DIE NEUE EU-DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO) UND IHRE AUSWIRKUNGEN AUF SCHWEIZER UNTERNEHMEN, INSB. TREUHÄNDER

KLAUS KROHMANN
Anlass der EXPERTsuisse
18. April 2018

BDO

REFORM DES EU-DATENSCHUTZES

REFORM DES EU-DATENSCHUTZES

Entwicklung der Datenmengen

400 h Videoupload / Minute

205 Milliarden Mails / Tag

enthält 5.35 Millionen Artikel

217 neue Internetteilnehmer / Minute

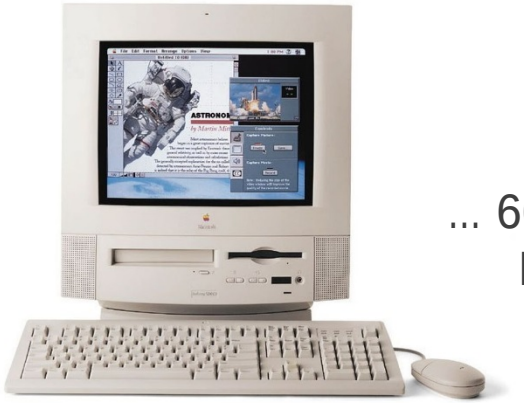
50 Milliarden Connected Devices in 2020

REFORM DES EU-DATENSCHUTZES

EU-Datenschutzrichtlinie 1995 / DSG 1994

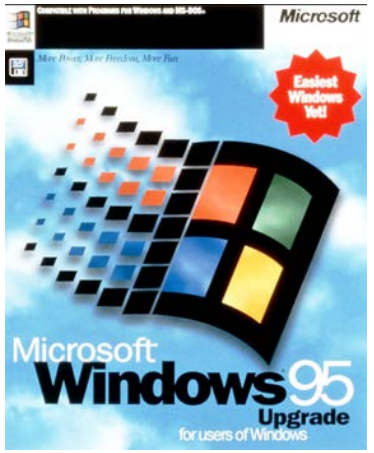
Im gleichen Jahr…

… Siemens S3 mit SMS …



… 66MHz Prozessor und 80 MB Festplatten…

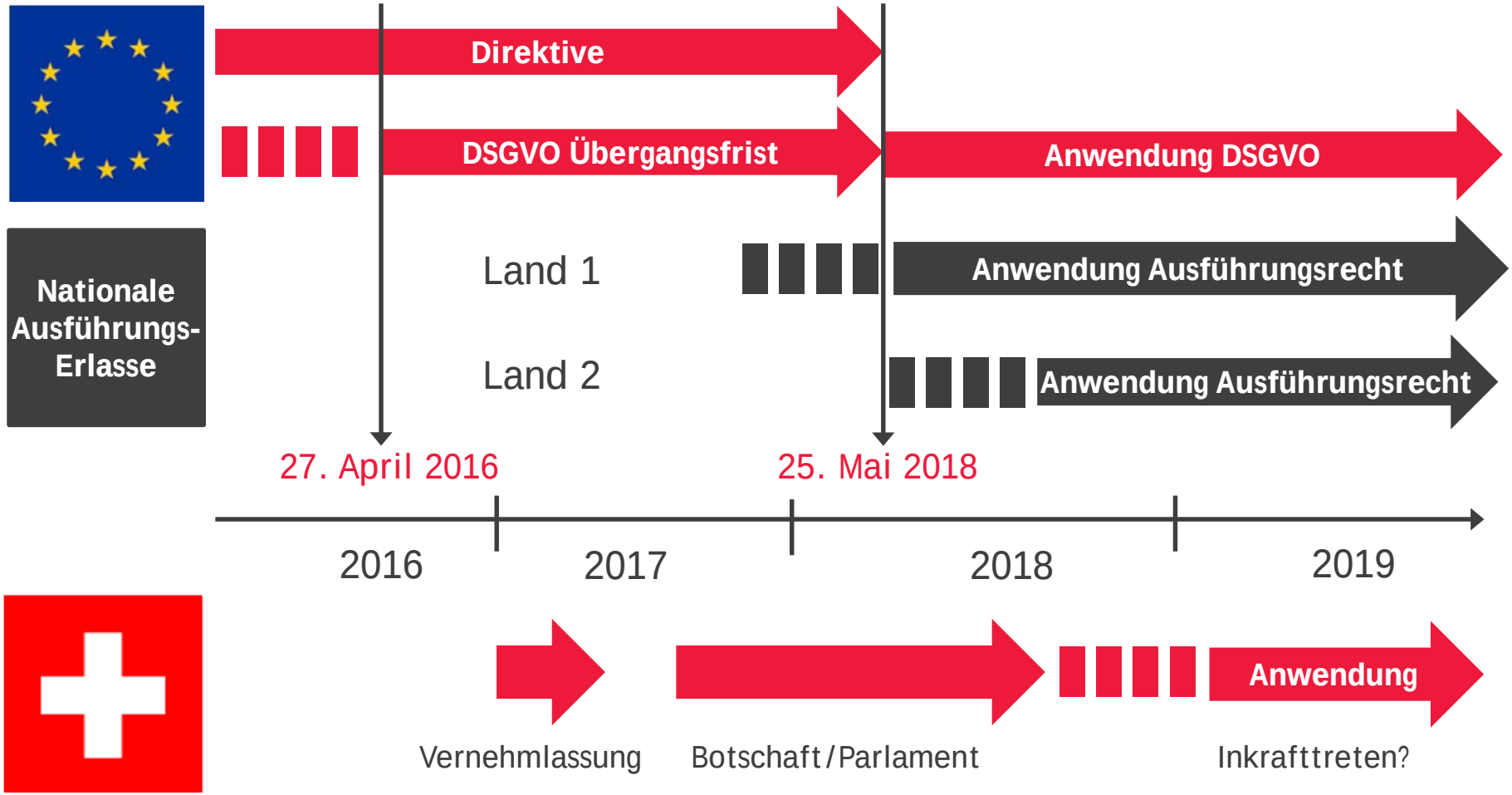
… Windows 95 …



DVD TM

REFORM DES EU-DATENSCHUTZES

Status der Gesetzesentwicklung



WAS IST NEU?

WAS IST NEU?

Neuerungen der DSGVO

- **Direkte Verbindlichkeit für die ganze EU**
  Gleiche Gesetzesnormen für alle direkt anwendbar; jedoch mit Möglichkeit für länderspezifische Öffnungsnormen

- **Strengere Bussgelder**
  bis 4% des weltweiten Jahresumsatzes des ganzen Konzerns, mind. EUR 20 Mio.!

- **Dokumentationspflichten**
  Insbesondere aus neuen Prinzipien der «Accountability» und «Privacy by design»

- **Meldepflicht von Verletzungen**
  «Incident Reporting» innerhalb von 72 Stunden

WAS IST NEU?

... und das auch noch...

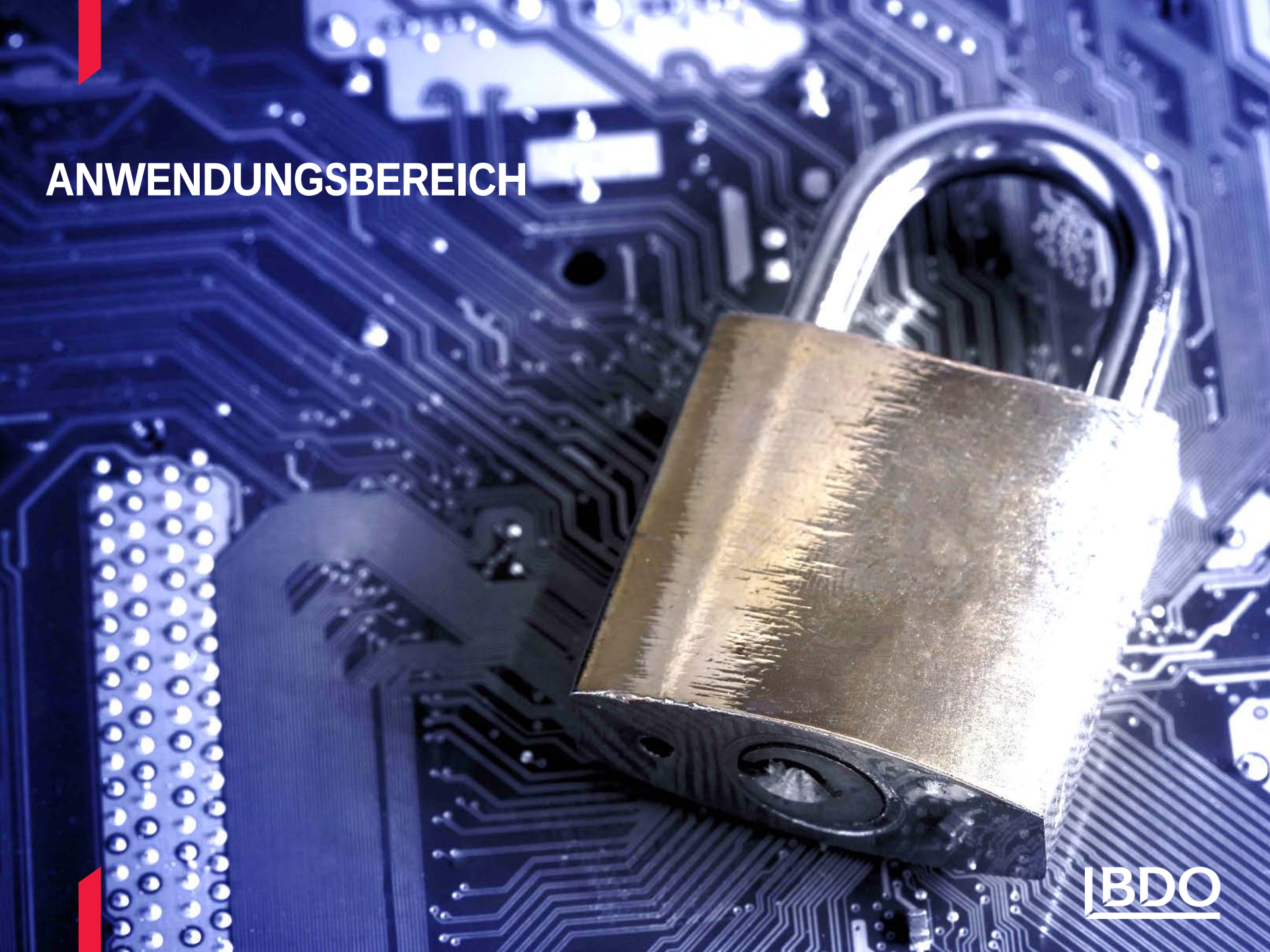
- **Recht auf «Vergessenwerden»**
  Vorschiften und zur Pflicht zur Löschung
- Recht auf Datenherausgabe
- Erweiterte Kompetenzen der Aufsichtsbehörden
- Beschränkte Pflicht für Einsetzung eines betrieblichen Datenschutzverantwortlichen
- Abschaffung formalistischer Meldepflichten
- Abschaffung des Schutzes von Daten juristischen Personen (für Österreich)

WAS IST NEU?

Was plant die Schweiz?

- **Neu Bussgelder**
  bis zu CHF 250’000
- **Dokumentationspflichten**
  Insbesondere bei der Datenschutz-Folgeabschätzung
- **Meldepflicht von Verletzungen**
  Unbefugte Datenbearbeitung muss so rasch als möglich gemeldet werden
- **Recht auf Löschung**
- Erweiterte Kompetenzen der Aufsichtsbehörden
- Möglichkeit zur Einsetzung eines Datenschutzberaters
- Andere Meldepflichten
- Abschaffung des Schutzes von Daten juristischen Personen

ANWENDUNGSBEREICH



ANWENDUNGSBEREICH

Räumlicher Anwendungsbereich

Anwendung auf die Verarbeitung personenbezogener Daten im Rahmen der Tätigkeit

- eines **Verantwortlichen** mit Niederlassung in der EU
- eines **Auftragsverarbeiters** mit Niederlassung in der EU

und zwar unabhängig davon, ob die Verarbeitung in der EU oder nicht stattfindet.

ANWENDUNGSBEREICH

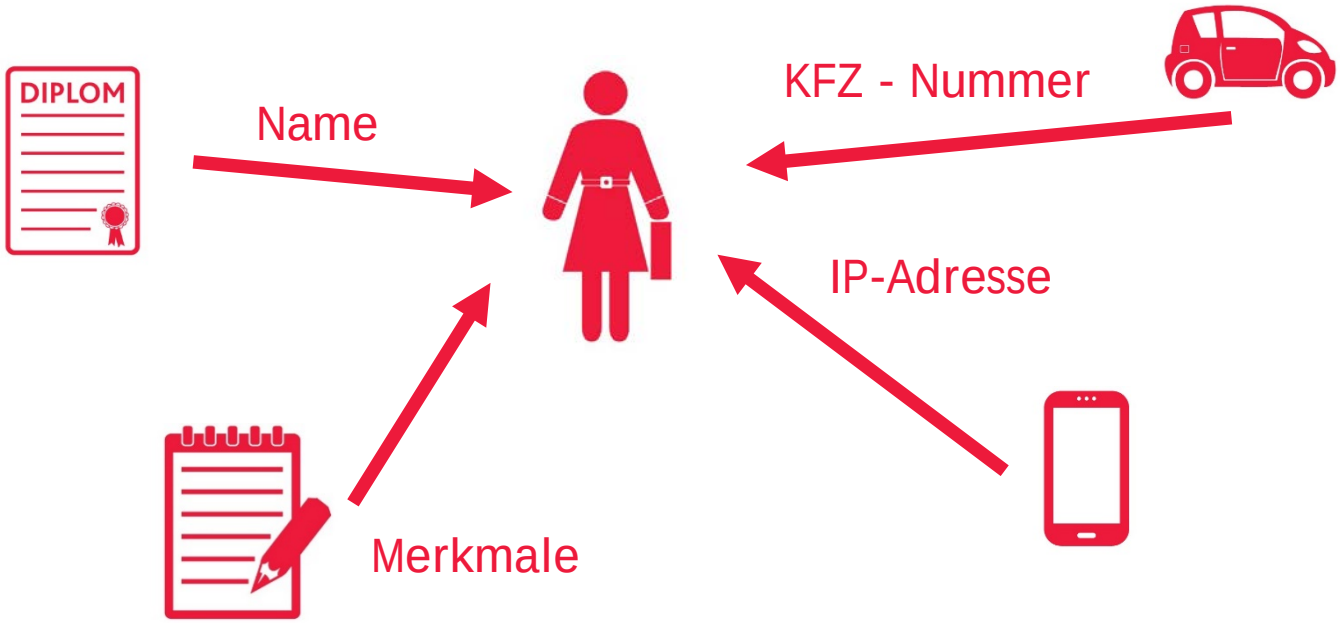
Extraterritorialer Anwendungsbereich

WICHTIGE BEGRIFFE

WICHTIGE BEGRIFFE

Personenbezogene Daten

Informationen, die sich auf eine identifizierbare natürliche Person («betroffene Person» [*Data Subject*] genannt) beziehen



WICHTIGE BEGRIFFE

Verarbeitung...

...ist jeder - mit oder ohne Hilfe automatisierter Verfahren - ausgeführter Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie

- das Erheben,
- das Erfassen,
- die Organisation,
- das Ordnen,
- die Speicherung,
- die Verwendung,
- das Auslesen,
- das Abfragen,
- die Anpassung oder Veränderung, die Offenlegung durch Übermittlung,
- Verbreitung oder eine andere Form der Bereitstellung,
- den Abgleich oder die Verknüpfung,
- die Einschränkung,
- das Löschen oder
- die Vernichtung.

WICHTIGE BEGRIFFE

Besondere Kategorien [SPECIAL CATEGORIES]

Die Verarbeitung personenbezogener Daten, aus denen

- die rassische und ethnische Herkunft,
- politische Meinungen,
- religiöse oder weltanschauliche Überzeugungen oder
- die Gewerkschaftszugehörigkeit

hervorgehen sowie die Verarbeitung von

- genetischen Daten,
- biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person,
- Gesundheitsdaten oder
- Daten zum Sexualleben oder der sexuellen Orientierung

einer natürlichen Person ist untersagt.

Nationales Recht kann weitere Kategorien definieren.

WICHTIGE BEGRIFFE

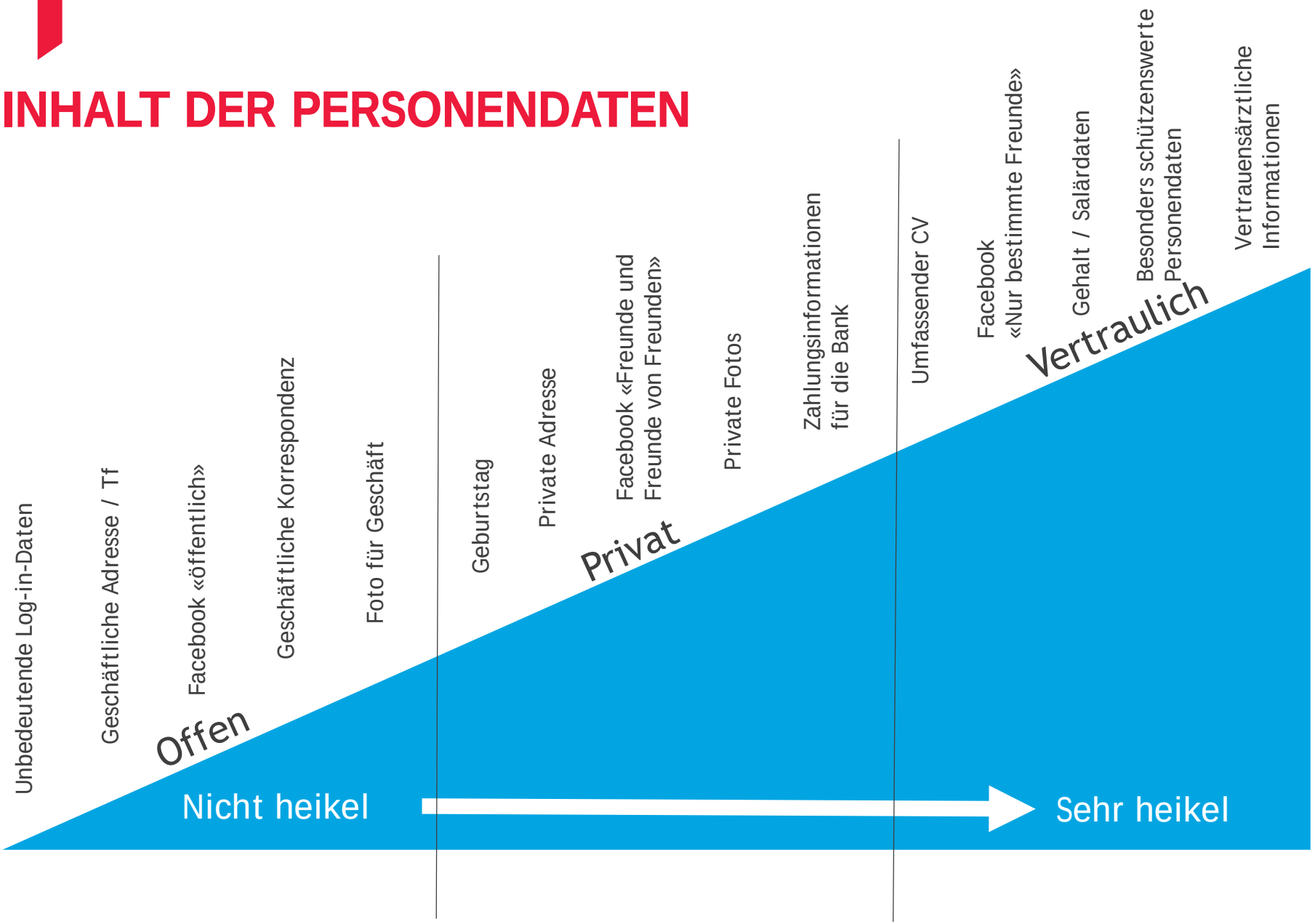
Besonders Schützenswerte Personendaten

Besonders schützenswerte Personendaten:

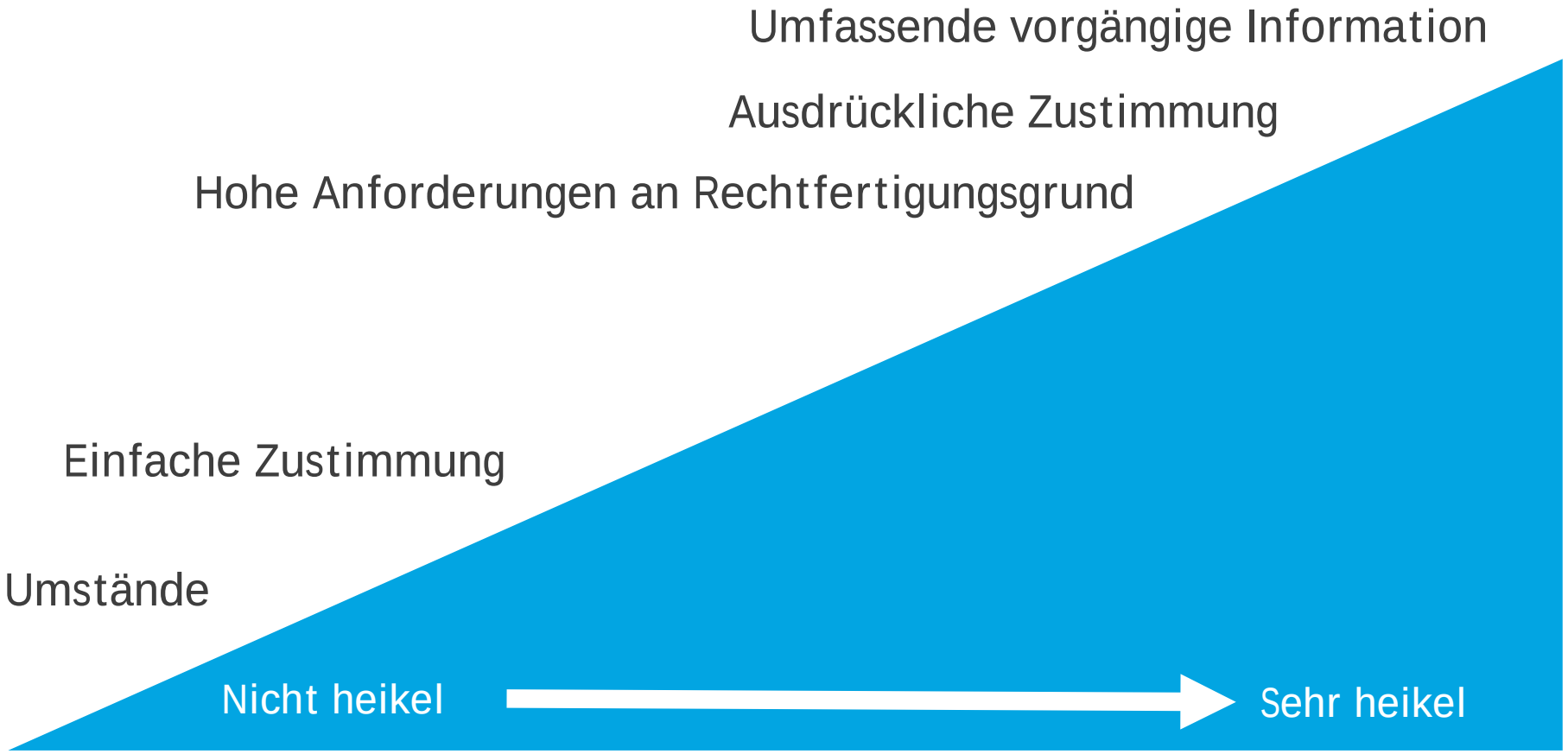
- die rassische und ethnische Herkunft
- politische Meinungen
- religiöse oder weltanschauliche Überzeugungen oder
- die Gewerkschaftszugehörigkeit
- genetischen Daten,
- biometrischen Daten zur Identifizierung einer natürlichen Person,
- Gesundheitsdaten oder
- Daten über die Intimsphäre
- Daten über verwaltungs- oder strafrechtliche Verfolgungen und Sanktionen
- Daten über Massnahmen der sozialen Hilfe

Annahme einer Persönlichkeitsverletzung, wenn besonders schützenswerte Personendaten Dritten weiter gegeben werden.

INHALT DER PERSONENDATEN



RECHTFERTIGUNGSGRÜNDE & INFORMATION



9 GRUNDSÄTZE

9 GRUNDSÄTZE

PRIVACY BY DEFAULT

Verantwortliche muss möglichst schonend Daten sammeln:

- Schutz von Personendaten ohne Konfiguration
- Benachrichtigung der betroffenen Personen
- Koppelungsverbot (EU)

Opt-in nicht Opt out!

~~☑ Ich abonniere den Newsletter~~

☐ Ich abonniere den Newsletter ✓

PRIVACY BY DESGIN

Privacy by Design bedeutet

- **Datenschutzprobleme schon bei der Entwicklung neuer Technologien prüfen**
- **den Datenschutz von vorneherein in die Gesamtkonzeption einbeziehen**

AUSGEWÄHLTE RECHTE UND PFLICHTEN

DOKUMENTATIONSPFLICHT

Der Verantwortliche setzt unter Berücksichtigung [...] der **Risiken** für die Rechte und Freiheiten natürlicher Personen **geeignete technische und organisatorische Massnahmen** um, um sicherzustellen und den **Nachweis** dafür erbringen zu können, dass die Verarbeitung gemäss dieser Verordnung erfolgt.

Diese Massnahmen werden erforderlichenfalls überprüft und aktualisiert.

DOKUMENTATIONSPFLICHT

Art. 7 Datensicherheit

1 Der Verantwortliche und der Auftragsbearbeiter gewährleisten durch geeignete technische und organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit.

2 Die Massnahmen müssen es ermöglichen, Verletzungen der Datensicherheit zu vermeiden.

3 Der Bundesrat erlässt Bestimmungen über die Mindestanforderungen an die Datensicherheit.

VERZEICHNIS VON BEARBEITUNGSTÄTIGKEITEN
[PROCESSING REGISTER]

Die Verantwortlichen und Auftragsbearbeiter führen ein Verzeichnis ihrer Bearbeitungstätigkeiten («**Verfahrensverzeichnis**»), welches mindestens enthält:

- Identität des Verantwortlichen
- Bearbeitungszweck
- Kategorien betroffenen Personen und der Kategorien Personendaten
- Kategorien von Empfängern
- Aufbewahrungsdauer
- Dokumentierung geeigneter Garantien bei Übermittlung ins Ausland sowie Angabe des Staates
- Beschreibung der technischen und organisatorischen Massnahmen

BEISPIEL

Verzeichnis der Bearbeitungstätigkeiten

Name und Kontaktdaten des Verantwortlichen:

Verzeichnis der Bearbeitungstätigkeiten der Muster AG

Allgemeines							Personendaten												Bezug zur Person (Kategorien betroffener Personen)							Zugriff / Transfer			
									besonders schützenswerte Personendaten / besondere Kategorien personenbezogener Daten																					
Name der Datensammlung	**Applikationsname**	**System**	**Datum der Inbetriebnahme**	**Zweck der Bearbeitung**	**Rechtfertigungsgrund der Bearbeitung**	**Applikationsowner und Ansprechpartner**	Daten natürlicher Personen	Daten juristischer Personen	Religion	Politisch / Ämter / Mitgliedschaften	Gewerkschaft	Gesundheit	Intimsphäre / Hinweise auf Partner	Rassenzugehörigkeit	Genetische / biometrische Daten	Sozialhilfe	Verfahren und Sanktionen	Andere Datenkategorien	Profiling	Mitarbeiter	Kunde	Lieferant	Besucher	Bewerber	ungefähre Anzahl betroffener Personen	Andere (bitte angeben)	Anzahl zugriffsberechtigter Personen	Zugriffsberechtigte Divisionen / Corporate Center der Datenschutz AG	Zugriffsberechtigte Gruppengesellschaften	Andere Zugriffsberechtigte Dritte
Beispiel: HR Adminstration	SAP Personalverwaltung	SAP	01.01.2008	Verwaltung von Personaldossiers / Mitarbeiterdaten	Gesetzliche Verpflichtung	Human Resources, Hans Muster	Ja	Ja	Ja	Ja	Nein	Ja	Nein	Nein	Ja	Nein	Nein		Ja	Ja	Nein	Nein	Ja	Nein	Nein	600		ca. 300	HR, GL, Finance	Muster AG	

DOKUMENTATIONSPFLICHT

- Verfahren mit personenbezogenen Daten zu dokumentieren
- Jedes Verfahren mit einer Risikoabschätzung bewerten & dokumentieren
- Basierend auf der Risikoabschätzung sind adäquate technische und organisatorische Massnahmen zu treffen & dokumentieren
- Korrekte Implementierung überprüfen & dokumentieren
- Die Aktualität regelmässig überprüfen und allenfalls ist diese nachzuführen; Überprüfung dokumentieren

BETROFFENENRECHTE

Auskunfts-, Herausgabe- Berichtigungs- und Löschbegehren [SUBJECT ACCESS REQUEST]

Betroffene Personen können in der Regel verlangen, dass Sie innert 30 Tagen erhalten:

AUSKUNFT
über die Kategorien und Bearbeitung Ihrer Daten

HERAUSGABE
ihrer elektronischen Daten (nur EU)

Bestätigung der **BERICHTIGUNG** Ihrer Daten

Bestätigung der **LÖSCHUNG** ihrer Daten

MELDEPFLICHT VON DATENSCHUTZ-VERLETZUNGEN

[Incident Response]

Grundlagen

- Benachrichtigung der Aufsichtsbehörde unverzüglich und möglichst **binnen 72 Stunden (CH: möglichst rasch)**.
- Der Auftragsverarbeiter alarmiert und informiert den für die Verarbeitung Verantwortlichen unverzüglich nach Feststellung einer Verletzung des Schutzes personenbezogener Daten.
- Im Anschluss: Der für die Verarbeitung Verantwortliche benachrichtigt im Anschluss an die Meldung an die Aufsichtsbehörde unverzüglich das Datensubjekt, sofern der Schutz der personenbezogenen Daten, die Privatsphäre oder die Rechte des Datensubjektes durch eine Verletzung beeinträchtigt werden.
  CH: Information des Datensubjekts, wenn für es für dieses erforderlich ist oder der Beauftragte dies verlangt
- CH: Eine Meldung darf in einem Strafverfahren gegen den Meldepflichtigen nur mit dessen Einverständnis verwendet werden.

Inhalt der Benachrichtigung

Die Benachrichtigung enthält mindestens:

- Eine **Beschreibung** der Art der Verletzung des Schutzes personenbezogener Daten mit Angabe der **Kategorien** und der **Zahl der betroffenen** Datensubjekte, der betroffenen Datenkategorien und der Zahl der betroffenen Datensätze;
- Name und **Kontaktdaten** des Datenschutzbeauftragten oder eines sonstigen Ansprechpartners;
- eine **Beschreibung der wahrscheinlichen Folgen** der Verletzung des Schutzes personenbezogener Daten;
- gegebenenfalls eine Beschreibung der vorgeschlagenen oder **ergriffenen Massnahmen**.

→ **Vorbereitende Handlungen für die Meldung**

→ **Checkliste bei Vorfällen**

HAFTUNG UND SANKTIONEN

HAFTUNG UND SANKTIONEN

Haftung

Jede Person, der wegen eines Verstosses gegen die Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen (Controller) oder gegen den Auftragsverarbeiter (Processor).

Sanktionen

Bei Verstössen gegen bestimmte Bestimmungen werden Geldbussen von bis zu EUR 20 Mio. oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist.

HAFTUNG UND SANKTIONEN

Sanktionen (Beispiele)

Mit Busse bis zu 250’000 Franken werden private Personen auf Antrag bestraft, die

- Ihre Melde- und Auskunftspflichten verletzten (Informationspflicht bei der Beschaffung, Informations- und Anhörungspflichten bei einer automatisierten Verarbeitung, Auskunftspflicht, Ergebnisse PIA, Bekanntgabe ins Ausland, falsche Angaben in Untersuchungen, Unterlassung von Meldung von Verletzungen)
- Ihre Sorgfaltspflichten verletzen (Unerlaubte Bekanntgabe ins Ausland, ungenügender Vertrag mit Auftragsbearbeiter, Mindestanforderungen an Datensicherheit nicht eingehalten)

Fällt eine Busse von höchstens 50 000 Franken in Betracht … so kann die Behörde von einer Verfolgung dieser Personen absehen und an ihrer Stelle den Geschäftsbetrieb zur Bezahlung der Busse verurteilen.

EMPFOHLENE MASSNAHMEN

ERSTE MASSNAHMEN

1. Verantwortlichkeiten festlegen:

- Projektverantwortlichen bestimmen
- Ressourcen freistellen
- Interne & externe Unterstützung
- Reporting

2. Übersicht gewinnen und Prioritäten festlegen:

- Verfahrensverzeichnis erstellen
- Risiken abschätzen
- Technische und organisatorische Massnahmen der IT dokumentieren
- Weitere Massnahmen ableiten und Prioritäten festlegen

EMPFOHLENE MASSNAHMEN

1. Schritt – Verzeichnis Verarbeitungstätigkeiten

Abteilung / Bereich

Name und Kontaktdaten Verantwortlicher

Verfahren Nr. 1		Verfahren Nr. 2		Verfahren Nr. ...	
▶ Zweck ▶ Datentransfer Drittländer ▶ Löschfristen	▶ Kategorien – Betroffene – Daten – Empfänger	▶ Zweck ▶ Datentransfer Drittländer ▶ Löschfristen	▶ Kategorien – Betroffene – Daten – Empfänger	▶ Zweck ▶ Datentransfer Drittländer ▶ Löschfristen	▶ Kategorien – Betroffene – Daten – Empfänger

EMPFOHLENE MASSNAHMEN

2. Schritt – Risiko-Bewertung

Abteilung / Bereich

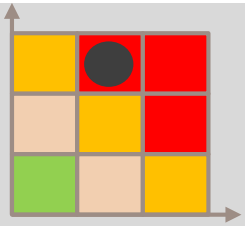
Name und Kontaktdaten Verantwortlicher

Verfahren Nr. 1

- Zweck
- Datentransfer Drittländer
- Löschfristen

- Kategorien
  - Betroffene
  - Daten
  - Empfänger

Risiko-beurteilung

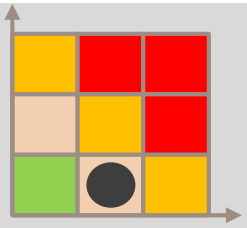


Verfahren Nr. 2

- Zweck
- Datentransfer Drittländer
- Löschfristen

- Kategorien
  - Betroffene
  - Daten
  - Empfänger

Risiko-beurteilung

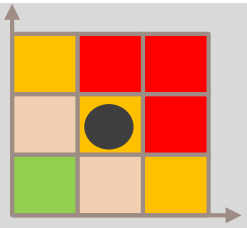


Verfahren Nr. ...

- Zweck
- Datentransfer Drittländer
- Löschfristen

- Kategorien
  - Betroffene
  - Daten
  - Empfänger

Risiko-beurteilung



EMPFOHLENE MASSNAHMEN

3. Schritt – Bestimmung Schutzmassnahmen

Abteilung / Bereich

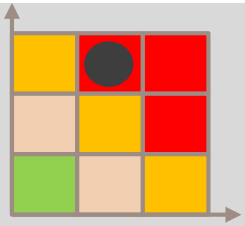
Name und Kontaktdaten Verantwortlicher

Verfahren Nr. 1

- Zweck
- Datentransfer Drittländer
- Löschfristen

- Kategorien
  - Betroffene
  - Daten
  - Empfänger

Risiko-beurteilung



Schutzmassnahmen (tech./org.)

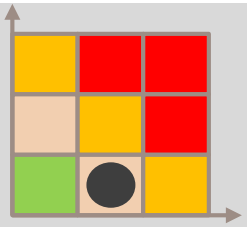
- Zugriffsbeschränkungen
- Pseudonymisierung
- ….

Verfahren Nr. 2

- Zweck
- Datentransfer Drittländer
- Löschfristen

- Kategorien
  - Betroffene
  - Daten
  - Empfänger

Risiko-beurteilung



Schutzmassnahmen (tech./org.)

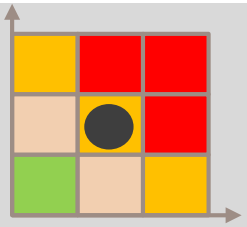
- Zugriffsbeschränkungen
- Pseudonymisierung
- ….

Verfahren Nr. …

- Zweck
- Datentransfer Drittländer
- Löschfristen

- Kategorien
  - Betroffene
  - Daten
  - Empfänger

Risiko-beurteilung



Schutzmassnahmen (tech./org.)

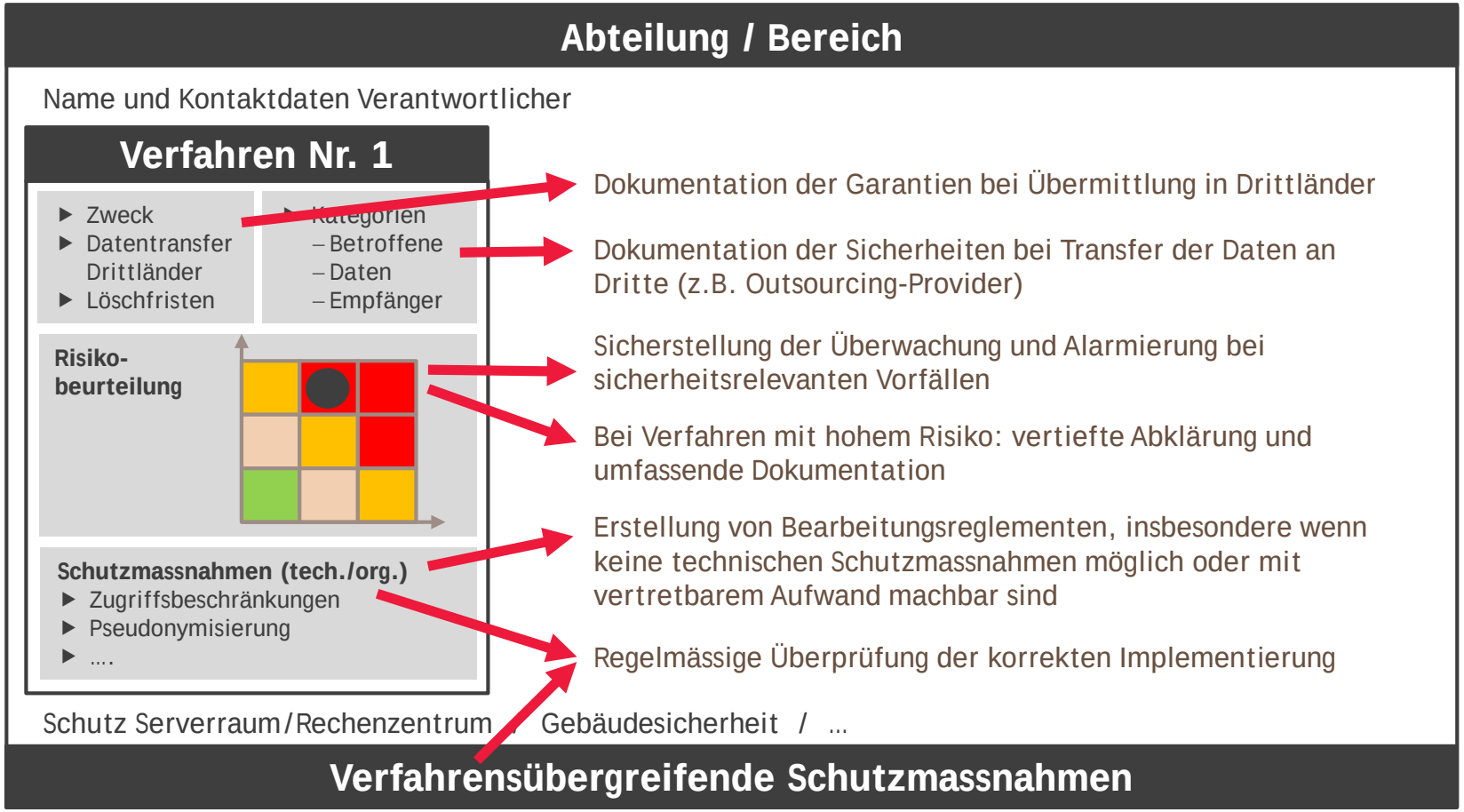
- Zugriffsbeschränkungen
- Pseudonymisierung
- ….

Schutz Serverraum/Rechenzentrum / Gebäudesicherheit / …

Verfahrensübergreifende Schutzmassnahmen

EMPFOHLENE MASSNAHMEN

4. Schritt – Festlegen weiterer nötiger Massnahmen



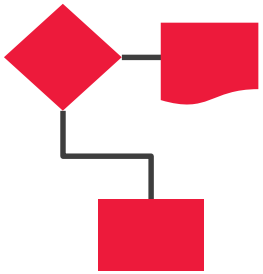
ERSTE MASSNAHMEN

1. Verantwortlichkeiten festlegen:

- Projektverantwortlichen bestimmen
- Ressourcen freistellen
- Interne & externe Unterstützung
- Reporting

2. Übersicht gewinnen und Prioritäten festlegen:

- Verfahrensverzeichnis erstellen
- Risiken abschätzen
- Technische und organisatorische Massnahmen der IT dokumentieren
- Weitere Massnahmen ableiten und Prioritäten festlegen



3. Prozesse einrichten:

- Datenschutzverletzungen (72 h)
- Betroffenenrechte (30 Tage)
- Neue IT Systeme / Änderungen (mit Planung)

SOFORTMASSNAHMEN

Feststellen, ob von der Firma verarbeitete Personendaten der EU-Datenschutz-Grundverordnung unterstellt sein könnten.

Falls ja, bis 25. Mai 2018:

- Einwilligungserklärungen dokumentieren
- Provisorischen Prozess für Datenschutz-Verletzungen etablieren
- Provisorischen Prozess für Betroffenrechte (Auskunft, Berichtigung und Löschung) etablieren

- Aufnahme des Verfahrensverzeichnisses planen

Falls nein:

- Aufnahme des Verfahrensverzeichnisses planen

FRAGEN UND DISKUSSION

ARE YOU READY?

Testen Sie mit einem Self Assessment der englischen Aufsichtsbehörde, dem UK ICO (Information Commissioner's Office), ob Sie die Vorgaben der EU bereits alle erfüllen:

https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/getting-ready-for-the-gdpr/

DATENSCHUTZ

Praxisorientiert und kompakt

Klaus Krohmann
BDO AG, Zürich
Rechtsanwalt

044 444 36 25
klaus.krohmann@bdo.ch