CERTIFIED DATA & IT SECURITY EXPERT

:get know howww

WKO Unternehmensberatung · Buchhaltung · IT STEIERMARK

Verfasser: Harald Schenner, Gerald Kortschak

Thema: Vorgehensweise, Verfahrensverzeichnis, Folgenabschätzung

Ablauf 13:30 – 16:30

CERTIFIED DATA & IT SECURITY EXPERT

:get know howww

- Begrüßung
  - Fachgruppenobmann Dominic Neumann, MBA
- Fragebogen-Auswertung und Einweisung in Gruppen
  - DI(FH) Harald Schenner, CMC und DI Gerald Kortschak, CMC
- Vertragsimplikationen
  - Rechtsanwalt MMag. Dr. Rainer Beck

- DI(FH) Harald Schenner, CMC und DI Gerald Kortschak, CMC
  - 1: Grundlagen und Vorgehensweise zur DSGVO
  - 2: Workshop Verfahrensverzeichnis

- Abschluss

CERTIFIED
DATA & IT SECURITY
EXPERT

:get know howww

Strengere Verpflichtungen für Unternehmen

DIE PFLICHTEN für Unternehmen

INFORMATIONSPFLICHT UND RECHTE VON BETROFFENEN PERSONEN	PFLICHT ZUR DATENSCHUTZ-FOLGENABSCHÄTZUNG	UNTERNEHMER MÜSSEN MELDUNG MACHEN
1 Monat	**Folgenabschätzung**	**72 Stunden**

Quelle: WKÖ Informationsfolder Juni 2017

FAKTEN

CERTIFIED DATA & IT SECURITY EXPERT

:get know howww

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.

MAI 2018

20 Mio.

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

Vertragsimplikationen

CERTIFIED DATA & IT SECURITY EXPERT

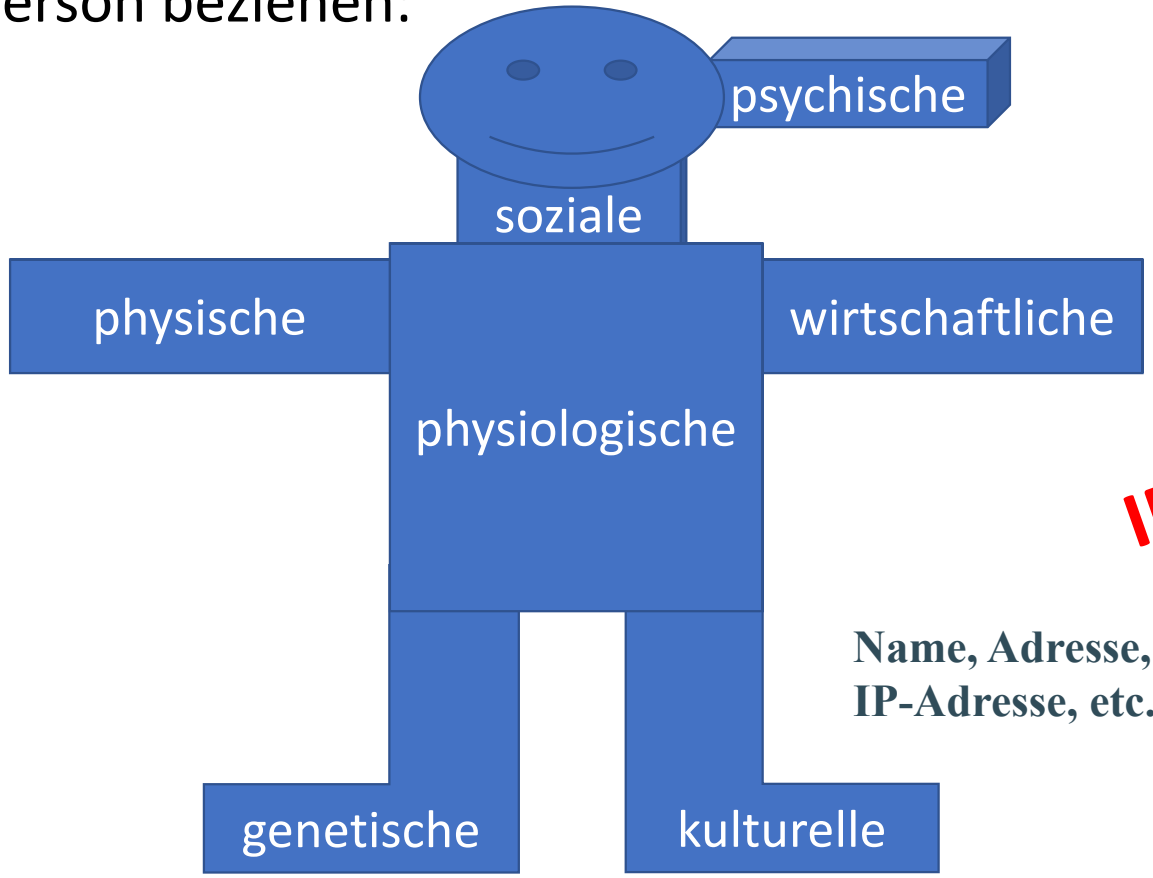
:get know howww

- Rechtsanwalt MMag. Dr. Rainer Beck

Um welche Daten geht es (Art. 4, Abs. 1)?

CERTIFIED DATA & IT SECURITY EXPERT

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



IDENTITÄT

Name, Adresse, Geburtsdatum, Bankdaten, IP-Adresse, etc.

:get know howww

SENSITIVE DATA

rassische Herkunft

ethnische Herkunft

genetische & biometrische Daten

Gesundheits -daten

Gewerkschafts -zugehörigkeit

politische Meinung

Religion

sexuelle Orientierung

Weltanschaung

DSGVO – Rechte der betroffenen Personen

CERTIFIED DATA & IT SECURITY EXPERT

:get know howww

- 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)

DSGVO - Vorgehensweise

CERTIFIED DATA & IT SECURITY EXPERT

:get know howww

Erhebung der Datenquellen → Kontrolle der Einverständniserklärungen → Erhebung der Datenkategorien und des Schutzbedarfs → Erhebung der Verarbeitungszwecke → Erhebung der Datenverarbeitungstätigkeiten in allen Fachabteilungen → ...

DSGVO - Vorgehensweise

CERTIFIED DATA & IT SECURITY EXPERT

:get know howww

...

Erhebung der Auftragsverarbeiter und Informationstreuhänder

Erhebung der Zugriffsrechte, Benutzerrollen im IT-System

Erhebung der Datenempfänger (LV, BH, Behörden, ...)

Erhebung des technischen Schutzniveaus

Erhebung bestehendes Backup- und Löschkonzept

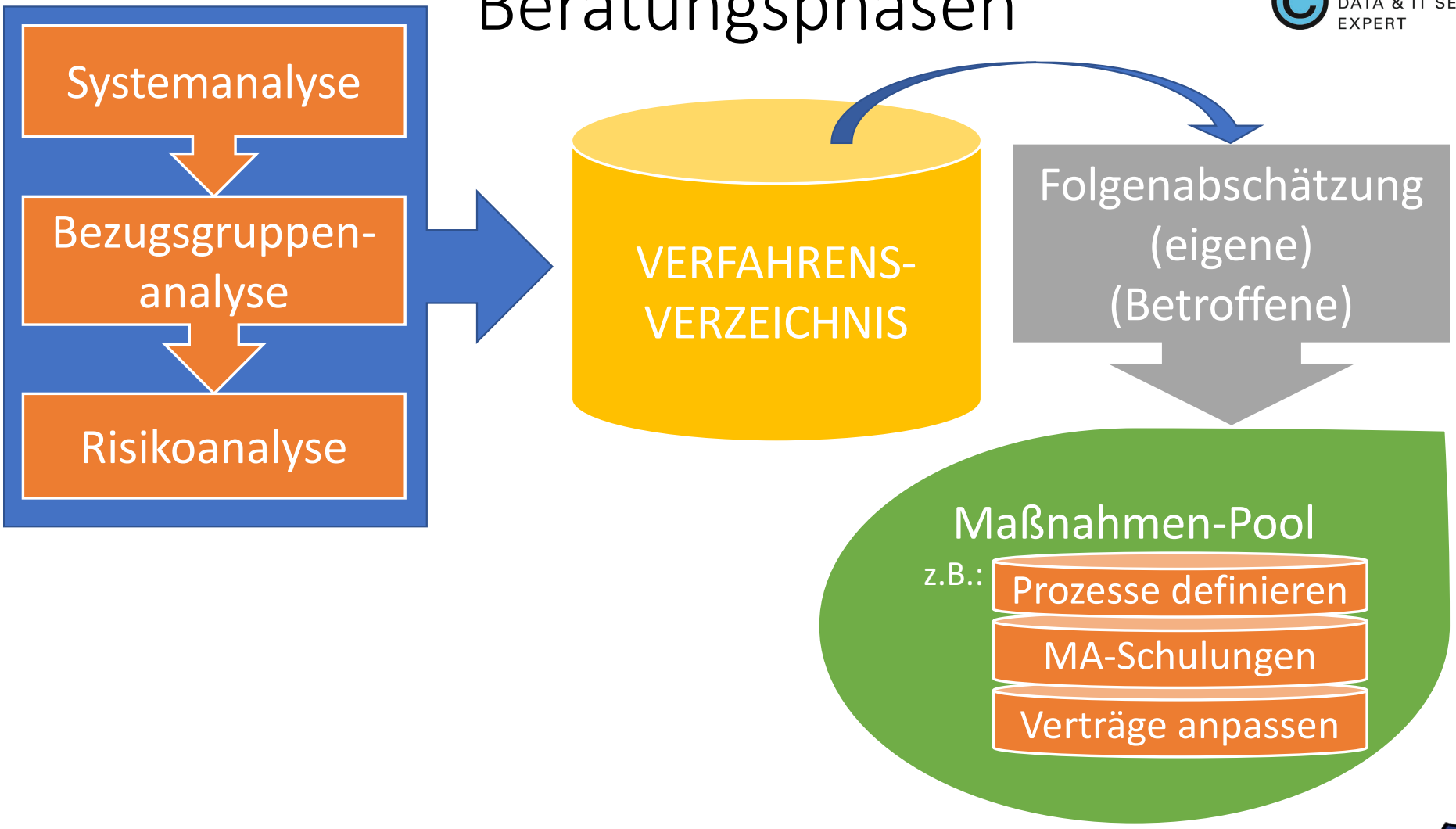
Was braucht man mindestens?

CERTIFIED DATA & IT SECURITY EXPERT

:get know howww

- Verfahrensverzeichnis
- Prozess Meldung Datenschutzverstöße
- Prozess Informationsbegehren
- Prozesse Betroffenenrechte
- Etwaige Folgenabschätzungen
- Verträge / Einwilligungserklärungen anpassen
- Nachweis der Datensicherheit

Beratungsphasen



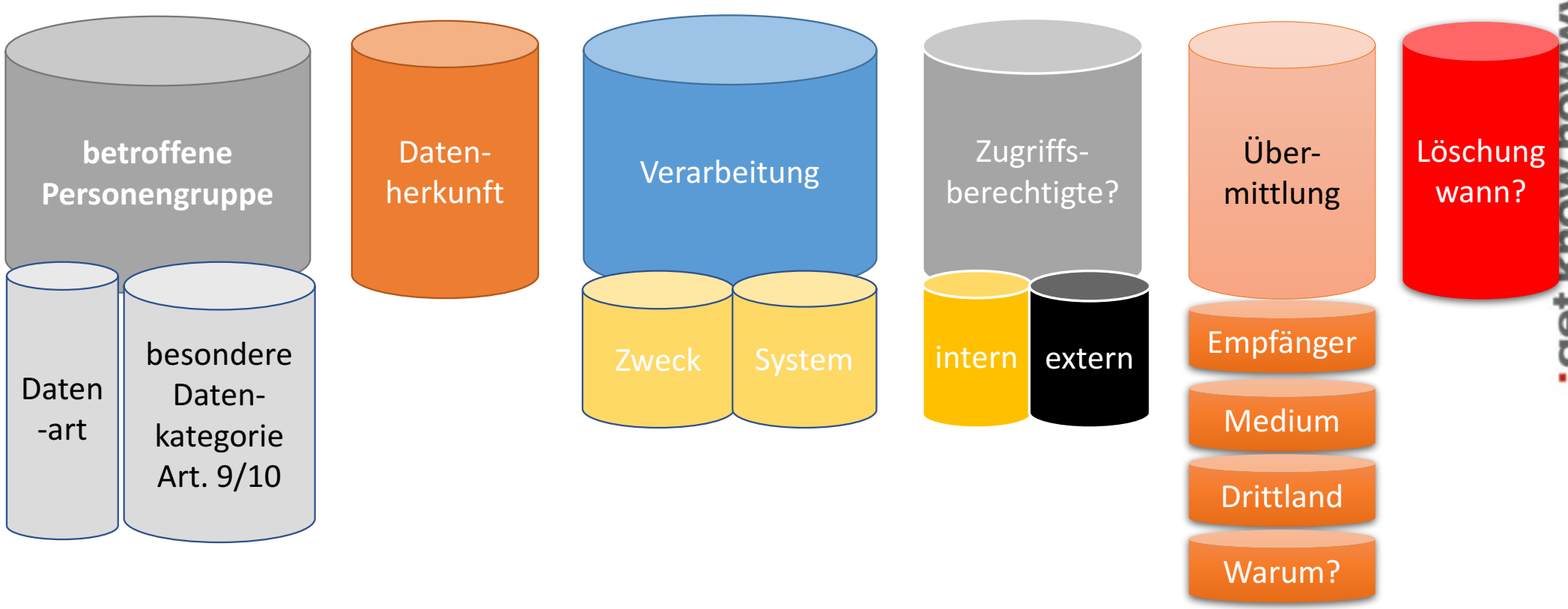
CERTIFIED DATA & IT SECURITY EXPERT

:get know howww

Beispiel Verfahrensverzeichnis einfach

CERTIFIED DATA & IT SECURITY EXPERT

:get know now www



Erhebungsgrundlage?
gesetzliche / Einwilligung

Störfall tritt ein

CERTIFIED DATA & IT SECURITY EXPERT

:get know howww

Risiko für Rechte und Freiheit natürlicher Personen (Art. 33)

Verantwortlicher → **72h** → Meldung an Aufsichts-behörde

Verarbeiter → **unverzüglich** → Verantwortlichen

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

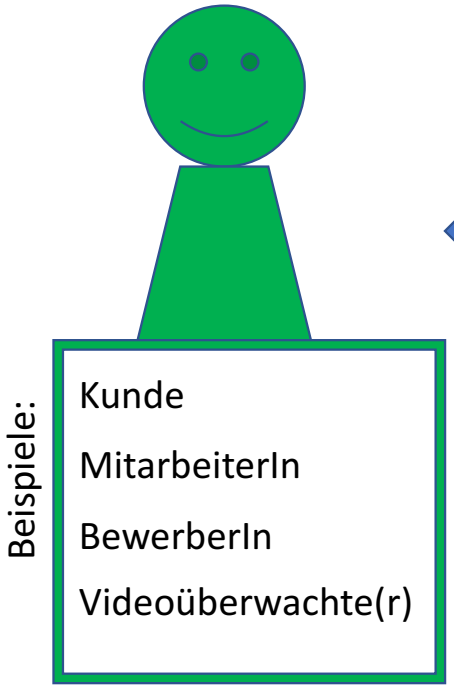
entdeckt

Betroffene Person (Art. 34)

Auskunftsrecht (Art. 15)

CERTIFIED DATA & IT SECURITY EXPERT

:get know howww



Welche Daten?

Informationsbegehren

Verant-
wortlicher

Antwort innerhalb 4 Wochen

Verfahrens-
verzeichnis

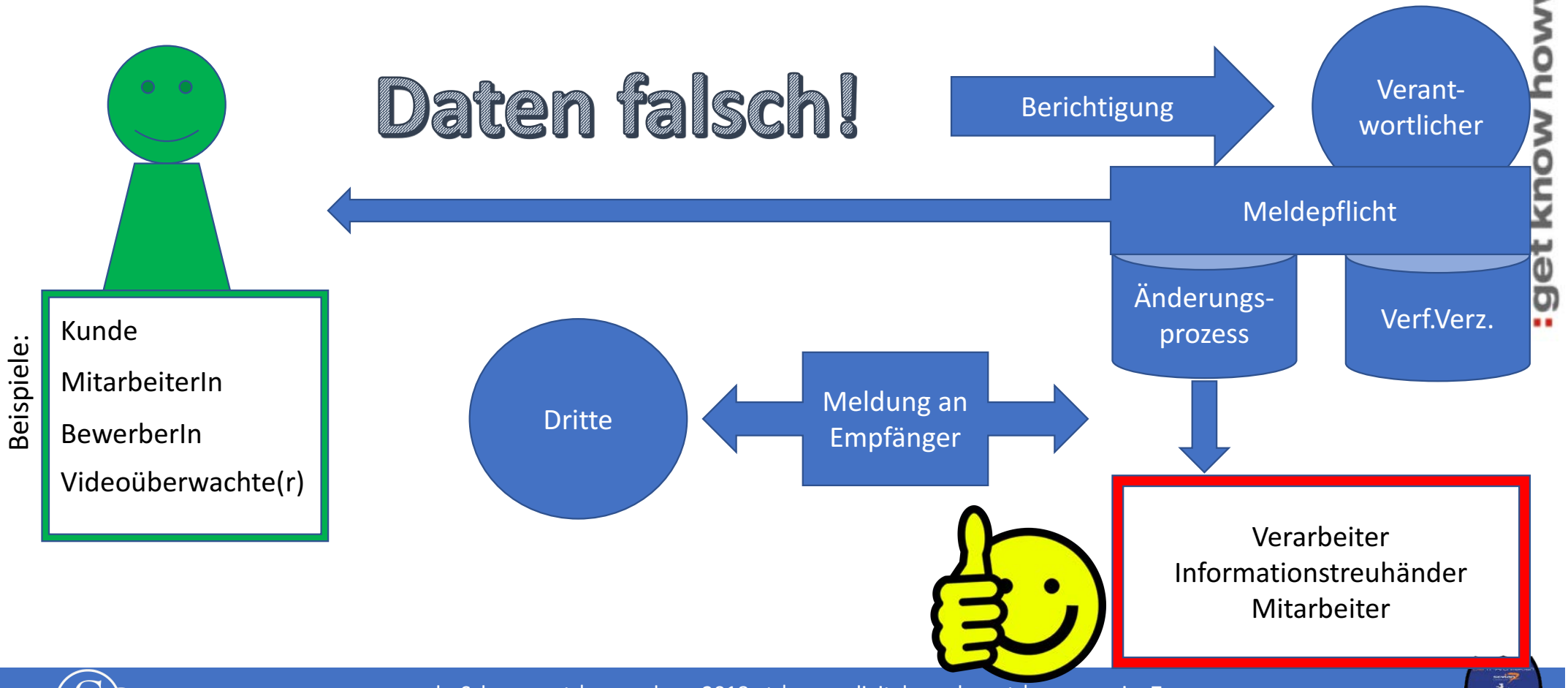
Auskunfts-
prozess

Grundlage Gesetz / explizite Einwilligung

Berichtigung (Art. 16)

CERTIFIED DATA & IT SECURITY EXPERT

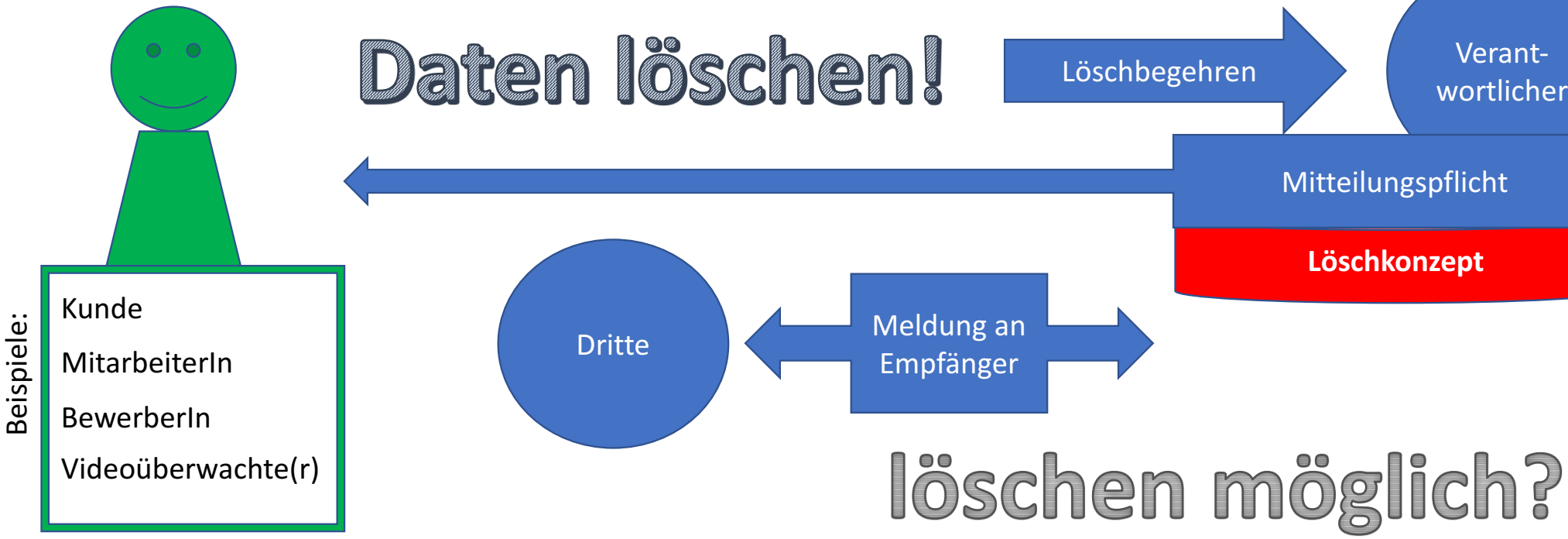
:get know howww



Recht auf Vergessenwerden (Art. 17)

CERTIFIED DATA & IT SECURITY EXPERT

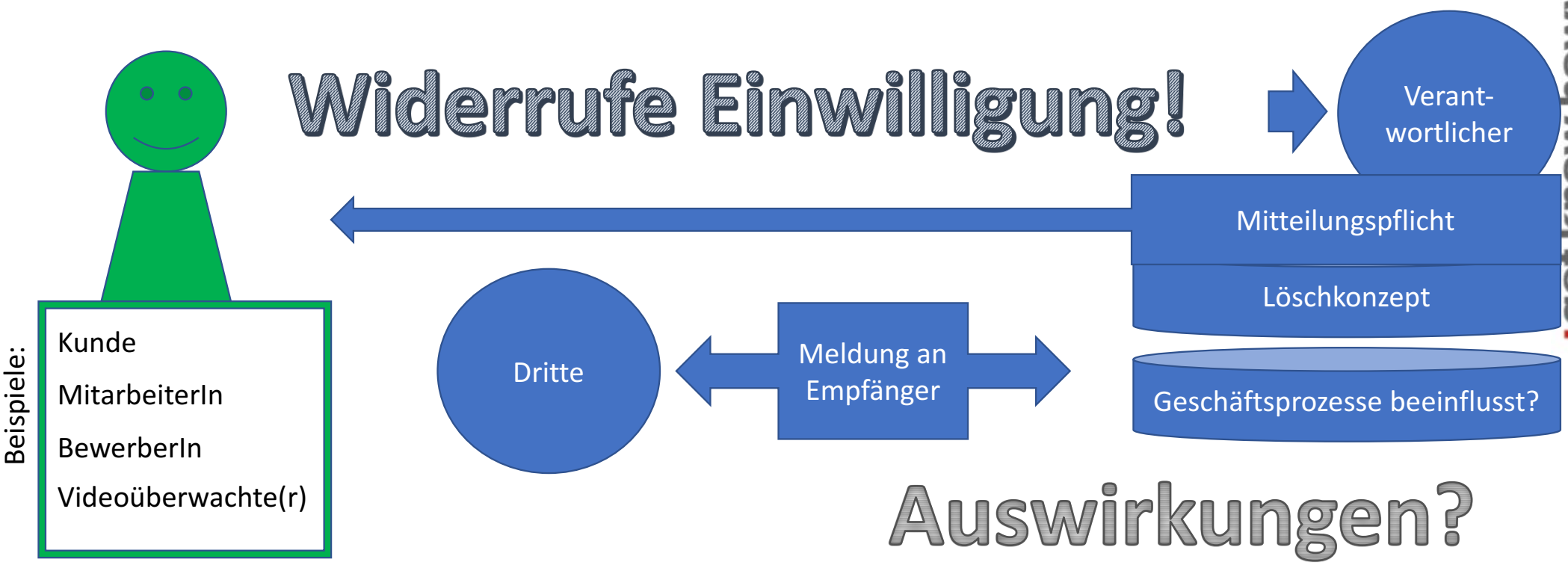
:get know howww



Widerruf / Widerspruch (Art. 21)

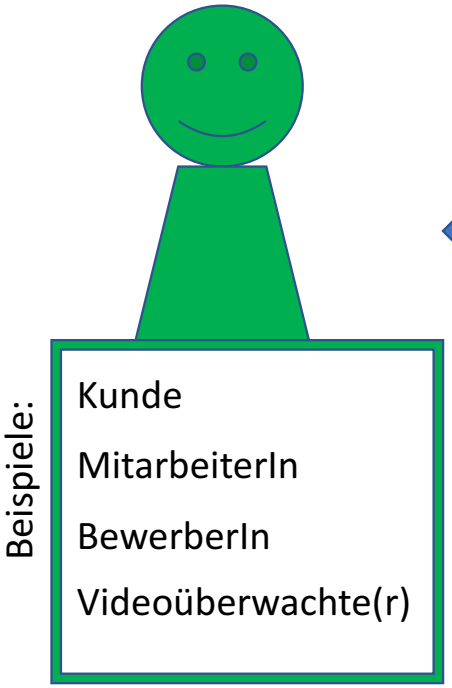
CERTIFIED DATA & IT SECURITY EXPERT

:get know howww



Einschränkung (Art. 18)

CERTIFIED DATA & IT SECURITY EXPERT



Einschränkung

der Verarbeitung

Verant-
wortlicher

Mitteilungspflicht

Löschkonzept

Dritte

Meldung an
Empfänger

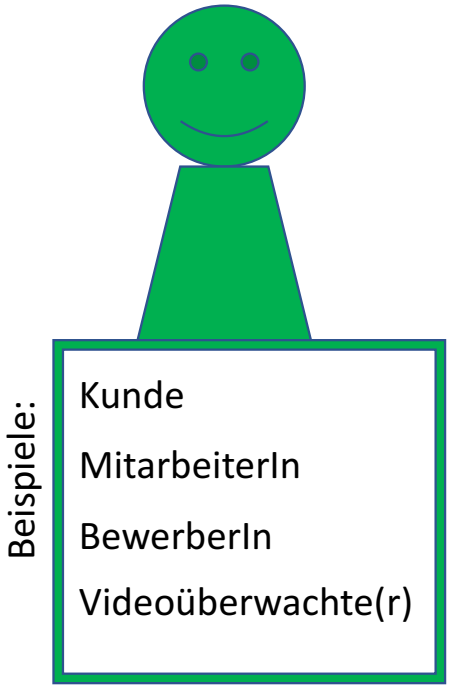
Eingeschränkte oder keine Nutzung?

:get know howww

Datenübertragbarkeit (Art. 20)

CERTIFIED DATA & IT SECURITY EXPERT

:get know howww



Übertragen

Datenübertragbarkeit

Verant-
wortlicher

strukturiertes, gängiges und maschinenlesbares Format

Übermittlung

Folgenabschätzung, wenn ... (Art. 35, Abs. 1+3)

CERTIFIED DATA & IT SECURITY EXPERT

:get know howww

- Wenn voraussichtlich hohes Risiko für Rechte und Freiheiten natürlicher Personen aufgrund
  - Art,
  - Umfang,
  - Umstände und
  - Zwecke der Verarbeitung
- Insbesondere, wenn
  - Automatisierte systemische, umfassende Bewertung (inkl. Profiling) als Grundlage für Entscheidungen
  - Unfangreiche Verarbeitung bes. Kategorien (Art. 9 + 10)
  - Systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche

Folgenabschätzung, wie... (Art. 35, Abs. 7)

CERTIFIED DATA & IT SECURITY EXPERT

:get know howww

- Die Folgenabschätzung enthält zumindest
  - Systematische Beschreibung der Verarbeitungsvorgänge und Zwecke der Verarbeitung, verfolgte berechtigte Interessen des Verantwortlichen
  - Bewertung der Notwendigkeit + Verhältnismäßigkeit in Bezug auf den Zweck
  - Bewertung der Risiken für Rechte und Freiheiten der betroffenen Personen
  - Zur Bewältigung der Risiken geplante Abhilfemaßnahmen, Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sicher gestellt wird
  - ...

Ihre Datenschutz-Experten

CERTIFIED DATA & IT SECURITY EXPERT

DER SCHENNER Consulting & Training

Die IT-Architekten

sevian7 e pluribus unum

>> www.sevian7.com

:get know howww

Ing. Dipl.-Ing.(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

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.