



Verfasser: Gerald Kortschak, Harald Schenner
Thema: DSGVO/DSG (Was – Wie – bitte konkret)



- 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.



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 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.



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?

RECHT
DSGVO / DSG /
Materiengesetze

PROZESSE
Abläufe definieren



ORGANISATION

Team
Mitarbeiter

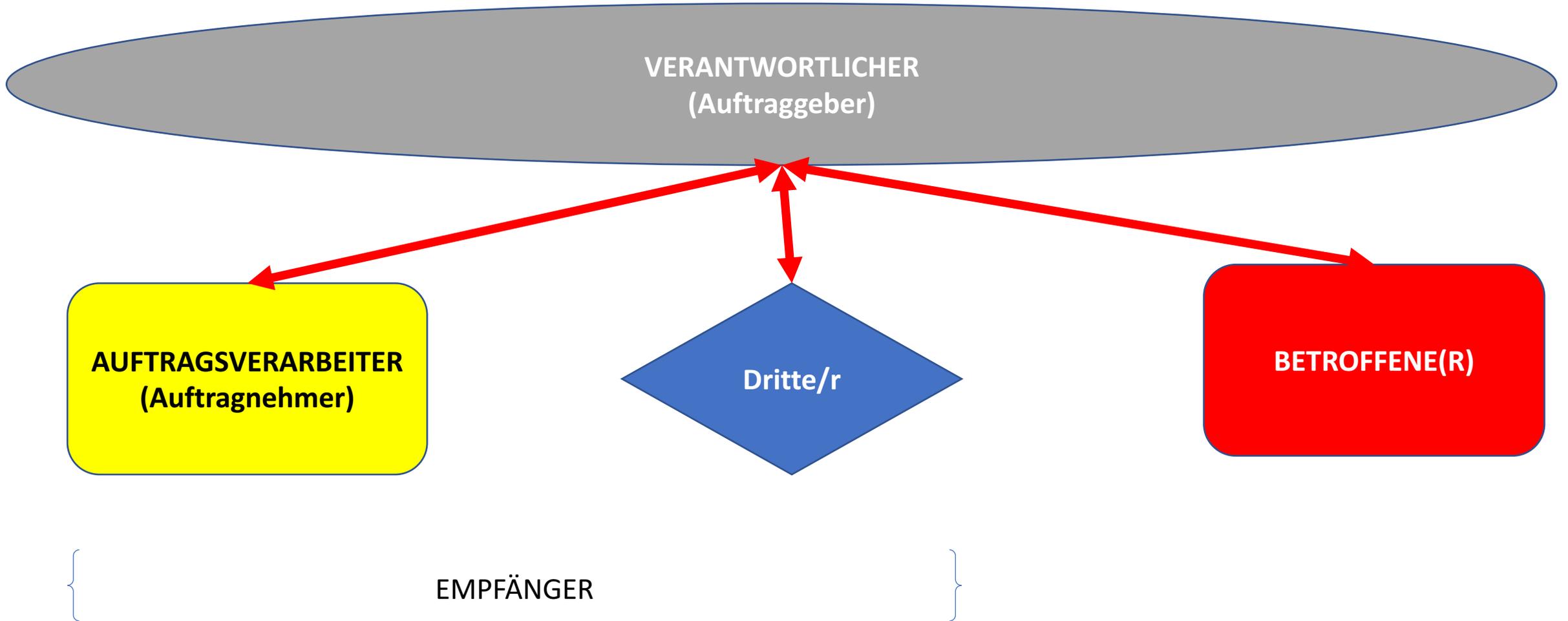
IT & SYSTEME

Technik
Computer-Netzwerk

AK Daten/Bernd Schauer, lawvision

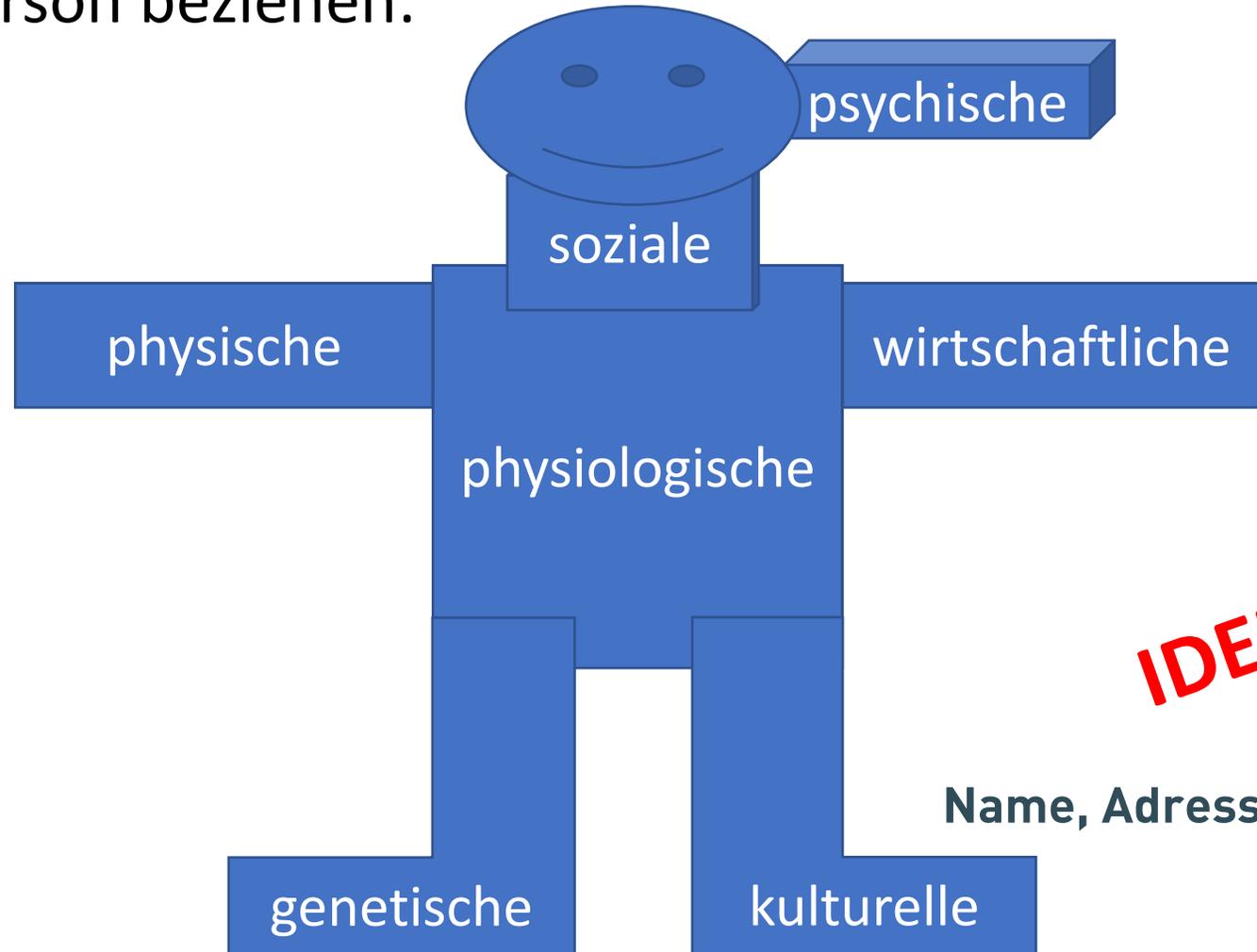
Quelle: <https://www.wko.at/branchen/information-consulting/unternehmensberatung-buchhaltung-informationstechnologie/it-dienstleistung/it-dienstleister-als-datenschutzbeauftragter.html>

Rollen in der DSGVO



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

ethnische
Herkunft

genetische &
biometrische
Daten

Gesundheits-
daten

Gewerkschafts-
zugehörigkeit

politische
Meinung

Religion

sexuelle
Orientierung

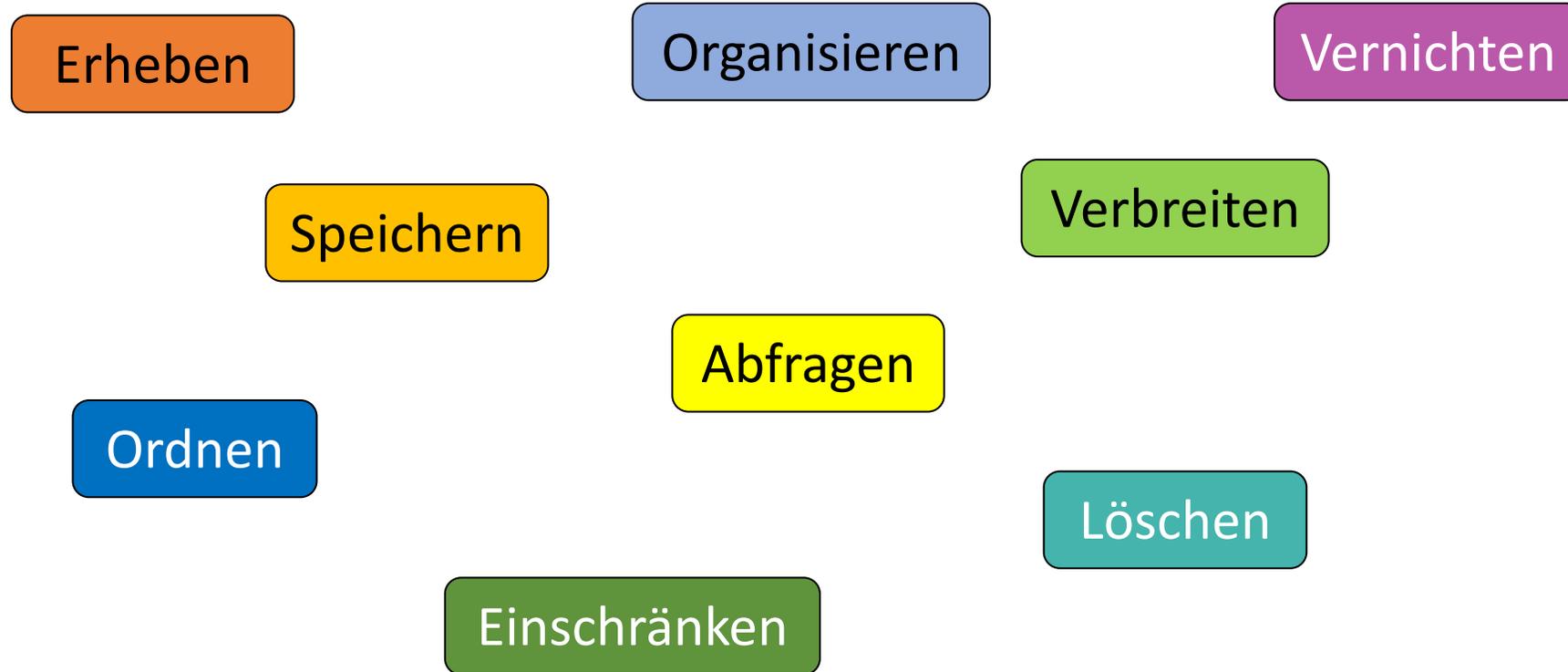
Weltanschauung

Beispiele

- eMail-Adresse Kunden
- Telefonnummer Kunden
- IP-Adressen in OnlineShops
- Sozialversicherungsnummer Mitarbeiter
- Videoüberwachungsanlage
- WhatsApp Kommunikation mit Kunden („Buch ist da“)
- AUVA Meldungen
- Daten der Lohnverrechnung

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.

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 oder Tourismus (Gastronomie)

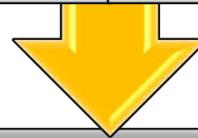
Rechtmäßigkeit der Verarbeitung 2/2

Generell Verbotsgesetz, außer:

Wahrung eines berechtigten Interesses des Verantwortlichen

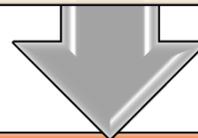
Betrugsverhinderung (ErwG: 47)

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

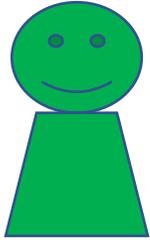
zu welchem Zweck (zB Newsletter) gespeichert und/oder

an wen übermittelt? (Firma, Land, Zweck)

Widerrufsbelehrung

schriftlich empfohlen!

Beispiel 1 - Angebotslegung



Kunde

Bitte ein Angebot

Unternehmen

Daten für Angebotslegung
Name, Adresse, ...

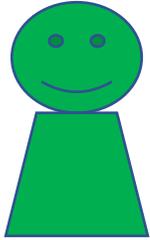
- ✓ Betriebliches Interesse
- ✓ „nur“ für Angebotserstellung

Angebot übermitteln

Angebot wird nicht angenommen

Daten werden gelöscht.
„Kunde“ wird vergessen.

Beispiel 1 - Angebotslegung



Kunde

Bitte ein Angebot

Unternehmen

Daten für Angebotslegung
Name, Adresse, ...

- ✓ Betriebliches Interesse
- ✓ „nur“ für Angebotserstellung

Angebot übermitteln

Angebot wird angenommen / Auftrag

- ✓ Daten zur Auftrags Erfüllung
- ✓ Daten zur Rechnungslegung
- ✓ Aufbewahrung 7 Jahre (bis zu 30 Jahre)
- ✓ Nach Aufbewahrungsdauer „Einmal“-Kunde wird vergessen



Wie gehe ich konkret vor?



Was muss ich tun? 1/2

Erfassung der Verarbeitungstätigkeiten (VT) und Datensysteme (IT-Systeme und Papier)

Erfassung bestehender Verträge zu externen Dienstleistern und Auftragsverarbeiter

Risiko-Abschätzung (Folgenabschätzung?)

Technische und organisatorische Maßnahmen definieren (+ Lösch- und Backup-Konzept)

Erstellung Verzeichnis der Verarbeitungstätigkeiten (VdV)

Was muss ich tun? 2/2

Verträge mit externen Dienstleistern und Auftragsverarbeitern

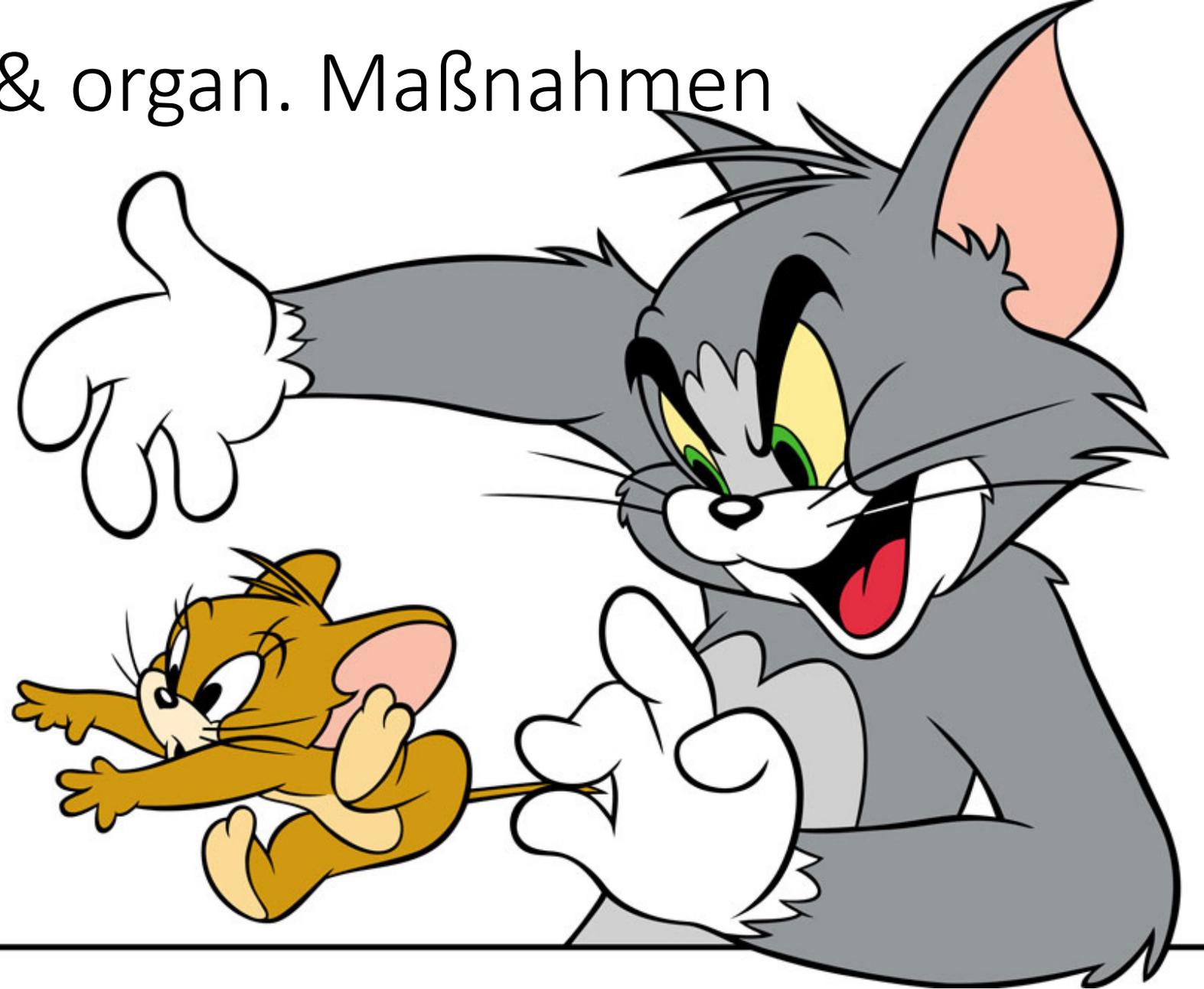
Geheimhaltungs-/Verschwiegenheitsvereinbarungen mit Kooperationspartnern und Mitarbeitern

Prozesse zur Wahrung der Betroffenenrechte

Prozess zur Meldung Datenschutz-Verstoß an die DSB

Schulung der eigenen Mitarbeiter und Planung jährliches Review

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 DSGVO)

Risikobewertung

Maßnahme

STAND DER TECHNIK

Zugangskontrolle

Datenträgerkontrolle

Speicherkontrolle

Benutzerkontrolle

Zugriffskontrolle

Übertragungskontrolle

Eingabekontrolle

Transportkontrolle

Wiederherstellung

stabiles System: Zuverlässigkeit / Datenintegrität

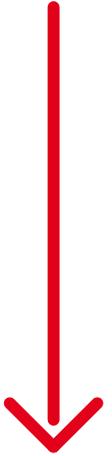
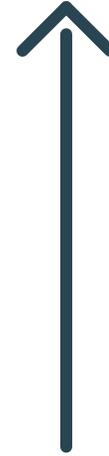
Unter Berücksichtigung

- des Standes der Technik,
- der Implementierungskosten und
- der Art,
- des Umfangs,
- der Umstände und
- der Zwecke der Verarbeitung sowie der
- unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen

Stand der Technik – Ist machbar!



**LOS
GEHT'S!**



EFFIZIENZ

QUALITÄT

KOSTEN

Mindest-Inhalt

Beschreibung des
Verantwortlichen und
Datenschutzbeauftragten

Zweck der Verarbeitung
und Rechtsgrundlage

Kategorien der
betroffenen Personen

Kategorien der
personenbezogenen
Daten

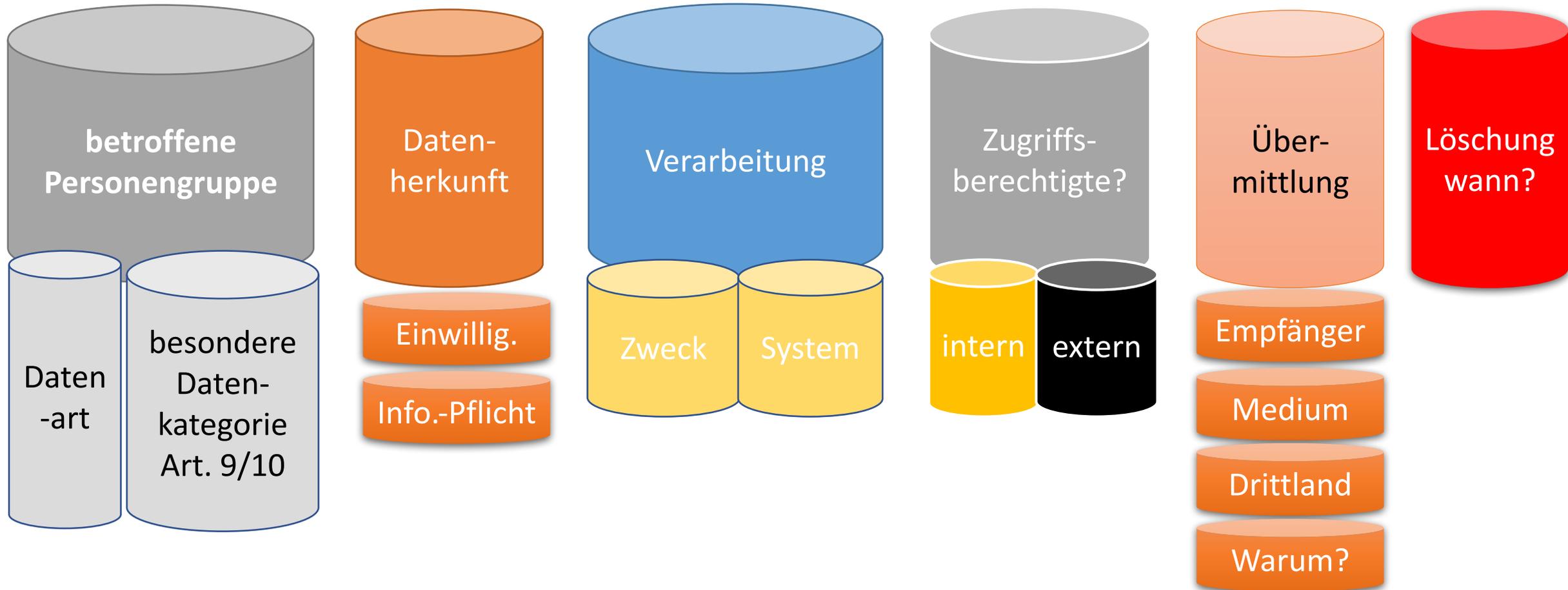
Kategorien der
Empfängerkreise

Löschungsroutine /
Löschfristen

Beschreibung TOM

Verwendung von Profiling

Schritt 3: VdV - Verarbeitungsverzeichnis



Erhebungsgrundlage?
gesetzliche Vorgabe / Vertragserfüllungsnotwendigkeit / berechtigtes Interesse / Einwilligung



Vorgehen Schritt 4: Prozesse & Pflichten

- Prozesse zur Wahrung der Betroffenenrechte
 - Auskunft
 - Löschung
 - Widerruf
 - Einschränkung
 - Berichtigung
 - Datenübermittlung
- Meldung an DSB bei Datenschutz-Verstoß

Vorgehen Schritt 5: Rahmenbedingungen

- Verträge mit Auftragsverarbeiter
- Verträge (Verschwiegenheit) mit Mitarbeitern
- Schulung der Mitarbeiter
- Planung des jährlichen Reviews

Verfahrensverzeichnis

Stammdatenblatt

Data-Breach-Notification

Logbuch

Antworttexte
Begehren

TOMs

Verträge

DSGVO – Rechte der betroffenen Personen

Auskunftsrecht (Art. 15)

Berichtigung (Art. 16)

Löschung (Art. 17) – Recht auf Vergessenwerden

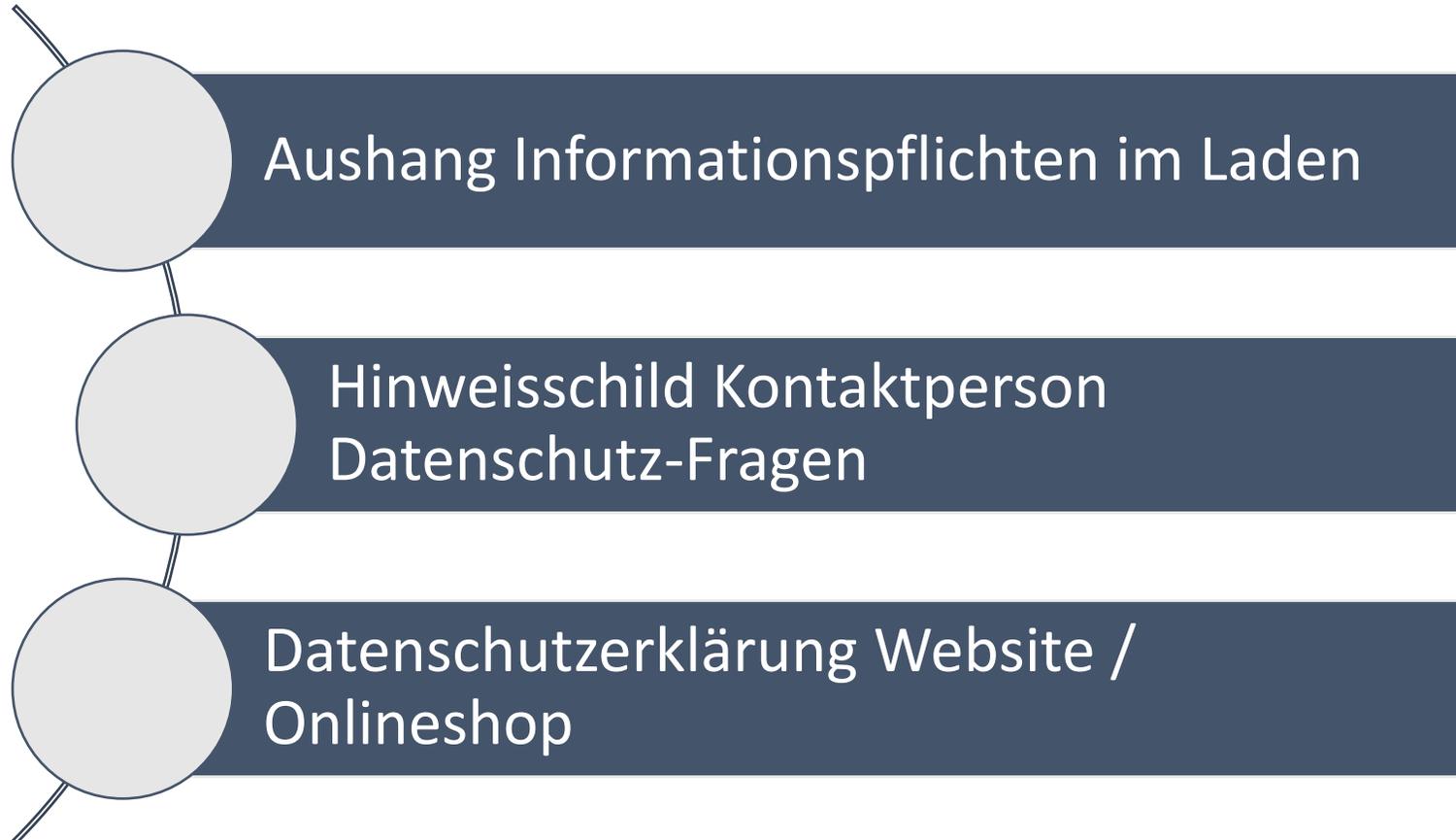
Widerspruch (Art. 21)

Einschränkung der Verarbeitung (Art. 18)

Recht auf Datenübertragbarkeit (Art. 20)

Buchtitel, die eine Person in einer **Online-Buchhandlung** gekauft hat, oder über einen Musik- Streaming-Dienst angehörte Musikstücke **sind weitere Beispiele für personenbezogene Daten, die generell in den Anwendungsbereich des Rechts auf Datenübertragbarkeit fallen**, da sie auf der Grundlage eines Vertrags verarbeitet werden, dessen Vertragspartei die betroffene Person ist.

ARTIKEL 29-DATENSCHUTZGRUPPE



- Kunde bestellt Buch
- Daten direkt an die Auslieferung
 - => Auftragsverarbeitungsvereinbarung erforderlich

Kataloge

- Kataloge mit Bestellformular
 - => Informationspflicht
 - Auskunftsbegehren

ACHTUNG – Deutschland

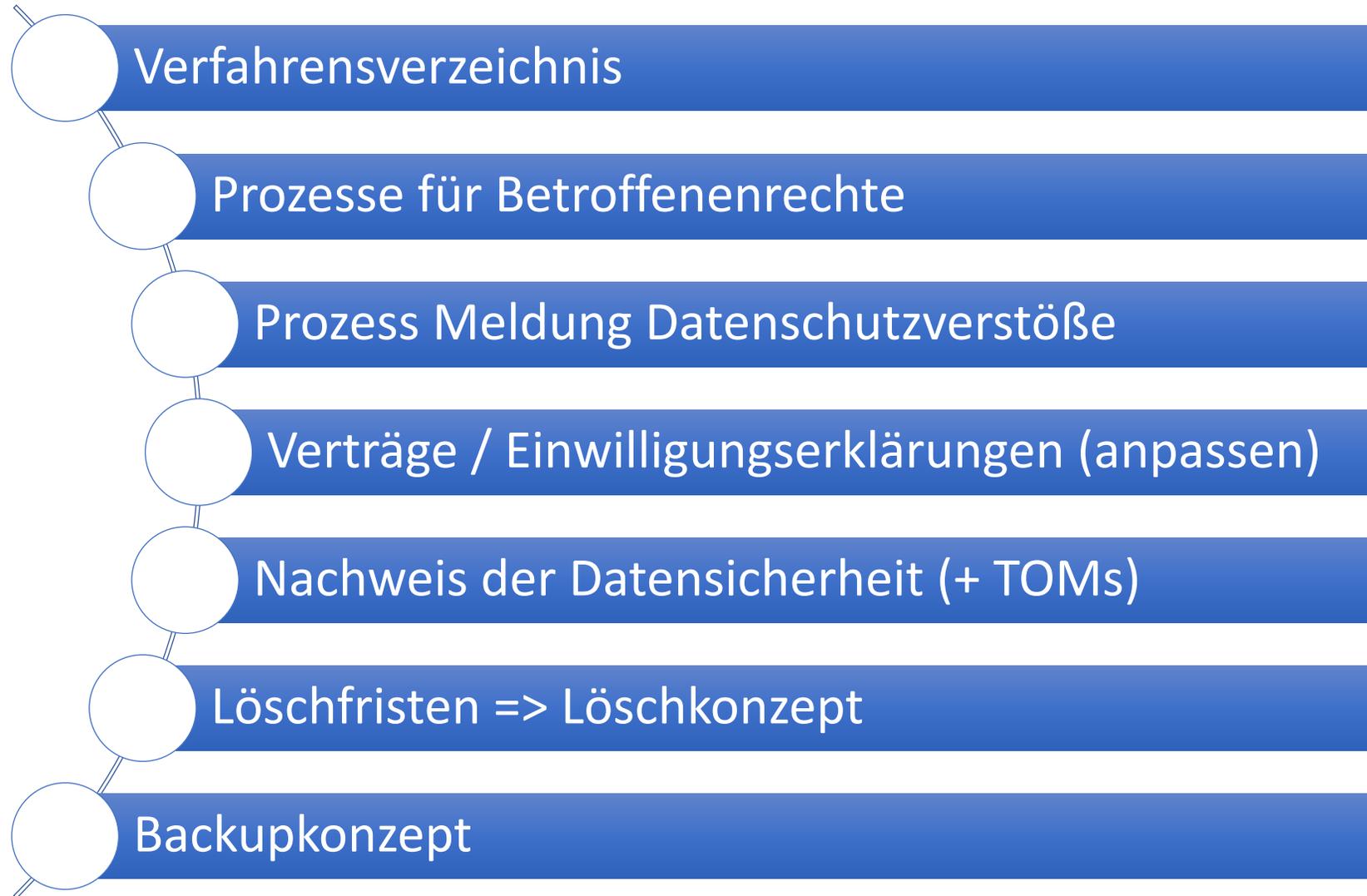
- **Unternehmensgröße / Anzahl der Mitarbeiter**
- Ab welcher Unternehmensgröße ein Datenschutzbeauftragter zu bestellen ist, hängt vom Umgang mit personenbezogenen Daten ab. Im Fokus steht das Ausmaß der Datenverarbeitung. **Sollten mehr als neun Mitarbeiter regelmäßig mit automatisierter Datenverarbeitung (Erhebung und Nutzung) zu tun haben, besteht die Pflicht.** Ebenso besteht eine Verpflichtung, sobald mindestens 20 Personen beschäftigt werden, die regelmäßig mit nicht automatisierter Datenverarbeitung zu tun haben.
 - Wird in Deutschland auf Medienhandel angewandt!

Artikel 40 DSGVO - Verhaltensregeln

2. Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, können Verhaltensregeln ausarbeiten oder ändern oder erweitern, mit denen die Anwendung dieser Verordnung beispielsweise zu dem Folgenden präzisiert wird:

- a) faire und transparente Verarbeitung;
- b) die berechtigten Interessen des Verantwortlichen in bestimmten Zusammenhängen;
- c) Erhebung personenbezogener Daten;
- d) Pseudonymisierung personenbezogener Daten;
- e) Unterrichtung der Öffentlichkeit und der betroffenen Personen;
- f) Ausübung der Rechte betroffener Personen;
- g) Unterrichtung und Schutz von Kindern und Art und Weise, in der die Einwilligung des Trägers der elterlichen Verantwortung für das Kind einzuholen ist;
- h) die Maßnahmen und Verfahren gemäß den Artikeln [24](#) und [25](#) und die Maßnahmen für die Sicherheit der Verarbeitung gemäß Artikel [32](#);
- i) die Meldung von Verletzungen des Schutzes personenbezogener Daten an Aufsichtsbehörden und die Benachrichtigung der betroffenen Person von solchen Verletzungen des Schutzes personenbezogener Daten;
- j) die Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen oder
- k) außergerichtliche Verfahren und sonstige Streitbelegungsverfahren zur Beilegung von Streitigkeiten zwischen Verantwortlichen und betroffenen Personen im Zusammenhang mit der Verarbeitung, unbeschadet der Rechte betroffener Personen gemäß den Artikeln [77](#) und [79](#).

Fazit – Was braucht man mindestens?





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
WIRTSCHAFTSKAMMER
ÖSTERREICH

bmwfw
Bundesministerium für
Wirtschaft, Innovation und Technologie

Online Hilfestellungen und Tipps:

wko.at/datenschutz

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



Ihre Regionalstelle: 0316 601 9360
Katharina LANG

Die IT-Architekten

DER  SCHENNER
Consulting & Training



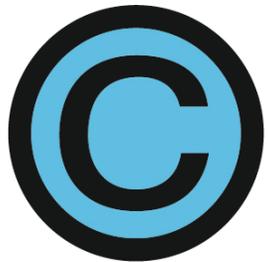
sevia
e pluribus unum

>> 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.

Alle Rechte, insbesondere das Recht der Vervielfältigung und Verbreitung sowie der Übersetzung, vorbehalten. Kein Teil dieser PowerPoint-Präsentation darf in irgendeiner Form (durch Fotokopie, Mikrofilm oder ein anderes Verfahren) ohne schriftliche Genehmigung der Autoren reproduziert oder unter Verwendung elektronischer Systeme gespeichert, verarbeitet, vervielfältigt oder verbreitet werden.

Die für Schulen und Hochschulen vorgesehene freie Werknutzung „Vervielfältigung zum eigenen Schulgebrauch“ gilt für dieses Werk nicht, weil es seiner Beschaffenheit und Bezeichnung nach nicht zum Unterrichtsgebrauch bestimmt ist.