DSGVO - KickOff

Verfasser: Gerald Kortschak, Harald Schenner

Thema: Anforderungen, Vorgehensweise, Ressourcenplanung

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.

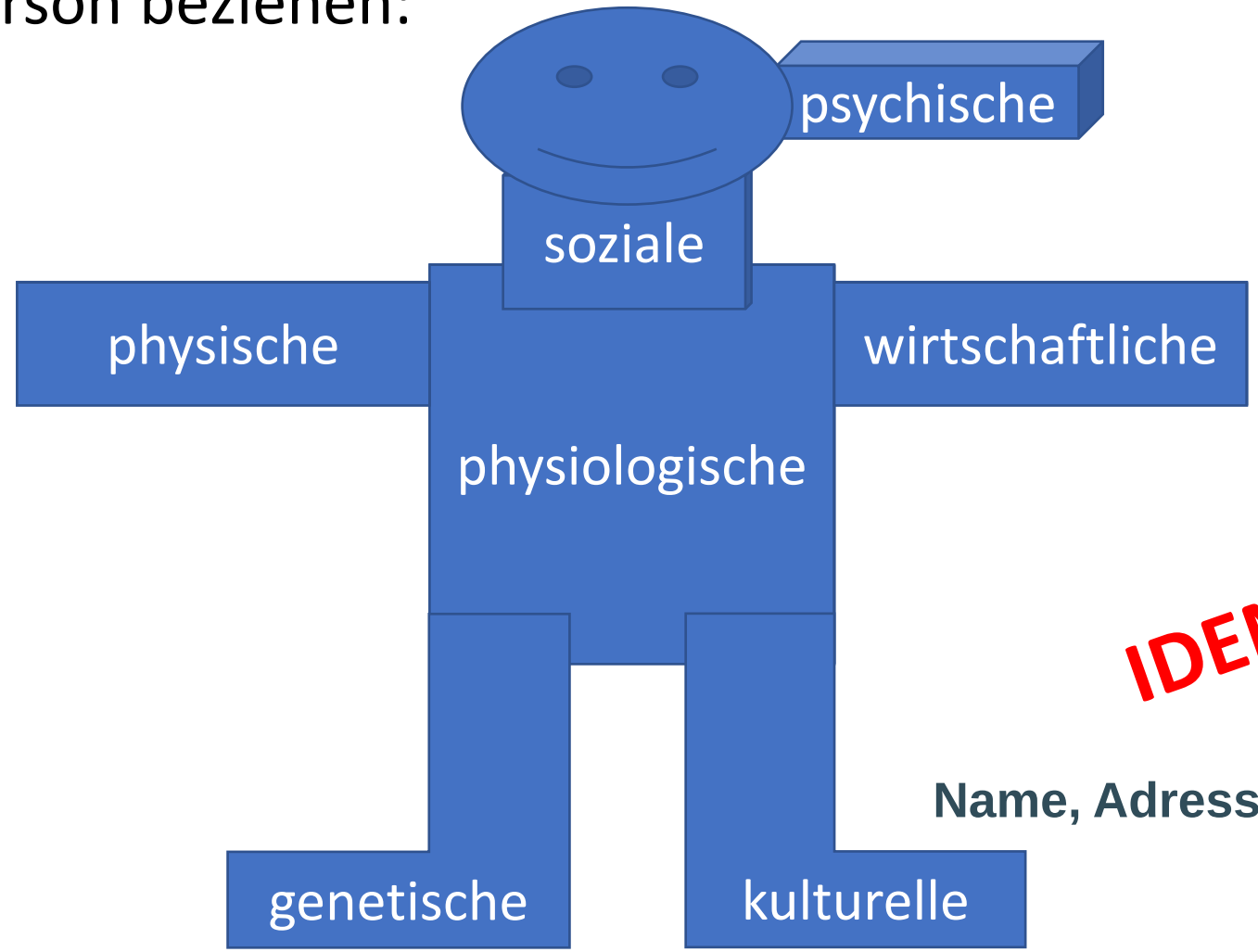
Tun Sie das nicht, drohen merklich höhere Strafen als bisher: Bis zu 20 Millionen Euro oder bis zu 4 Prozent des weltweiten Jahresumsatzes Ihres Unternehmens sind im Extremfall möglich.

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

Um welche Daten geht es?

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



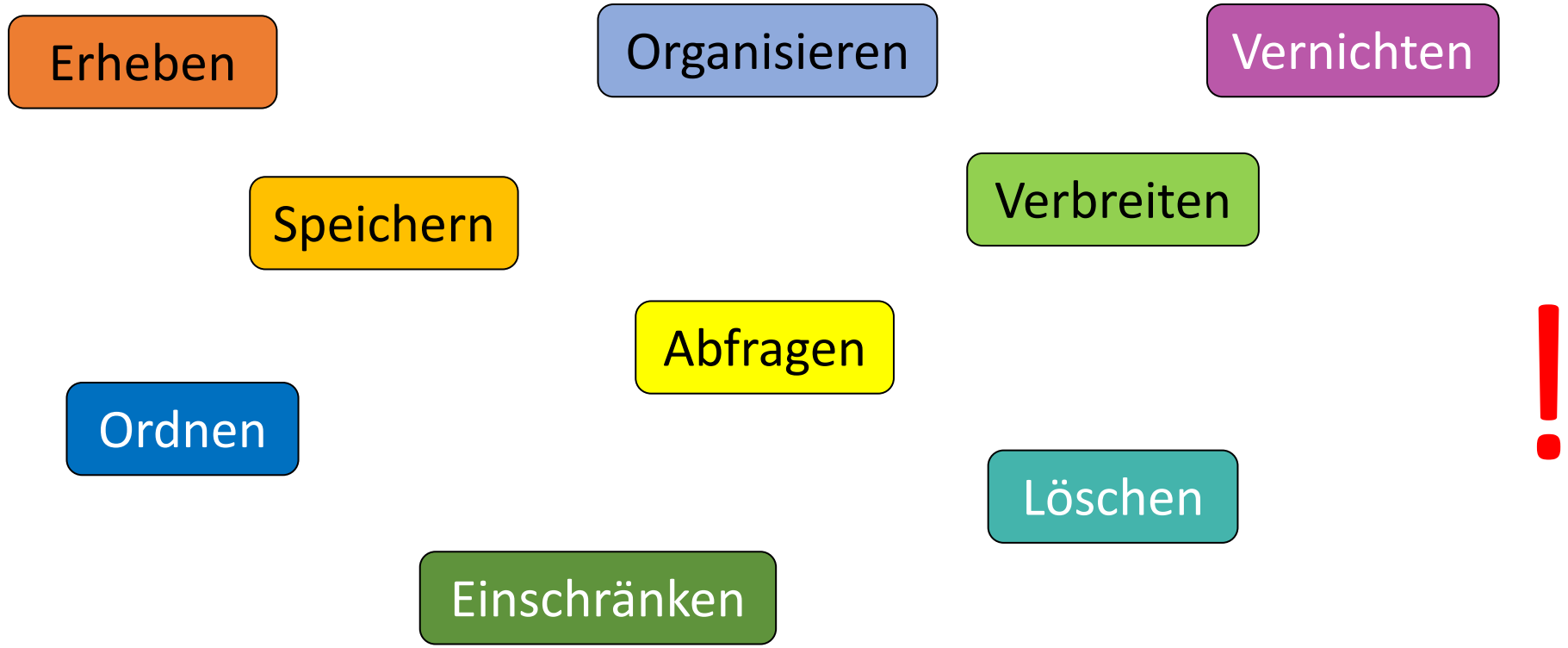
IDENTITÄT

Name, Adresse, Geburtsdatum, Bankdaten,


SENSITIVE DATA
rassische Herkunft
ethnische Herkunft
genetische & biometrische Daten
Gesundheits -daten
Gewerkschafts -zugehörigkeit
politische Meinung
Religion
sexuelle Orientierung
Weltanschauung

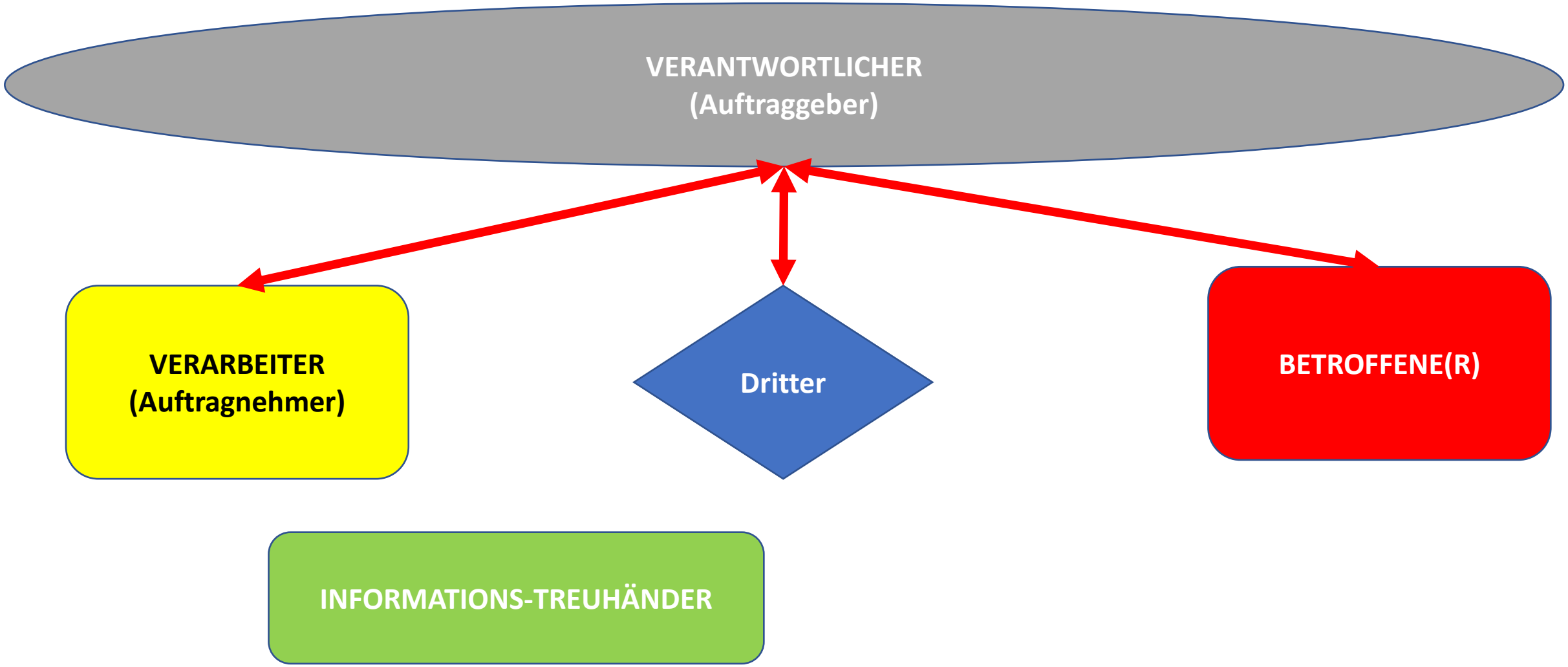
Was bedeutet Datenverarbeitung?

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

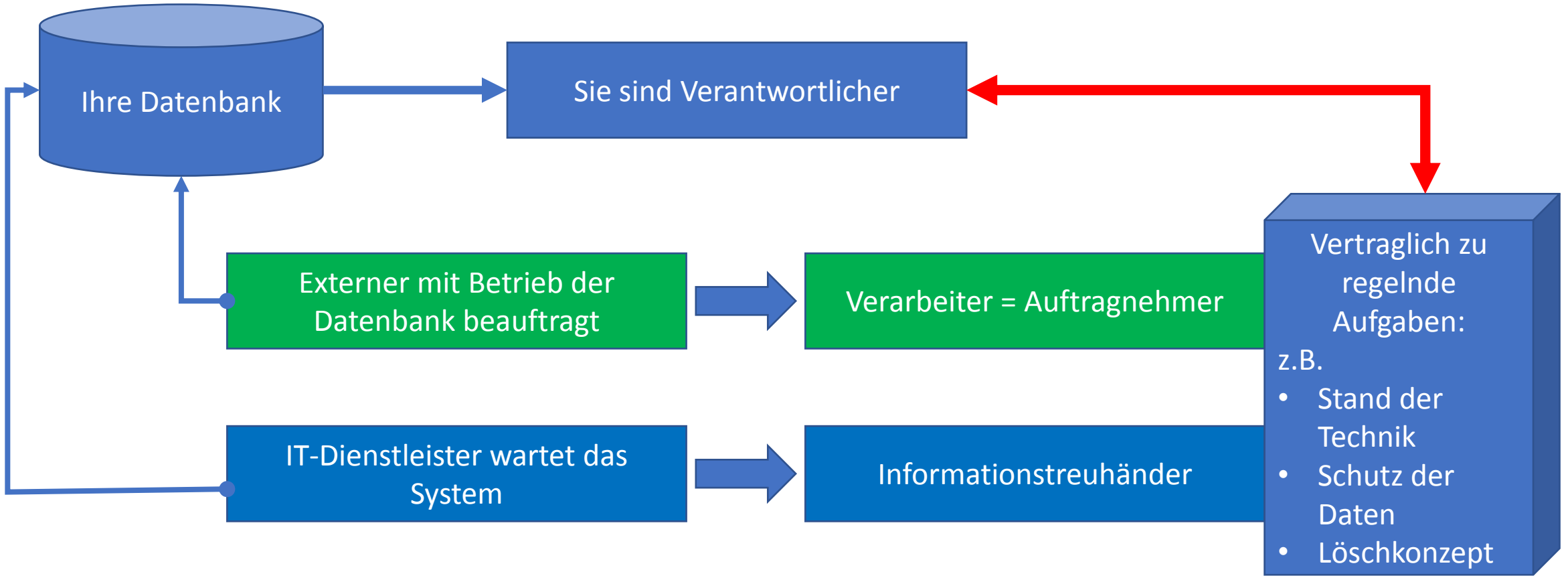


Auch **manuelle Daten** unterliegen der DSGVO, wenn sie in einem Dateisystem gespeichert sind und einer gewissen Ordnung unterliegen.

Rollen in der DSGVO



Verkettung von Daten



Rechtmäßigkeit der Verarbeitung 1/2

Datenverarbeitungen sind **verboten**, außer

- Verarbeitung für Erfüllung eines **Vertrages** notwendig
  - z.B.: Online-Bestellung → Name, Lieferadresse
  - Angebotslegung, Auftragserfüllung, ...

- Erfüllung einer **rechtlicher Verpflichtung**, z.B.:
  - z.B. Rechnungslegung (Finanzrecht)
  - Mitarbeiter-Abrechnung (Sozialversicherungsnummer)

- **lebenswichtiges Interesse** des Betroffenen
  - z.B.: Medizinischer Bereich

Rechtmäßigkeit der Verarbeitung 2/2

Datenverarbeitungen sind **verboten**, außer

- Wahrung eines **berechtigten Interesses** des Verantwortlichen
  - Direktwerbung (ErwG: 47)

- **Einwilligung** seitens des Betroffenen liegt vor
  - Bedingungen für Einwilligung erfüllen!
  - Achtung: Eigene Bedingungen für Einwilligung eines Kindes

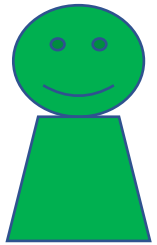
- **Anonymisierte** od. **pseudonymisierte** Verarbeitung
  - Keine Identifizierung der betroffenen Person möglich

Bedingungen für gültige Einwilligung

- Welche **Datenarten** (Name, Geburtsdatum, ...) werden
- zu welchem **Zweck** (zB Newsletter) gespeichert und/oder
- an wen **übermittelt**? (Firma, Land, Zweck)
- **Widerrufsbelehrung**

- **Form:** schriftlich, elektronisch, mündlich, konkludent (bei nicht-sensiblen Daten) möglich; Schriftlichkeit empfohlen
- **Wichtig!** Einwilligung muss **freiwillig** sein – Kopplungsverbot beachten!

Beispiel 1 - Angebotslegung



Kunde

Bitte ein Angebot

Unternehmen

Daten für Angebotslegung
Name, Adresse, ...

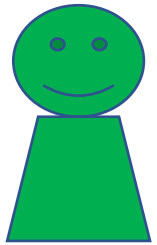
- ✓ Betriebliches Interesse
- ✓ „nur“ für Angebotserstellung

Angebot übermitteln

Angebot wird nicht angenommen

Daten werden gelöscht.
“Kunde“ wird vergessen.

Beispiel 1 - Angebotslegung



Kunde

Bitte ein Angebot

Daten für Angebotslegung
Name, Adresse, ...

Unternehmen

- ✓ Betriebliches Interesse
- ✓ „nur“ für Angebotserstellung

Angebot übermitteln

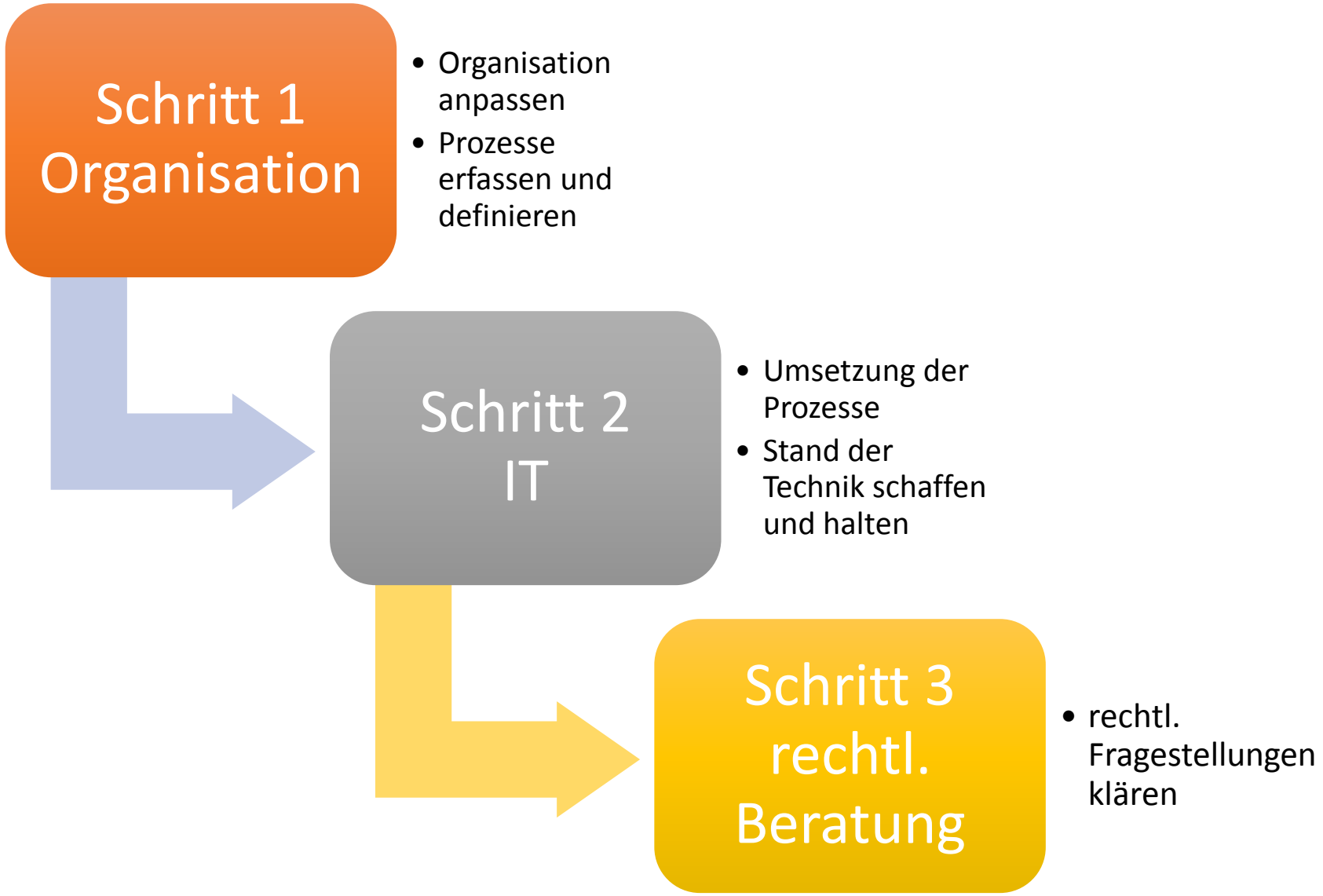
Angebot wird angenommen / Auftrag

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

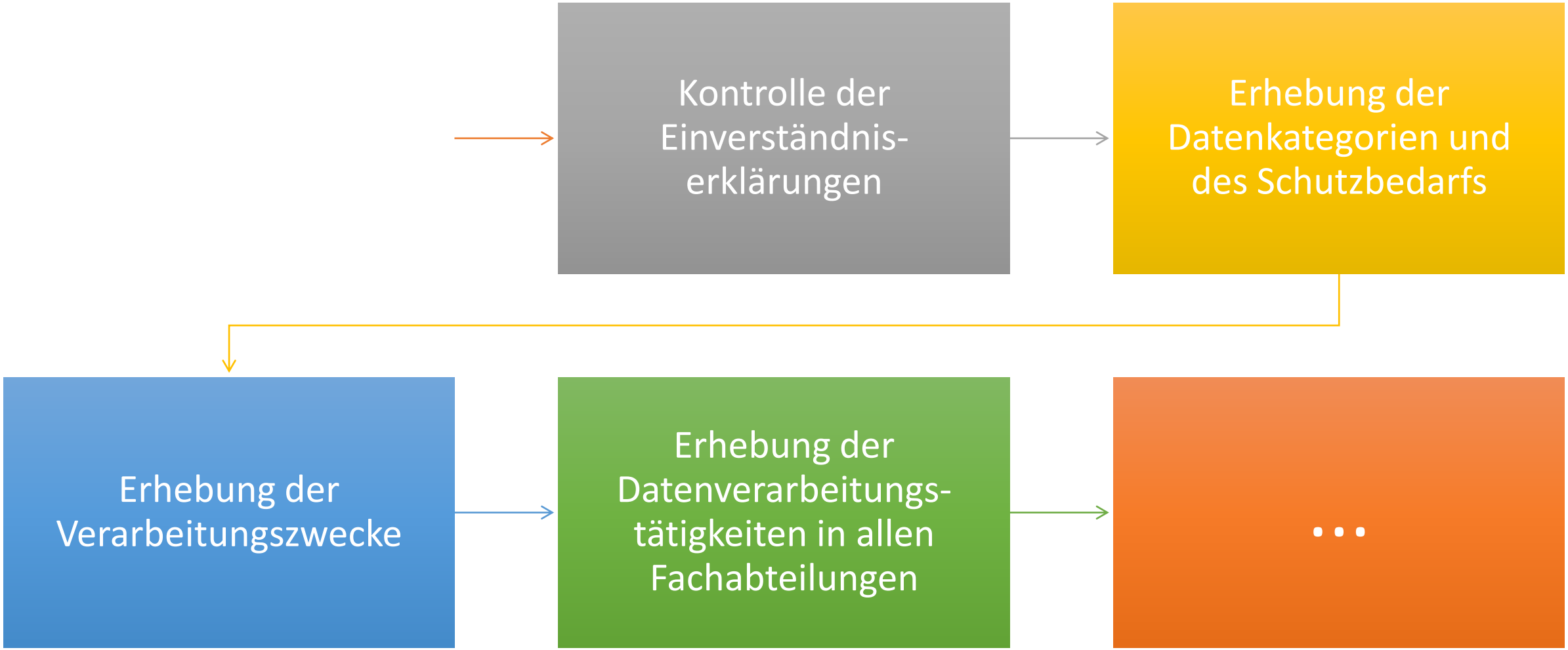
Was muss man tun?

- Verfahrensverzeichnis
- TOM – techn. org. Maßnahmen
- Löschen wann?
- Verträge mit Dritten (zB IT)
- MitarbeiterInnen Schulung / Verschwiegenheitsvereinbarungen

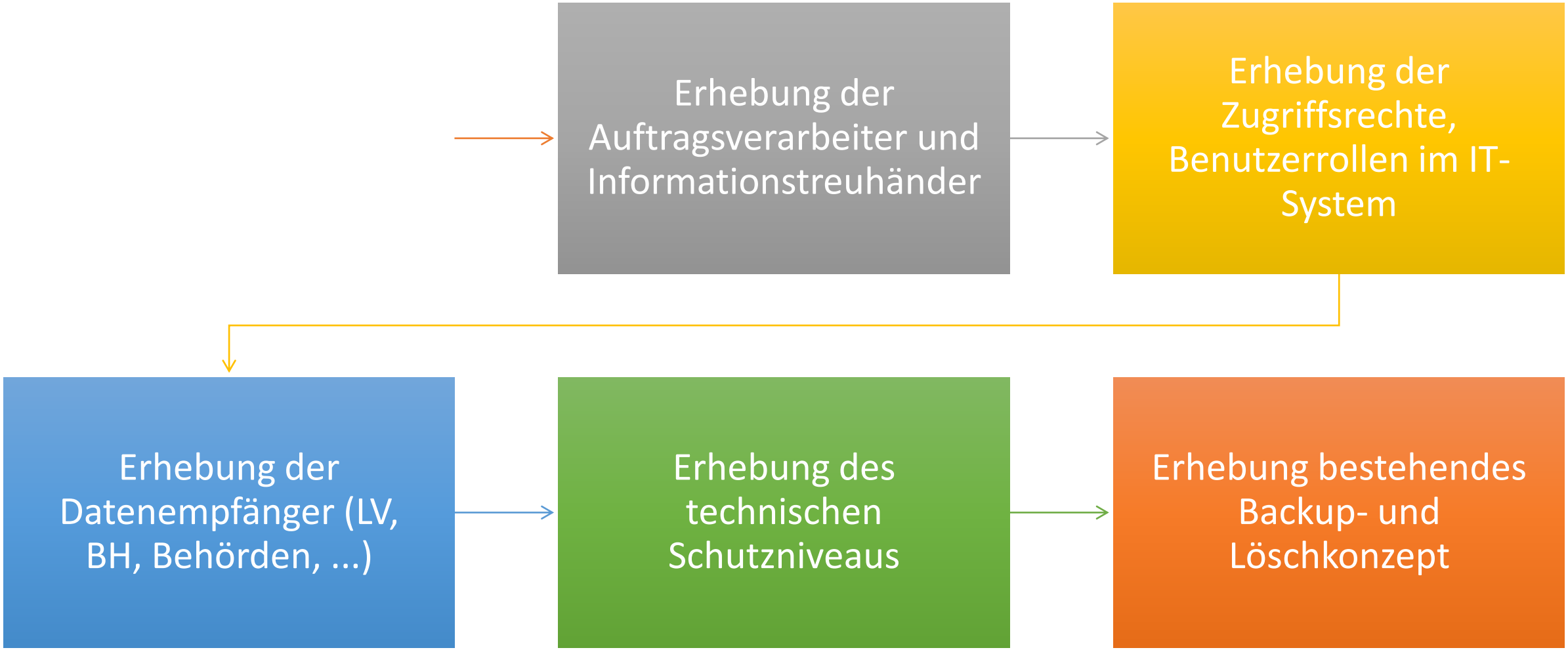
In 3 Schritten zum Ziel



DSGVO - Vorgehensweise



DSGVO - Vorgehensweise



Verfahrensverzeichnis Was ist zu tun?

- **Verzeichnis der Verarbeitungstätigkeiten:**
  - Wo und wie werden Daten erhoben (Datenquellen)
  - Wo und wie werden Daten gespeichert, verarbeitet (Verarbeitungssysteme)
  - Welche Kategorien von Daten werden verarbeitet
  - Daten von welchen Personengruppen werden verarbeitet
  - Zu welchem Zweck werden Daten verarbeitet
  - Wer hat Zugriff auf welche Daten
  - Backup- und Löschkonzept
  - Welche Dritte erhalten welche Daten zu welchem Zweck
- Folgenabschätzung bei Datenmissbrauch oder Datendiebstahl
- Beurteilung Notwendigkeit DSB (Datenschutzbeauftragter)

Was ist eine Verarbeitungstätigkeit

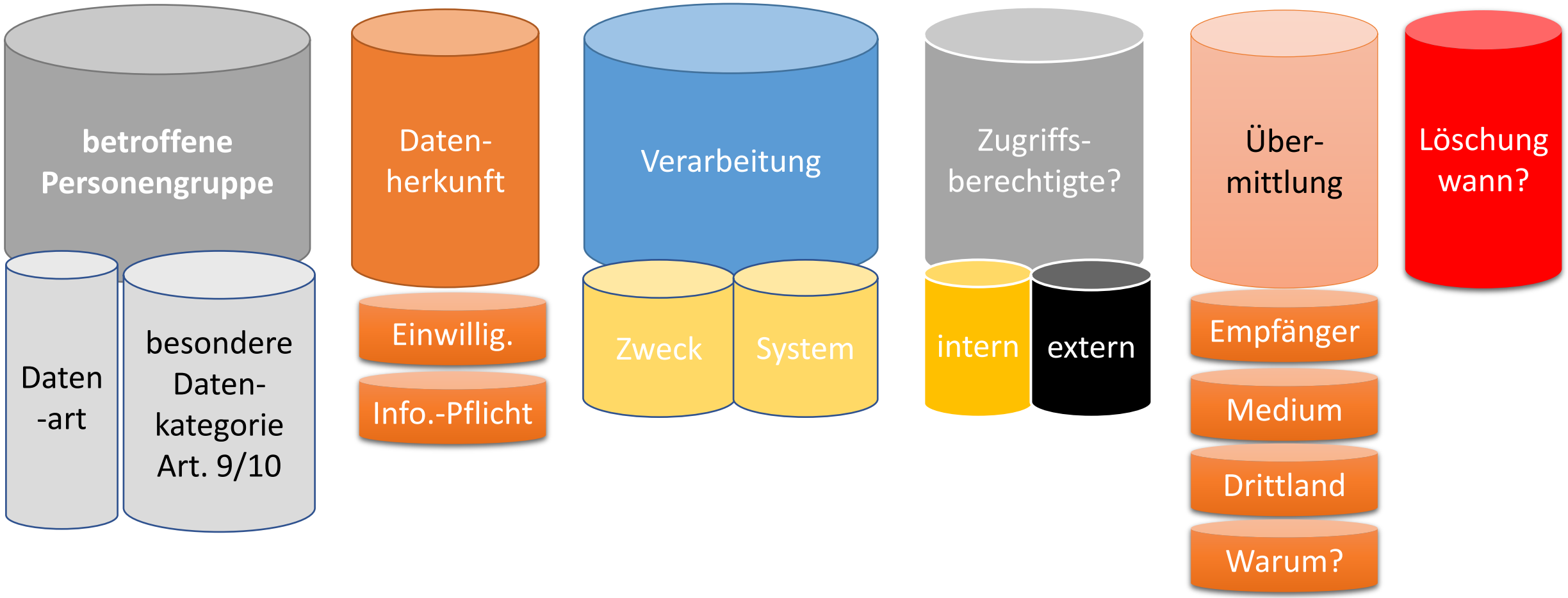
Eine "**Verarbeitungstätigkeit**" iSd Art 30 DSGVO ist die **Tätigkeit**, Verarbeitungen iSd Art 4 Z 2 DSGVO durchzuführen, und bezieht sich daher **nicht** auf **Applikationen** oder **Programme**, sondern auf konkrete **Abwicklungen** und **Vorgänge** beim **Verantwortlichen**, die **personenbezogene Daten verwenden.**

DAHER Phase 1:
Kein Thema der IT/Rechts-Abteilung

Mindest-Inhalt

- Beschreibung des Verantwortlichen / Dienstleisters
- Informationen zum Datenschutzbeauftragten
- Zweck der Verarbeitung
- Kategorien der betroffenen Personen
- Kategorien der personenbezogenen Daten
- Kategorien der Empfängerkreise
- Löschungsroutine
- Beschreibung TOM

Beispiel Verfahrensverzeichnis einfach



Erhebungsgrundlage?
gesetzliche Vorgabe / Vertragserfüllungsnotwendigkeit / berechtigtes Interesse / Einwilligung

“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.

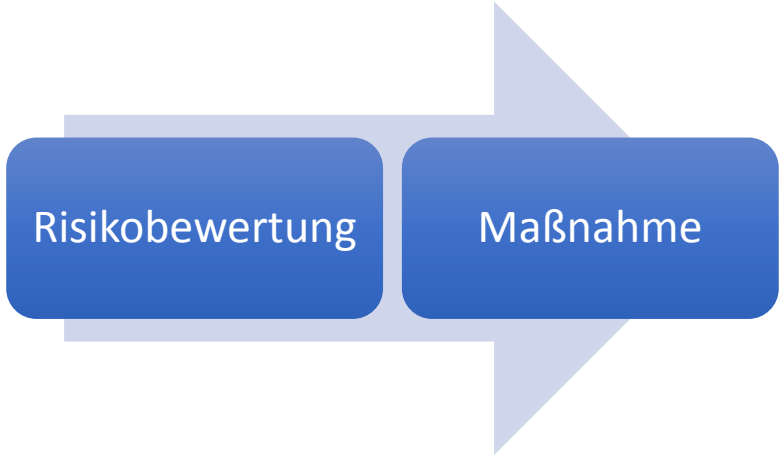
DAHER:
Backup-Konzept erstellen!

“geeignete“ TOM – techn. und org. Maßnahmen

Unter Berücksichtigung

- des Stands 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

Datensicherheitsmaßnahmen (§54 DSG)



- Zugangskontrolle
- Datenträgerkontrolle
- Speicherkontrolle
- Benutzerkontrolle
- Zugriffskontrolle
- Übertragungskontrolle
- Eingabekontrolle
- Transportkontrolle
- Wiederherstellung
- stabiles System

Informationspflichten

...des Verantwortlichen gegenüber der betroffenen Person

Zeitpunkt: Erhebung der personenbezogenen Daten

Inhalt:

- Name und Kontaktdaten des Verantwortlichen und Datenschutzbeauftragten
- Verarbeitungszwecke
- Datenempfänger (ggf. Empfänger im Drittland)
- Speicherdauer bzw. Kriterien zur Bestimmung
- Rechtsgrundlage für die Verarbeitung
- Betroffenenrechte
- Beschwerderecht
- Widerrufsmöglichkeit der Einwilligungserklärung

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)

Auskunftsrecht

Störfall tritt ein

Risiko für Rechte und Freiheit natürlicher Personen

Verantwortlicher

72h

Meldung an Aufsichts-behörde

Verarbeiter

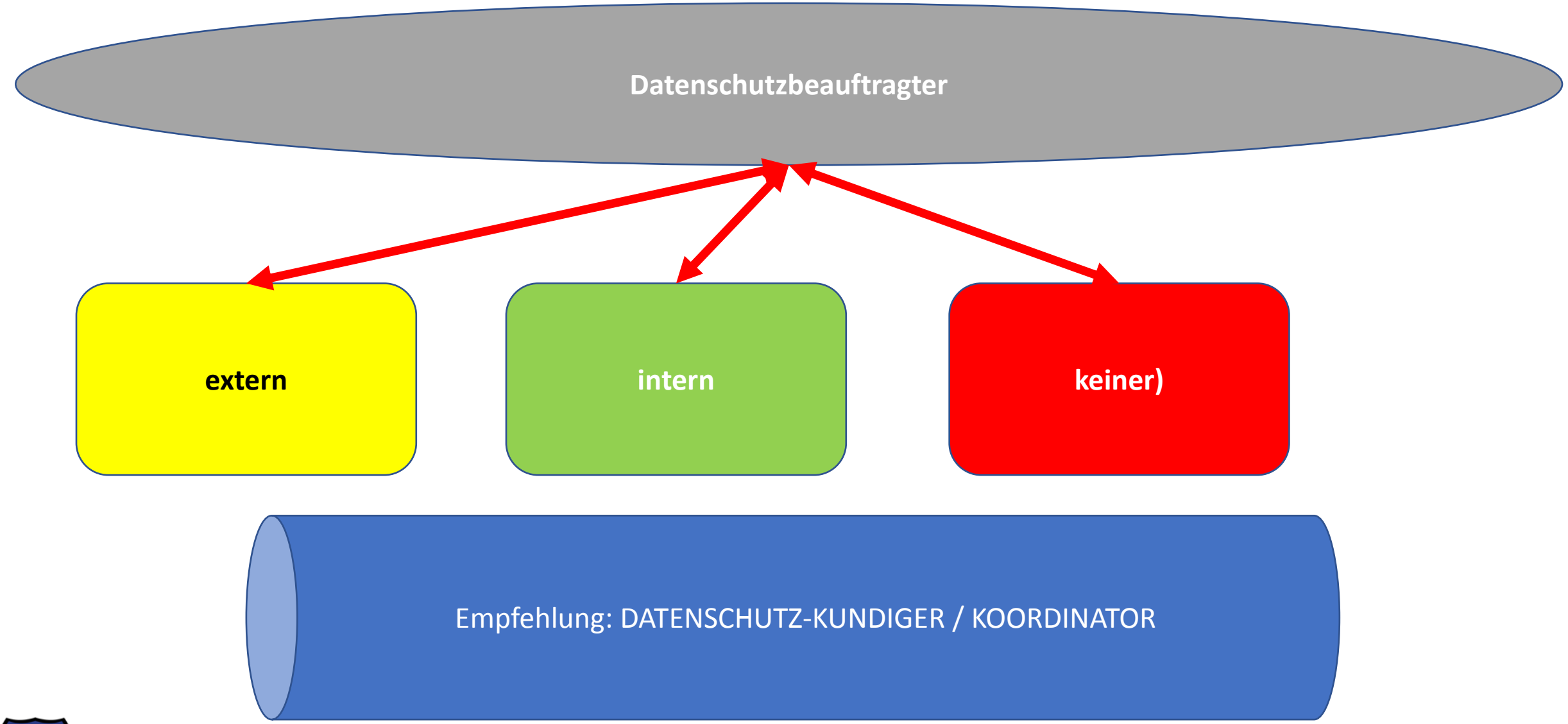
unverzüglich

Verantwortlichen

- Art der Schutzverletzung
- Personenkategorie
- Anzahl betroffener Personen
- Name + Kontaktdaten DSB
- Folgenbeschreibung
- Behebungsmaßnahmen
- Abmilderungsmaßnahmen

entdeckt

Der Datenschutzbeauftragte



Der Datenschutzbeauftragte

verpflichtend **vs** freiwillig

- darf nicht abberufen oder benachteiligt werden (Kündigung erlaubt)
- Eingliederung in Arbeitsablauf, Ressourcenallokation
- Beratung der Beteiligten
- Überwachung (insb Datenfolgeabschätzung)
- Anlaufstelle für Aufsichtsbehörde

- angestellt vs externer Dienstleister (Auswahlverschulden)
- Haftung / zulässiger Haftungsausschluss
- weisungsfrei

Fazit – Was braucht man mindestens?

WK hilft

Förderung für:
WIFI-Kurse
Beratungen (Fokus C) von certified Data & IT Security Experts

50% bis max € 1.000,--

Online Hilfestellungen und Tipps:
wko.at/datenschutz

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

Ihre Ansprechpartnerin:
Mag. Tamara Charkow

Quelle: WKÖ Informationsfolder Juni 2017

Ihre Datenschutz-Experten

DI Gerald KORTSCHAK und DI(FH) Harald SCHENNER
+43 316 71 39 48
+43 676 84 17 13 19
www.sevian7.com
www.dsgvo2018.at
office@sevian7.com

CERTIFIED DATA & IT SECURITY EXPERT

Wir weisen ausdrücklich darauf hin, dass es sich bei den vorliegenden Unterlagen um ein unentgeltliches Service der sevian7 IT development GmbH handelt und die Informationen keine Unternehmensberatung darstellen. Jegliche Haftung für die Aktualität, Richtigkeit und Vollständigkeit der dargestellten Informationen wird ausgeschlossen.

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.