT-System sind insbesondere, Zugriffskontrollen (sichere Passwörter), Pseudonymisierung und Verschlüsselungssysteme, Firewalls, Spam-Filter, Anti-Viren-Programme und Backups wichtig.**

Drucker als Sicherheitslücke

Transaktionsdruck

Kontrolle des Datenflusses erschwert.
Potential für OEMs lt. Druckerhersteller-Branche.

Rechte der Betroffenen

DSGVO – Rechte der betroffenen Personen

- Auskunftsrecht (Art. 15)
- Berichtigung (Art. 16)
- Löschung (Art. 17) – Recht auf Vergessenwerden
- Widerspruch (Art. 21)
- Einschränkung der Verarbeitung (Art. 18)
- Recht auf Datenübertragbarkeit (Art. 20)

Recht auf Löschung

Dem Verlangen ist grundsätzlich Folge zu leisten, es sei denn spezielle Ablehnungsgründe liegen vor. Der wichtigste Ablehnungsgrund sind die gesetzlichen Aufbewahrungsfristen.

Daten, die nur aufgrund einer Einwilligung länger als die gesetzlichen Fristen gespeichert wurden, sind auf Verlangen des Betroffenen umgehend zu löschen.
Im Verarbeitungsverzeichnis sind die Aufbewahrungsfristen, wenn möglich, ebenfalls anzuführen.

Aufbewahrungsfristen - Allgemein

- Steuerrechtliche Aufbewahrungspflicht nach § 132 Abs 1 BAO: 7 Jahre
- Unternehmensrechtliche Aufbewahrungspflicht nach §§ 190, 212 UGB: 7 Jahre
- Allgemeiner Schadenersatz nach § 1489 ABGB (Entschädigungsklagen): 3 Jahre (wenn Schaden und Schädiger bekannt) /ansonsten 30 Jahre

Recht auf Datenübertragbarkeit

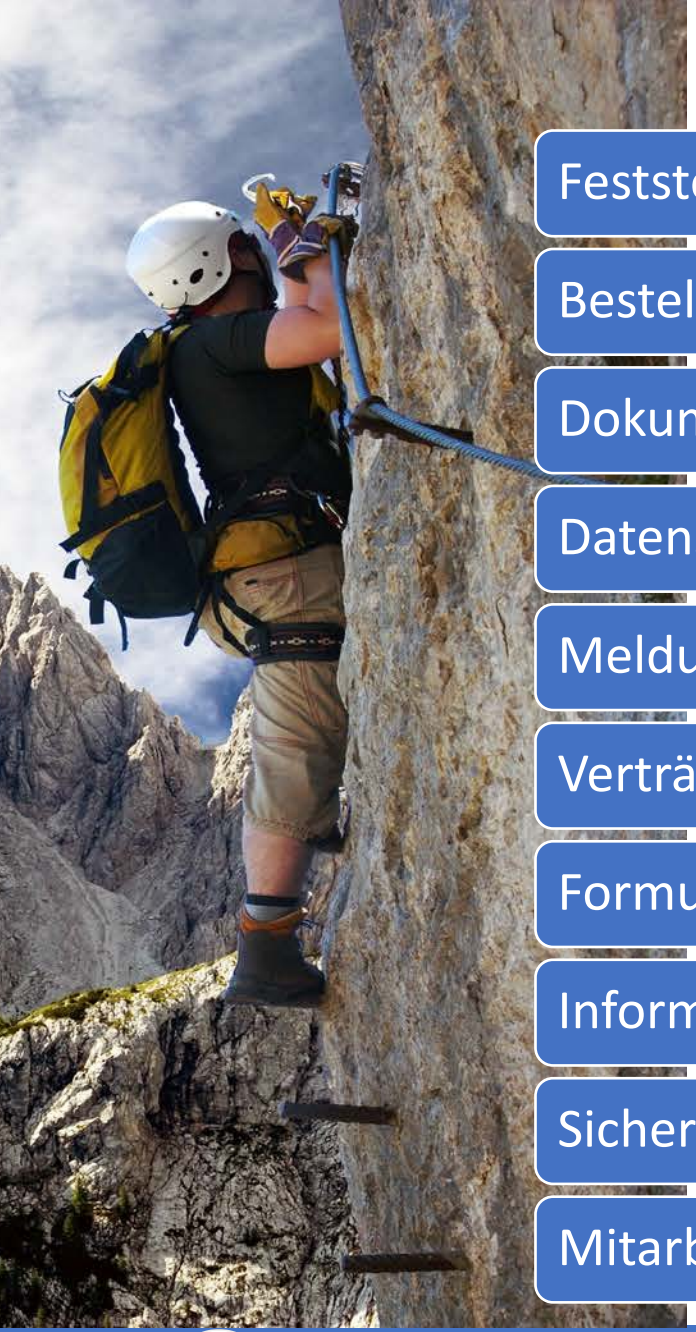
- **Beispiel:** Ein Kunde möchte die Druckerei wechseln und seine Daten mitnehmen. Um die Pflicht zu erfüllen reicht es aus, ihm die Daten in einem gängigen Format (Word, Excel,… elektronisch (E-Mail, USB-Stick,…) zukommen zu lassen.

- PDFs sollten hierfür nicht verwendet werden

- Voraussetzung:
  - automatisierte Verarbeitung
  - gilt nicht für Papier

Datenschutzbeauftrager & Risiko

FAZIT



10 Wegpunkte zur DSGVO

- Feststellung IST-Zustand
- Bestellung Datenschutzbeauftragter ja/nein
- Dokumentation der Verarbeitungsvorgänge
- Datenschutz-Folgenabschätzung
- Meldung von Verstößen
- Verträge mit Auftragsverarbeitern
- Formulare prüfen und Anpassen
- Informationspflichten / Betroffenenrechte
- Sicherheitsmaßnahmen
- Mitarbeiterschulungen

Verfahrensverzeichnis

Stammdatenblatt

Data-Breach-Notification

Logbuch

Antworttexte Begehren

TOMs

Verträge

WK hilft

Förderung für:
WIFI-Kurse
Beratungen (Fokus C) von Certified Data & IT Security Expert
50% bis max. € 1.000,--
Potential-Analyse zu 100% gefördert (Certified Digital Consultant)

KMU DIGITAL

WKO bmwfw

Online Hilfestellungen und Tipps:

- **wko.at/datenschutz**

Mit Rat und Tat:
Rechtsservice WK-STMK
0316 / 601 - 601

WKO STEIERMARK

Ihre Fachgruppe

Die IT-Architekten

DER SCHENNER Consulting & Training

sevian7 e pluribus unum

>> www.sevian7.com

Ing. DI(FH) Harald SCHENNER, CMC und DI Gerald Kortschak, BSc, CMC
www.derSchenner.at | www.sevian7.com
www.dsgvo2018.at

CERTIFIED DATA & IT SECURITY EXPERT

CERTIFIED DIGITAL CONSULTANT

Geprüfte Datenschutz-Experten

Wir weisen ausdrücklich darauf hin, dass es sich bei den vorliegenden Unterlagen um ein unentgeltliches Service der Autoren handelt und die Informationen keine Unternehmensberatung darstellen. Jegliche Haftung für die Aktualität, Richtigkeit und Vollständigkeit der dargestellten Informationen wird ausgeschlossen.