KOMMEN WIR AUF DEN **PUNKT.**

Die neue Europäische Datenschutz-Grundverordnung - aktuelle Herausforderungen für Großunternehmen

Industrieakademie

9. Mai 2017

Basics

- Datenschutz-Grundverordnung (DS-GVO):
  - ab 25. Mai 2018
  - unmittelbar (mit Öffnungsklauseln: zB Art 88 „*Daten im Beschäftigungskontext*“; Art 9 Abs 3 „*genetische, biometrische oder Gesundheitsdaten*“)
  - Verarbeitung personenbezogener Daten natürlicher Personen, die eine Person direkt oder indirekt identifizieren, wie zB Name, Standortdaten, Online- Kennzeichnung, wirtschaftliche Daten; NICHT Sachdaten
  - auch für Unternehmen ohne Niederlassung in der EU nach dem Marktortprinzip (Verkauf über Internet oder Beobachtung des Verhaltens betroffener Personen).

Struktur der DS-Grundverordnung

Grundsätze der Verarbeitung
Art. 5 Abs. 1

Verantwortlicher muss rechtmäßigen Datenumgang nachweisen
(Rechenschaftspflicht, Art. 5 Abs. 2)

Verantwortung des Verantwortlichen
Art. 24

DS by design & default Art. 25	**Auftrags-verarbeiter** Art. 28	**Sicherheit der Verarb.** Art. 32
Verzeichnis Art. 30	**Verletzung** Art. 33, 34	**DS-Folgenab-schätzung** Art. 33, 36

Datenschutzbeauftragter
Art. 37 - 39

Rechte der betroffenen Person
Art. 12 - 23

Transparente Information, Kommunikation und Modalitäten
Art. 12

Erhebung Art. 13,14	**Auskunft** Art. 15	**Widers-pruch** Art. 21
	Berichtigung Löschung Einschrän-kung Art. 16-19	**Automat. Entscheid.** Art. 22
	Datenüber-tragbarkeit Art. 20	**Verletzung** Art. 34

Grundsätze - Art. 5

- Verbot der Verarbeitung mit Erlaubnisvorbehalt
- Einhaltung und Nachweis = „***Rechenschaftspflicht***“ zu:
  - Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
  - Zweckbindung
  - Datenminimierung
  - Richtigkeit der Daten
  - Speicherbegrenzung und
  - Integrität/Vertraulichkeit/Sicherheit

Grundsatz – “Rechenschaft“

- WER? - Datenschutz ist Aufgabe der Geschäftsführung:
  - Datenschutzziele
  - Datenschutz-Governance-Struktur
  - Datenschutzleitlinie/-richtlinie

„**P**LAN-**D**O-**C**HECK-**A**CT“ (kontinuierlich)

Grundsatz – Rechtmäßigkeit/Rechtsgrundlage (Art. 6)

Zweck der Verarbeitung

BEI Erhebung der Daten

Informationspflicht

<u>Rechtsgrundlage</u>

- Gesetzliche Verpflichtung
- Einwilligung
- Vertragserfüllung
- berechtigtes Interesse
- etc

Grundsatz – Rechtmäßigkeit/Rechtsgrundlage (Art. 6)

Welche Informationen:

- ✓ Namen und Kontaktdaten des Verantwortlichen bzw des Vertreters in der EU;
- ✓ Kontaktdaten des Datenschutzbeauftragten;
- ✓ Zweck der Verarbeitung und Rechtsgrundlage;
- ✓ Empfänger bzw Kategorien von Empfängern;
- ✓ Übermittlung in ein Drittland (angemessenes Schutzniveau – Ja/Nein)
- ✓ Speicherdauer
- ✓ Hinweis auf Rechte Betroffener (Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch)

Grundsatz – Rechtmäßigkeit/Rechtsgrundlage (Art. 6)

- ✓ Recht auf Widerruf der Einwilligung;
- ✓ Recht auf Beschwerde bei einer Aufsichtsbehörde;
- ✓ Informationen, ob die Daten gesetzlich erhoben werden müssen – Ja/Nein;
- ✓ Folgen der Nichtbereitstellung der Daten;
- ✓ Automatisierte Entscheidungsfindung (Logik und Tragweite der Auswirkung);
- ✓ Wenn Daten von Dritten bezogen werden: Quelle der Daten.

Gültige Zustimmung

Struktur der Datenschutz-Verordnung

Grundsätze der Verarbeitung
Art. 5 Abs. 1

Verantwortlicher muss rechtmäßigen Datenumgang nachweisen
(Rechenschaftspflicht, Art. 5 Abs. 2)

Verantwortung des Verantwortlichen
Art. 24

DS by design & by default Art. 25	**Auftrags-verarbeiter** Art. 28	**Sicherheit der Verarb.** Art. 32
Verzeichnis Art. 30	**Verletzung** Art. 33, 34	**DS-Folgenab-schätzung** Art. 33, 36

Datenschutzbeauftragter
Art. 37 - 39

Rechte der betroffenen Person
Art. 12 - 23

Transparente Information, Kommunikation und Modalitäten
Art. 12

Erhebung Art. 13,14	**Auskunft** Art. 15	**Widers-pruch** Art. 21
	Berichtigung Löschung Einschrän-kung Art 16-19	**Automat. Entscheid.** Art. 22
	Datenüber-tragbarkeit Art. 20	**Verletzung** Art. 34

Verantwortung – Design by Default

- Datenschutzfreundliche Einstellungen bei Festlegung der Mittel und zum Zeitpunkt der Verarbeitung

Minimierung Daten

Schutz der Betroffenenrechte

- Pseudonymisierung, Aggregation von Daten, Zugangskontrollen
- Soziale Netze: nicht automatisch öffentlich / verbunden werden

Konkrete Anleitung: **NEIN!!!**

Anhaltspunkte: European Union Agency for Network and Information Security

(www.enisaeuropa.eu)

Privacy and Data Protection by Design – from policy to engineering:

*The principle „Privacy/data protection by design“ is based on the insight that building in privacy features from the **beginning of the design process** is preferable over the attempt to adapt a product of service at a later stage. The involvement in the design process supports the consideration of the full lifecycle of the data and its usage.*

*The principle „Privacy/data protection by default“ means that in the **default setting** the user is **already protected against privacy risks**. This affects the choice of the designer which parts are wired-in and which are configurable*

Design Strategies – 8 Prinzipien zur Datenerhebung

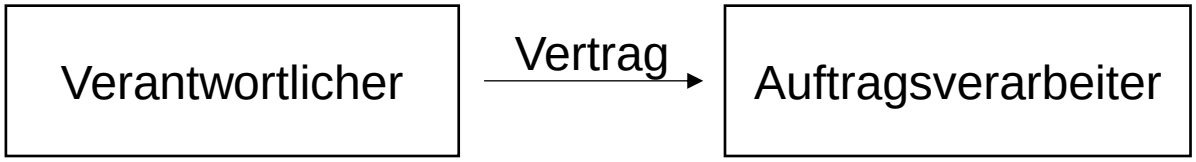
- Datenminimierung – „select before you collect“
- „Hide“ – Zusammenhang der Daten „verstecken“
- Trennung – Datenlagerung in verschiedenen „Datenbanken“ (dezentral): Beispiel Social Network Platform „Diaspora“
- Aggregation
- Information
- Kontrolle durch den Nutzer
- Durchsetzung: Policy und Durchsetzung der Einhaltung
- Nachweise/Dokumentation

Datenschutztechniken (Privacy Techniques)

- Authentifizierung: „end-to-end“
- Identifizierung durch Attribute, die nur der Benützer kennt („Attribute based credentials“) – nicht „übertragbar“, nicht nachverfolgbar, etc ➡ nicht über IP-Adresse
- Sicherstellung der privaten Kommunikation (*Pretty Good Privacy Software*): „Key-System“
- „Datenbank-Datenschutz“ („Privacy in database“):

  Datenabgleich über Datenaustausch bis Zugangskontrolle ➡ „Profiling“
- etc

Auftragsverarbeiter (Art. 28)



- Auswahl: „DD“ ⇒ technisch geeignete Garantien
- Vertrag: immer schriftlich

Planung

- Durchführung:
  - dokumentierte Anweisungen
  - Nachweis über Einhaltung
- Beendigung: Löschen / Transfer

Betrieb / Audit
Verbesserung

PDCA

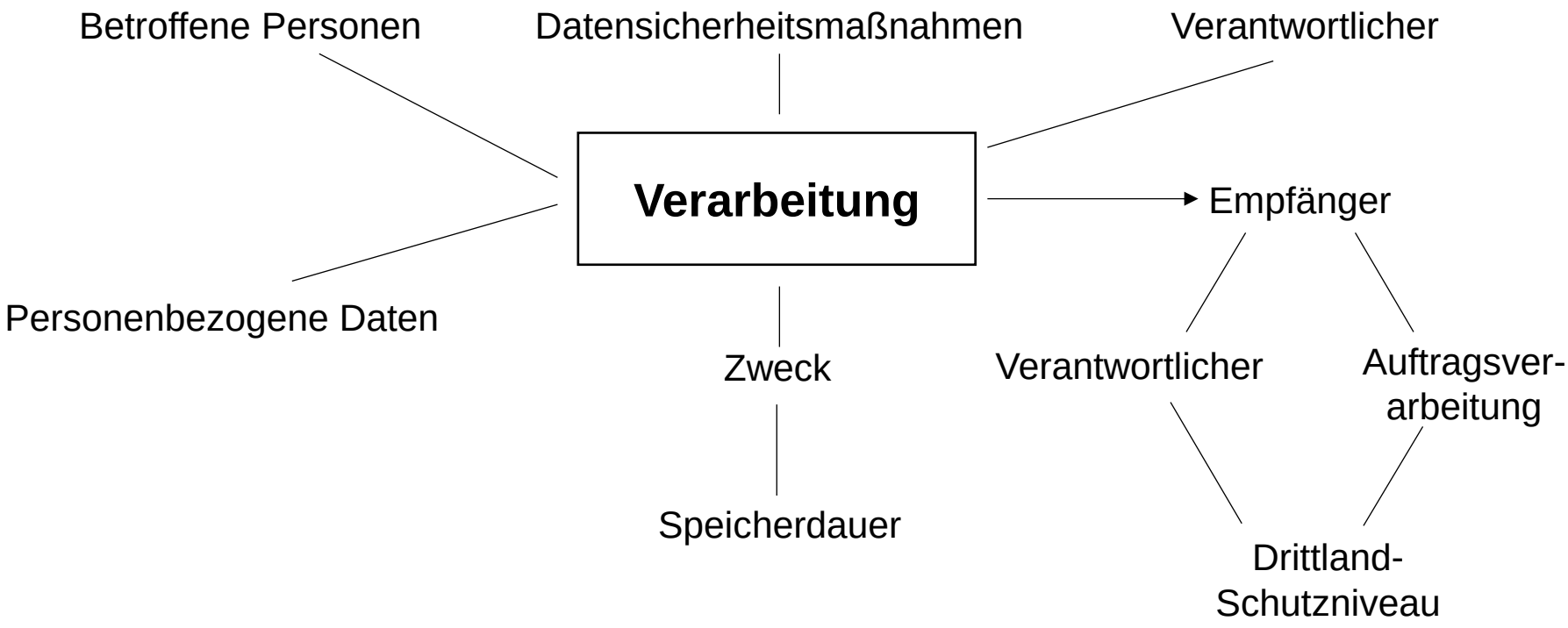
Verzeichnis (I) (Art. 30)

- **Wer muss**:
  - Unternehmen mit mehr als 250 Mitarbeitern
  - Besondere Datenkategorien (Gesundheitsdaten, genetische Daten, Gewerkschaftsangehörigkeit, etc.) ⇒ Verarbeitung nicht nur gelegentlich erfolgt:

    Einzelarzt: Nein / Gruppenpraxis: Ja
  - Verarbeitung strafrechtlich relevanter Daten

Einsichtsrechte der Behörde

Verzeichnis (II) (Art. 30)



Sicherheit (Art. 32) & DS – Folgenabschätzung (Art. 35/36) (I)

- Wann verpflichtend:
  - Hohes Risiko für Betroffene: neue Technologien
  - Verarbeitung besonderer Kategorien von personenbezogenen Daten
  - Strafrechtlich relevante Daten
  - Systematische & umfangreiche Bewertung natürlicher Personen (Profiling, Bonitätsprüfung, Bewerbung (automatisch ⇒ zB wer bestimmte Punktezahl bei Eignungstest nicht erreicht)
  - „Videoüberwachung“

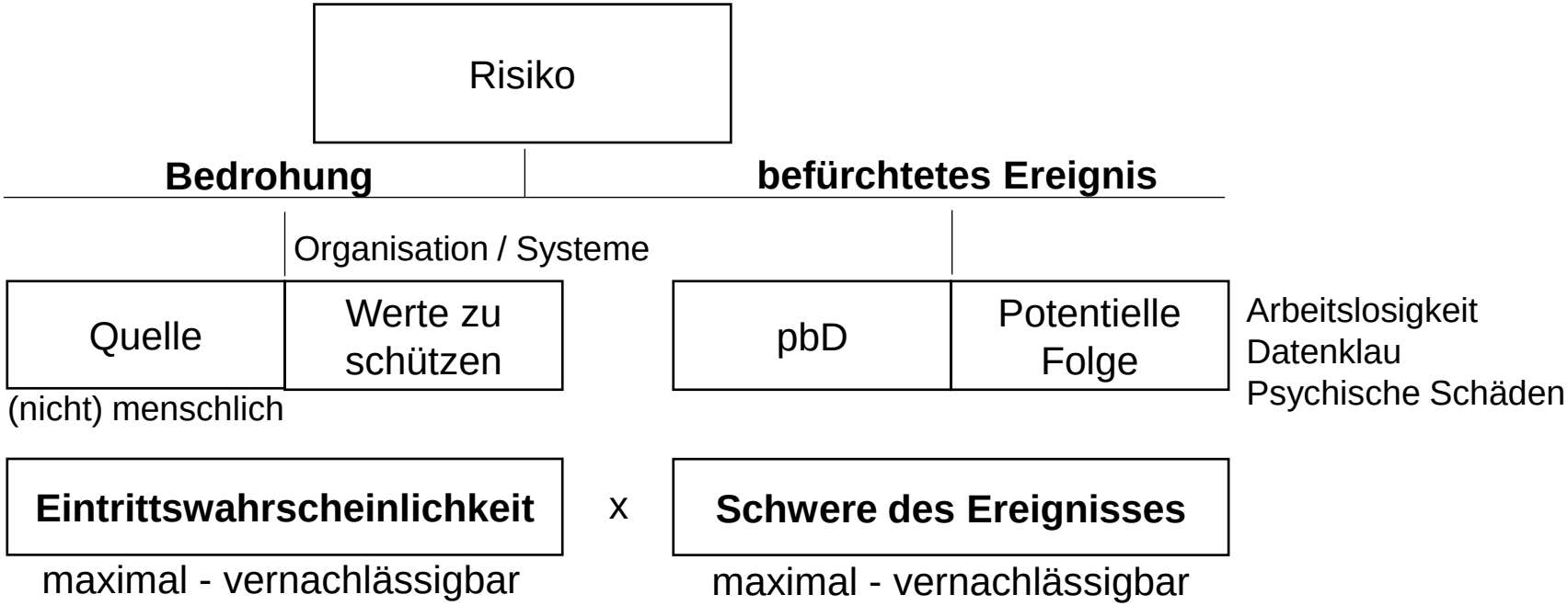
Sicherheit (Art. 32) & DS-Folgenabschätzung (Art. 35/36) (II)

- Woher: CNIL (Frankreich) & ICO aus UK
- Risikobasierter Ansatz:
  - Beurteilung: nach objektiven Merkmalen
  - Systematische Identifikation
  - Eintrittswahrscheinlichkeit und Schwere
  - Qualitative Beurteilung
  - „Eindämmung“ Risiko durch geeignete Maßnahmen

- **Risiko = Schadensausmaß x Eintrittswahrscheinlichkeit**

Sicherheit (Art. 32) & DS-Folgenabschätzung (Art. 35/36) (III)

„Flußschema“ CNIL:



⇒ Risikobeurteilung in Matrixform: Akzeptabel → Inakzeptabel

Datenschutzbeauftragter (Art. 37-39) (I)

- Wer ist verpflichtet:
  - Behörden (außer Gerichte)
  - Kerntätigkeit → regelmäßige & systematische Überwachung: Profiling, Detekteien, Videoüberwachung, systematische Auswertung von Fehlzeiten / Qualifikationen / etc., Fuhrparkmanagement, individualisierte Marketingstrategien …
  - Kerntätigkeit: Verarbeitung besonderer personenbezogener Daten
  - Nationale Sonderregelungen zulässig

Datenschutzbeauftragter (Art. 37-39) (II)

Qualifikationen:

- **Rechtliche Kenntnisse:**
  - Datenschutzrecht / EU Grundrechtscharta
  - Europarecht in Grundzügen
  - Arbeitsrecht in Grundzügen
  - Telekommunikationsrecht
  - Grundzüge des Verfahrensrechts
  - Grundkenntnisse Gesellschaftsrecht
- **Technische Kenntnisse**
  - ISO-Standards
  - Grundkenntnisse IT-Architektur
  - Grundkenntnisse Berechtigungsmanagement
  - Technische Mandantentrennung
  - Aufbau von Logdateien
  - Datensicherheitsmaßnahmen

Datenschutzbeauftragter (Art. 37-39) (III)

Aufgaben des Datenschutzbeauftragten:

- Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters;
- Überwachung der Einhaltung der DS-GVO;
- Überwachung der Einhaltung der Strategien (Policies, Procedures, Zuweisung von Zuständigkeiten, Sensibilisierung und Schulungen);
- Beratung iZm der Folgenabschätzung;
- Überwachung der Durchführung der Datenschutz-Folgenabschätzung;
- Zusammenarbeit mit der Aufsichtsbehörde;
- unter Umständen Management der entsprechenden Betroffenenrechte.

Datenschutzbeauftragter (Art. 37-39) (IV)

Qualifikation, Position im Unternehmen:

- ist an keine Anweisungen der Geschäftsführung gebunden – berichtet aber an diese;
- arbeitet in voller Unabhängigkeit;
- das Unternehmen hat ihm sämtliche erforderlichen Ressourcen zur Verfügung zu stellen (Regel: Je 500 Mitarbeiter eine Vollarbeitszeitkraft);
- Zugang zu personenbezogenen Daten muss jedenfalls notwendig sein.

Datenschutzbeauftragter (Art. 37-39) (V)

- **Wer haftet**:
  - Bestellung als verantwortlicher Beauftragter gem § 9 Abs 2 Verwaltungsstrafgesetz - nunmehr unzulässig: Interessenskonflikt;
  - Haftung verbleibt beim Management – Datenschutzbeauftragter hat zu berichten;
  - Besonderer „Kündigungsschutz“

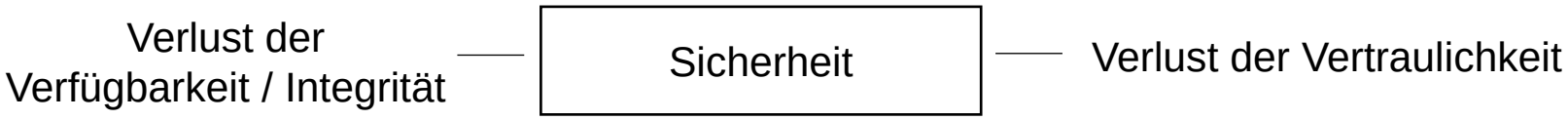
„Konzerndatenschutzbeauftragter“

- Benennung: unter einem für alle „Länder“

- Erreichbarkeit
  - *Räumlich*: persönliches Treffen ⇒ 1 Tagesreise
  - *Zeitlich*: kurzfristig erreichbar
  - *Sprachlich*: Sprache der Niederlassung ⇒ gegenüber der nationale Behörde Ansprechpartner

Verletzung (Art. 33 & 34) (I)

- Definition:



- Meldepflicht / **Behörde** binnen 72 Stunden (Verzögerung)
  - Anlaufstelle
  - Beschreibung:
    - Art der Verletzung
    - Anzahl betroffener Personen
    - Folgen: Risikoeinschätzung
    - Maßnahmen
  - Dokumentation

Verletzung (Art. 33 & 34) (II)

- Keine Meldepflicht/**Behörde**:
  - kein Risiko für die Rechte/Freiheiten des Betroffenen – Dokumentation des Analysepfades

- Meldepflicht / *Betroffener:* unverzüglich bei hohem Risiko
  - Kontaktdaten
  - Beschreibung: Verletzung – Folgen – Maßnahmen

  Außer:
  - Verschlüsselung
  - Maßnahmen ≠ hohes Risiko

Verletzung (Art. 33 & 34) (III)

Was ist zu tun	Zeitpunkt	Wer?
– Identifikation der Verletzung	Kenntniserlangung – Kontrolle!	Zentral/dezentral
– Risikoanalyse (Art, Wer, Auswirkungen)	Unverzüglich	DB, Externe, Techniker
– Maßnahmen	Unverzüglich	DB, Techniker, GF
– Meldung	Ja / Nein: Dokumentation	DB, Techniker, GF
– Vornahme Meldung	72h ab Kenntniserlangung	DB, GF
– Betroffener	Unverzüglich –bei hohem Risiko	DB, GF, Kundenbetreuer, etc
– Audit	Je nach Vorfall	

Struktur der Datenschutz-Verordnung

Grundsätze der Verarbeitung
Art. 5 Abs. 1

Verantwortlicher muss rechtmäßigen Datenumgang nachweisen
(Rechtschaftspflicht, Art. 5 Abs. 2)

Verantwortung des Verantwortlichen
Art. 24

DS by design & by default Art. 25	**Auftragsverarbeiter** Art. 28	**Sicherheit der Verarb.** Art. 32
Verzeichnis Art. 30	**Verletzung** Art. 33, 34	**DS-Folgenabschätzung** Art. 33, 36

Datenschutzbeauftragter
Art. 37 - 39

Rechte der betroffenen Person
Art. 12 - 23

Transparente Information, Kommunikation und Modalitäten
Art. 12

Erhebung Art. 13,14	**Auskunft** Art. 15	**Widerspruch** Art. 21
	Berichtigung Löschung Einschränkung Art 16-19	**Automat. Entscheid.** Art. 22
	Datenübertragbarkeit Art. 20	**Verletzung** Art. 34

Rechte der Betroffenen (Art. 15- 22) (I)

- **Auskunft**:√
- **Berichtigung**: √
- **Löschung- Vergessenwerden**: tlw √ - unverzüglich zu löschen (u.a):
  - Widerruf der Einwilligung – andere Rechtsgrundlage fehlt;
  - Daten werden nicht mehr für die ursprünglichen Zwecke benötigt;
  - Unrechtmäßige Verarbeitung;
  - Muss Dritte informieren, dass Löschung „beantragt“ wurde

  Außer:
  - Freie Meinungsäußerung;
  - Rechtsansprüche;
  - Forschungszwecke

Rechte der Betroffenen (Art. 15- 22) (I)

- **Einschränkung der Verarbeitung (= Sperrung):** √
- **Datenübertragbarkeit** - strukturierte, gängige und maschinenlesbare Form:
  - Die betroffene Person selbst betreffen;
  - Daten, die die betroffene Person bereitgestellt hat ≠ Daten bei Auswertung (Frage: vernetzte Fahrzeuge);
  - Einwilligung bzw. Vertrag;
  - nicht „manuelle“ Daten.

Rechte und Freiheiten Dritter dürfen dadurch nicht beeinträchtig werden

Rechte der Betroffenen (Art. 15 – 22) (II)

- **Widerspruch**:
  - Nur Daten des Betroffenen
  - Abwägung: überwiegende zwingende schutzwürdige Gründe → Beweislast: Verantwortlicher
  - Direktmarketing: keine Abwägung – immer!
  - Forschungszwecke/statistische Zwecke: zulässig wenn die Gründe der Betroffenen „in ihrer besonderen Situation“ liegen

Rechte der Betroffenen (Art. 15 – 22) (III)

- **Automatische Entscheidung im Einzelfall**:
  - Recht nicht unterworfen zu werden
  - keine Einbeziehung besonderer Datenkategorien (Gegenausnahme: explizite Zustimmung – nationale Verbote sind zu beachten!!!)
  - Zulässig:
    - Vertragserfüllung
    - Zustimmung
    - Besondere Maßnahmen: Recht auf Erwiderung, Darlegung des eigenen Standpunktes etc.

Recht auf Widerruf der Einwilligung (Art. 7 (3))

- Grundsatz anerkannt (zB klinische Versuche)
- Jederzeit & auch im vollem Umfang
- Kein „Verzicht“ im Voraus möglich
- Konsequenz:
  - ex nunc: für Zukunft
  - ex-tunc: iVm Art. 17 Abs. 1 – Recht auf Vergessenwerden (mit Einschränkung)

Implementierung der Betroffenenrechte

- **„Prozess“:**
  - Annahmeprozess für Anfragen: zentral/dezentral
  - Verifikation der Identität des Betroffenen
  - Konsistente Bearbeitung (wann wird Anfrage abgelehnt)
  - Umsetzung im Unternehmen: Löschung / Sperrung / etc.
  - Kommunikation mit Betroffenen (Information über Rechtsbehelf)
- **Zeitl. Rahmen**:
  - 1 Monat
  - „Fristerstreckung“ um 2 Monate, wenn begründet (Komplexität)

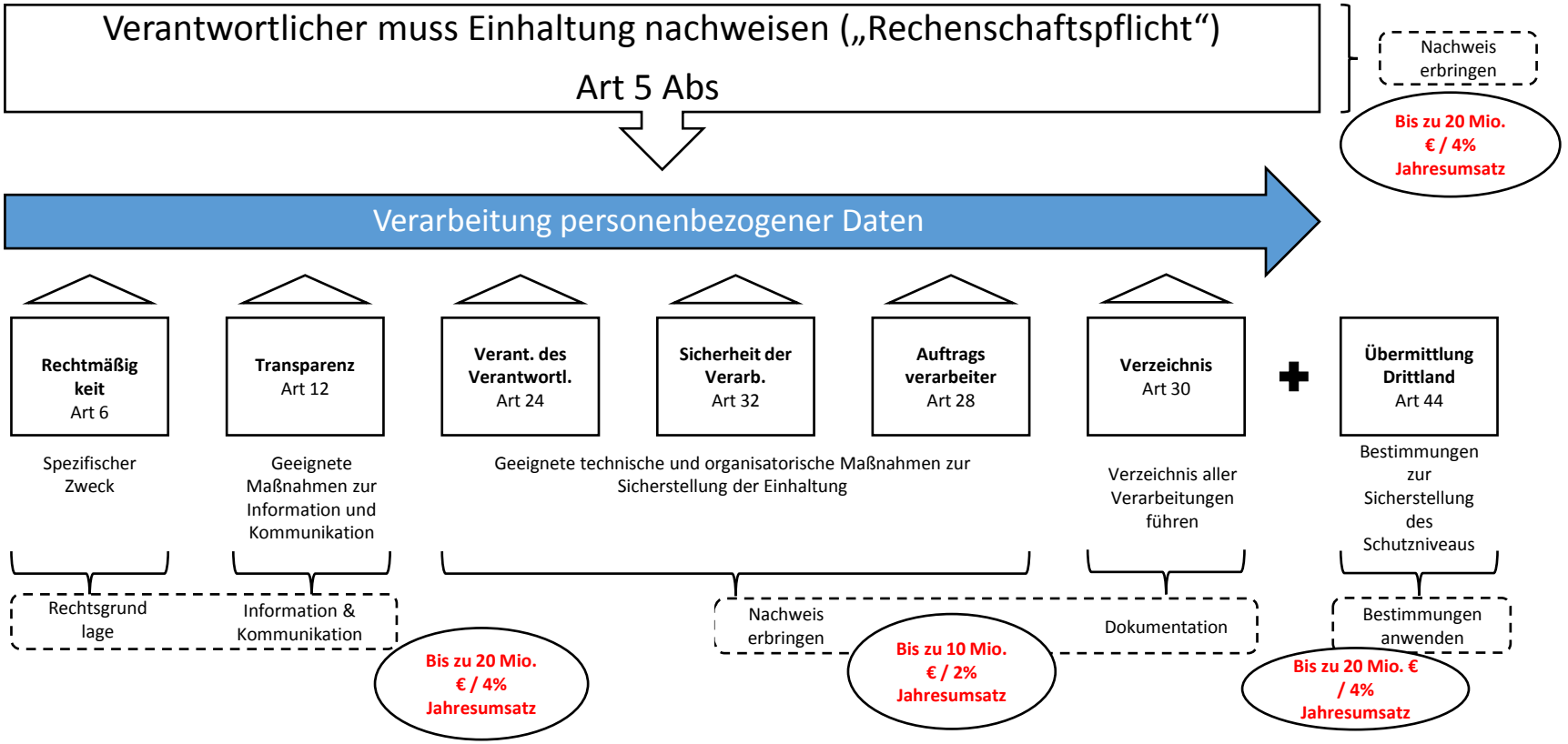
Dokumentationspflichten

- Rechenschaftspflicht: ✓
- Rechtmäßigkeit: ✓ (Grundlage)
- Einwilligung: ✓
- Einwilligung Kind (13-16): ✓
- Besondere Kategorien: ✓
- Erhebung beim Betroffenen: ✓ (Info)
- Erhebung durch Dritten: ✓ (Nutzung)
- Verarbeitung: ✓
- Privacy by design / default: ✓ (Risikobeurteilung)
- Auftragsverarbeiter
- Verarbeitungsverzeichnis: ✓ (Daten, Betroffene, Zweck, Frist,…)
- Sicherheit: ✓
- Datenschutzfolgeabschätzung: ✓
- Drittlandübermittlung: ✓
- Auskunft: ✓
- Berichtigung: ✓
- Löschung: ✓
- Einschränkung: ✓
- Datenübertragbarkeit: ✓
- Widerspruch: ✓
- Automatisierte Entscheidung: ✓
- Datenschutzverletzung: ✓

Aufgaben von Verbänden, die Kategorien von Verantwortlichen vertreten

- Problem: Unbestimmtheit gepaart mit hohen Strafen
- Soll zur „Konkretisierung der Generalklauseln beitragen“ (nicht verschärfen, nicht verwassern)
- Welche Punkte
  - transparente Verarbeitung
  - berechtigtes Interesse
  - Erhebung der Daten
  - Ausübung der Rechte
  - Schutz von Kindern
  - Maßnahmen etc
- Genehmigung Aufsichtsbehörde (unklar, widersprüchlich, unvollständig):
  - rein national: positive Stellungnahme
  - Übergreifend: Kohärenzverfahren
- Rechtswirkung: unklar $\Rightarrow$ außer Europäische Kommissionsentscheidung

Wieso das Ganze? – 20 Mio/4% bzw 10 Mio/2% des Umsatzes



©Krang/Sachs/Gierschmann, Datenschutz-Compliance nach der DS-GVO (2017)

Örtliche Zuständigkeit der Behörde

- Besondere Daten: Behörde, wo die Daten erhoben wurden
- „Federführende“ Aufsichtsbehörde und Aufsichtsbehörde:
  - nationale Behörde
  - Behörde der Hauptniederlassung bei „Grenzüberschreitung“ („federführend“) ⇒ „Beschlussentwurf“ durch örtliche Aufsichtsbehörde
  - Nur eine Niederlassung betroffen ⇒ jene der Niederlassung
  - Federführende „will nicht“ (3 Wochen): Behörde, wo die Beschwerde eingelangt ist
  - Amtshilfe und Koordination

Befugnisse der Behörde

- „Untersuchungsbefugnisse“
  - Zugang zu den Geschäftsräumlichkeiten
  - Zugang zu personenbezogenen Daten
  - Zugang zu Datenverarbeitungsanlagen

  ⇒ Datenschutzprüfung: Beschwerdeprüfung oder anlasslos (Konzeption / Angemessenheit / Wirksamkeit)
- Abhilfeinstrumente:
  - Löschung
  - Korrektur
  - Widerruf Zertifizierung
  - Strafen

DDr. Karina Hellbert

A-1060 Wien, Am Getreidemarkt 1
Telefon: +43 1 582 580
Telefax: +43 1 582 582
E-Mail: k.hellbert@fplp.at

Die Vortragende übernimmt keinerlei Gewähr für die Aktualität, Korrektheit, Vollständigkeit oder Qualität der bereitgestellten Informationen. Haftungsansprüche gegen die Vortragende, welche sich auf Schäden materieller oder ideeller Art beziehen, die durch die Nutzung oder Nichtnutzung der dargebotenen Informationen bzw. durch die Nutzung fehlerhafter und unvollständiger Informationen verursacht wurden, sind grundsätzlich ausgeschlossen.