DATENSCHUTZ-MANAGEMENT NACH DER GVO

Normative Grundlagen

Regelwerke

Best Practice

Andreas Sachs

ist **Informatiker** und **Vertreter des Präsidenten beim Bayerischen Landesamt für Datenschutzaufsicht (BayLDA)** in Ansbach.

Seit 2011 beschäftigt sich das technische Referat dabei mit verschiedensten Themen, z.B.:

Internet der Dinge

Verschlüsselungsverfahren

Datenpannen & Hacking

Vernetzte Fahrzeuge

Cloud Computing

IT-Sicherheit

Identitäten & Webportale

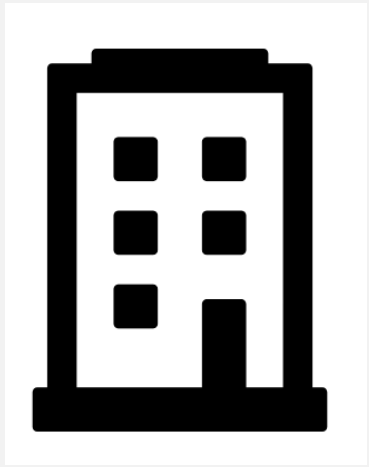
Apps & Smart Devices

Trackingverfahren

AGENDA

- DS-GVO – Big Picture
- Paradigmenwechsel Rechenschaftspflicht
- Datenschutzkonforme Verarbeitung
- Umgang mit Betroffenenrechten
- Meldung von Datenschutzverletzungen
- Verarbeitungsverzeichnis (2.0)
- „Formel“ zur Rechenschaftspflicht

DS-GVO – BIG PICTURE



Bußgelder?

Was ist zu tun?

Datenschutz-grundverordnung

25. Mai 2018

DS-GVO – BIG PICTURE

- Allgemeine Bestimmungen
- Grundsätze
- Betroffenenrechte
- Verantwortliche und Auftragsverarbeiter
- (Internationaler) Datentransfer
- Aufsichtsbehörden
- Haftung und Sanktionen
- Besondere Verarbeitungssituationen
- Durchführungsrechtsakte
- Schlussbestimmungen

GEGENSTAND UND ZIELE – ARTIKEL 1

- Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten

- Freier Datenverkehr in der EU darf dabei nicht eingeschränkt werden

SACHLICHER ANWENDUNGSBEREICH– ARTIKEL 2

- Automatisierte Verarbeitung

- Nichtautomatisierte Verarbeitung von Dateisystemen

RÄUMLICHER ANWENDUNGSBEREICH– ARTIKEL 3

- Verantwortliche / Auftragsverarbeiter in EU

- Verantwortliche / Auftragsverarbeiter außerhalb EU,
  wenn Dienste in EU angeboten werden

GRUNDSÄTZE DER VERARBEITUNG– ARTIKEL 5

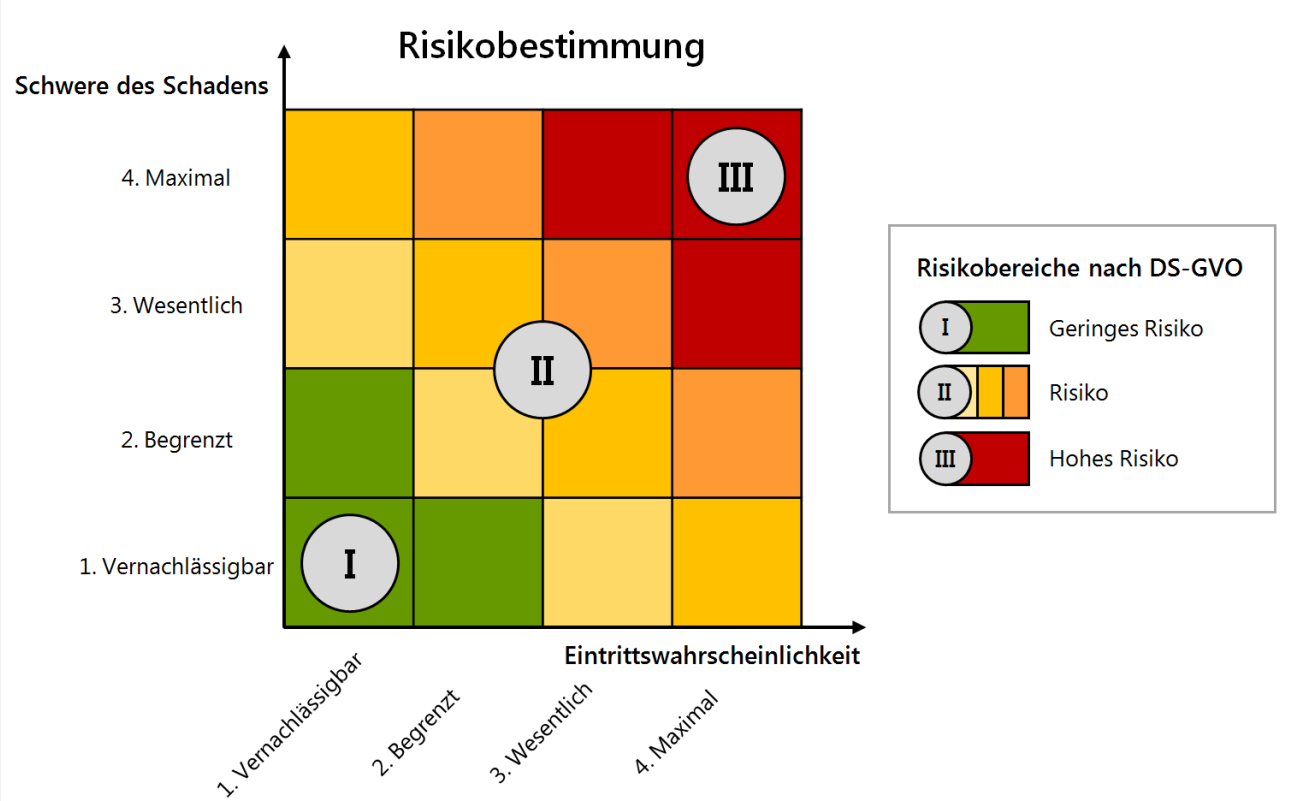
- Rechtmäßig und Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Sicherheit der Verarbeitung
- Rechenschaftspflicht

RISIKOORIENTIERTER ANSATZ

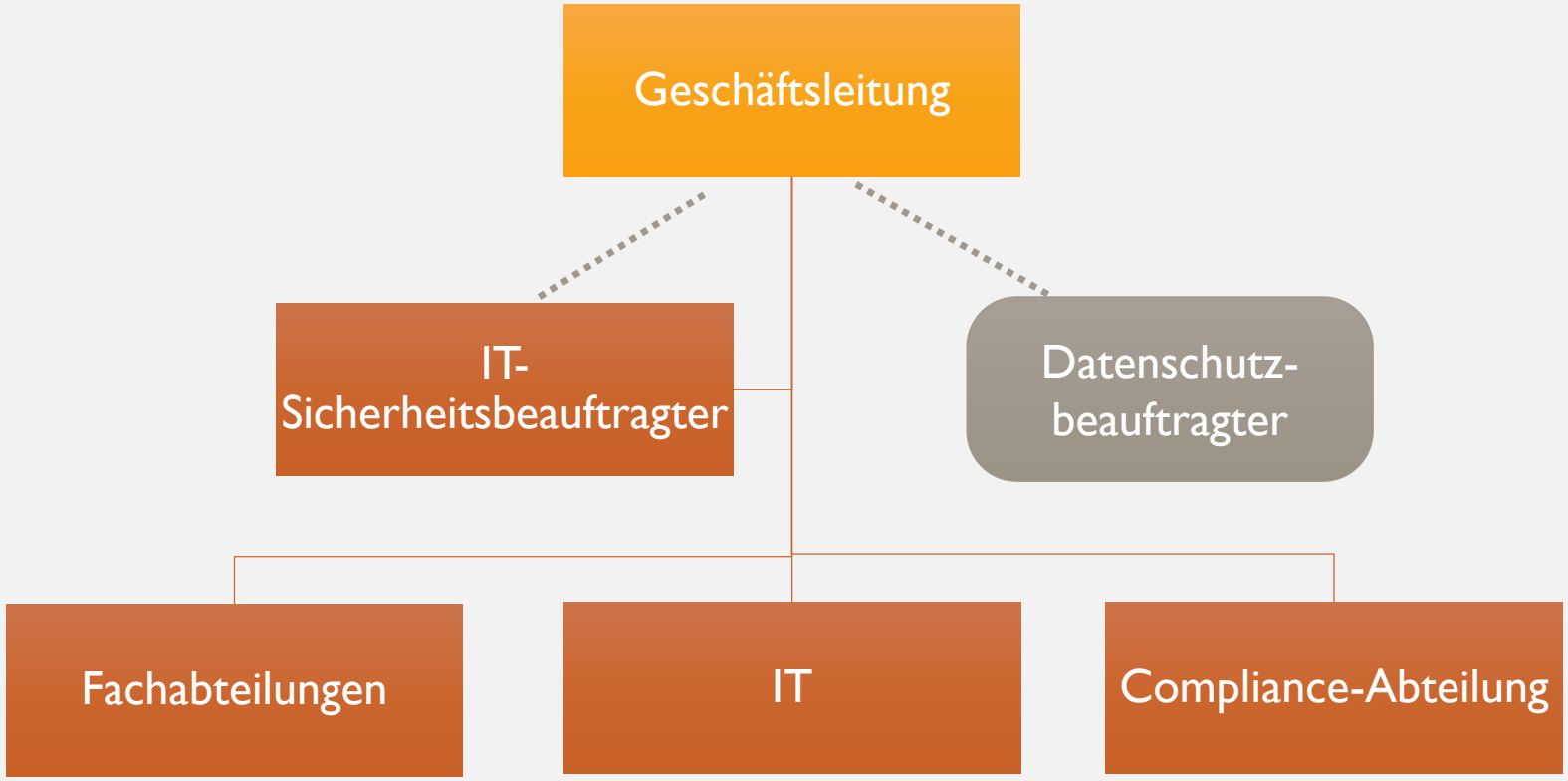
- Die DS-GVO hat einen **risikoorientierten Ansatz** bei der Auswahl der **technischen und organisatorischen Maßnahmen**
- Bei der Rechtmäßigkeit gilt: **Verbot mit Erlaubnisvorbehalt**
- Risiko = Spezifische **Eintrittswahrscheinlichkeit x Schwere** des Risikos
- **Risikobereiche** mit Rechtsfolgen:
  - Kein Risiko
  - Risiko
  - Hohes Risiko
- Datenschutzrisiko ≠ Unternehmensrisiko

RISIKOORIENTIERTER ANSATZ

- Die DS-GVO gibt keine konkrete „Risikoformel“ vor
- Art, Umfang, Umstände und Zweck der Verarbeitung sind zu Betrachten
- Eintrittswahrscheinlichkeiten und Schaden/Beeinträchtigungen ergeben spezifische Risiken
- Rechts: Vorschlag für eine Risikomethode



AUFBAUORGANISATION



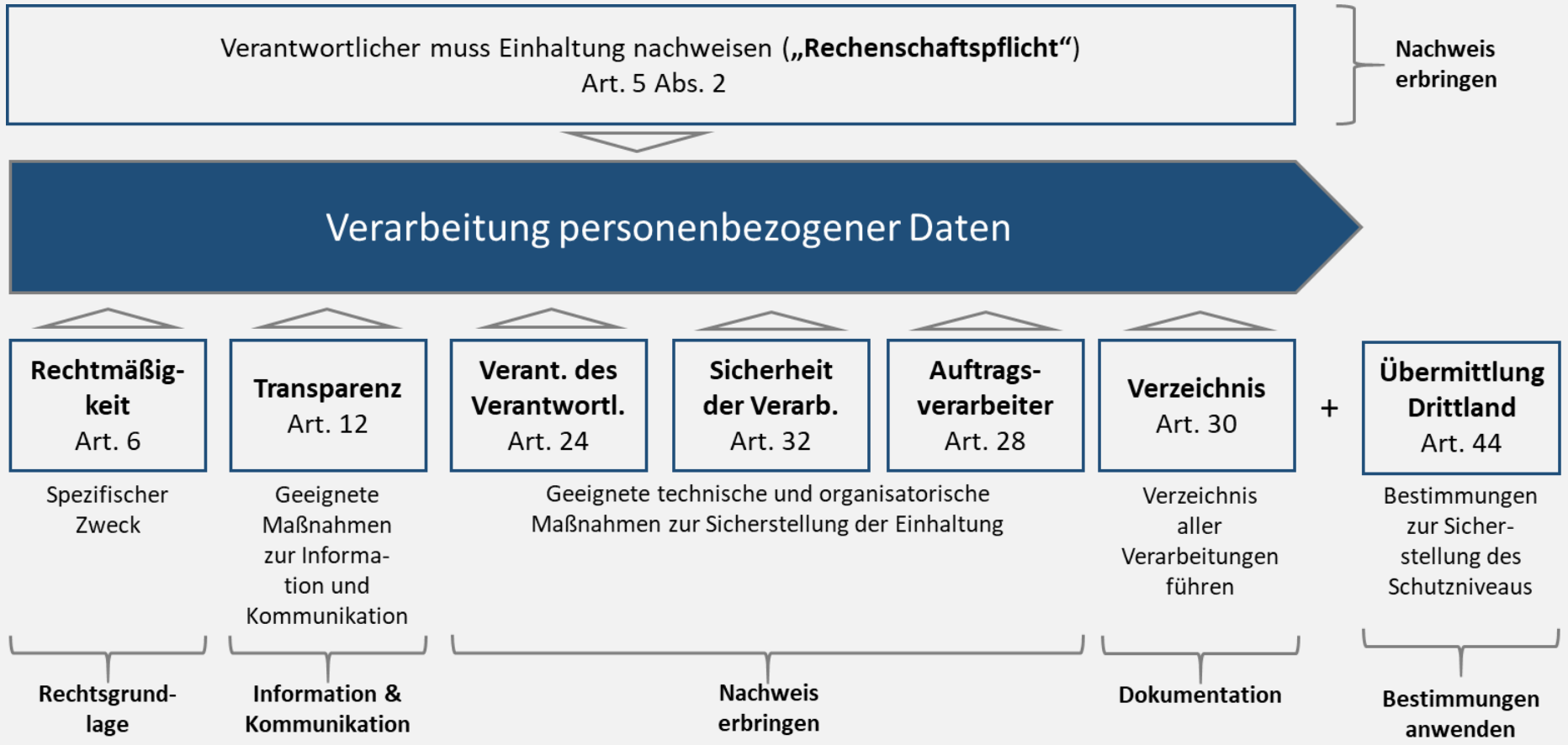
3 HAUPTBEREICHE UMSETZEN

- Datenschutzkonforme Verarbeitung
- Sicherstellung der Betroffenenrechte
- Meldung von Datenschutzverletzungen

3 HAUPTBEREICHE UMSETZEN

- Datenschutzkonforme Verarbeitung
- Sicherstellung der Betroffenenrechte
- Meldung von Datenschutzverletzungen

DATENSCHUTZKONFORME VERARBEITUNG



Quelle:
Kranig, Sachs, Gierschmann – Datenschutz-Compliance nach der DS-GVO

DOKUMENTATIONSPFLICHTEN

Bereich	Beschreibung	Artikel	
Rechenschaftspflicht	Nachweis zu erbringen. Wie – nicht genannt	5	☐
Rechtmäßigkeit	Rechtsgrundlagen der Verarbeitung	6	☐
Einwilligung	Einwilligungserklärungen	7	☐
Besondere Kategorien	Ausdrückliche Einwilligung	9	☐
Identifizierung	Nachweis, wenn Betroffener nicht identifiziert werden konnte	11	☐
Erhebung beim Betroffenen	Information an Betroffenen	13	☐
Erhebung durch Dritten	Information an Betroffenen bei Verwendung	14	☐

DOKUMENTATIONSPFLICHTEN

Bereich	Beschreibung	Artikel	
Datenschutzkonforme Verarbeitung	Dokumentation (Maßnahmen, Risikobewertung,…) für Nachweis	24	☐
Privacy by Design/Default	Rechtsgrundlagen der Verarbeitung	25	☐
Gemeinsame Verarbeitung (Artikel 26)	Regelung der Zuständigkeiten	26	☐
Keine EU Niederlassung	Benennung eines Vertreters	27	☐
Auftragsverarbeiter	ADV-Vertrag, weitere Dokumente zu Sicherheit der Verarbeitung	28	☐
Verarbeitung unter Aufsicht (Artikel 29)	Weisungen (schriftliche?)	29	☐

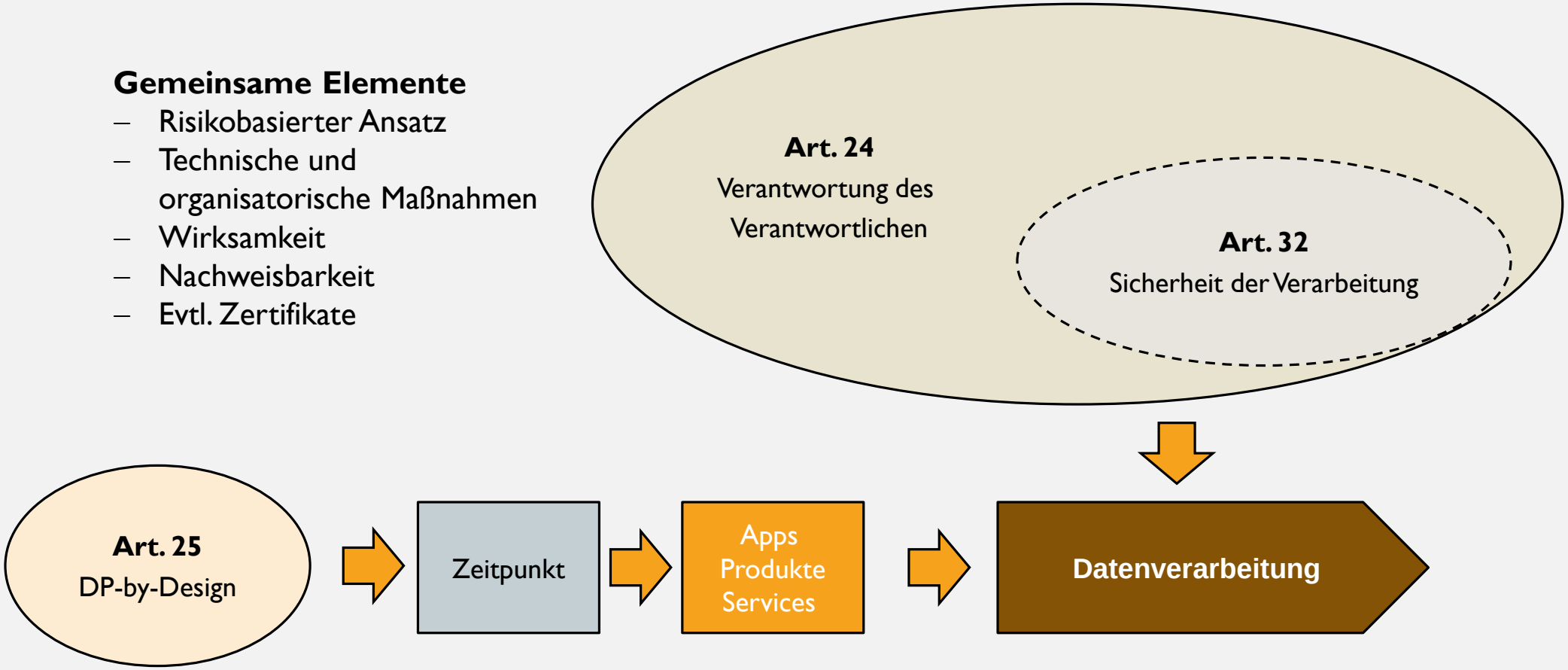
DOKUMENTATIONSPFLICHTEN

Bereich	Beschreibung	Artikel	
Verarbeitungsverzeichnis	Verzeichnis + Prozess zum Change-Management	30	☐
Sicherheit der Verarbeitung	Dokumentation für Nachweis, Risikobeurteilung, Prozess zur Überprüfung der Wirksamkeit	32	☐
Datenschutzfolge-abschätzung	Dokumentation gemäß Art. 35 Abs. 7 + Prozess/Methode zur Durchführung	35	☐
Konsultation	Dokumentation der Konsultation	36	☐
Drittlandübermittlung	Geeignete Garantie	44-47	☐

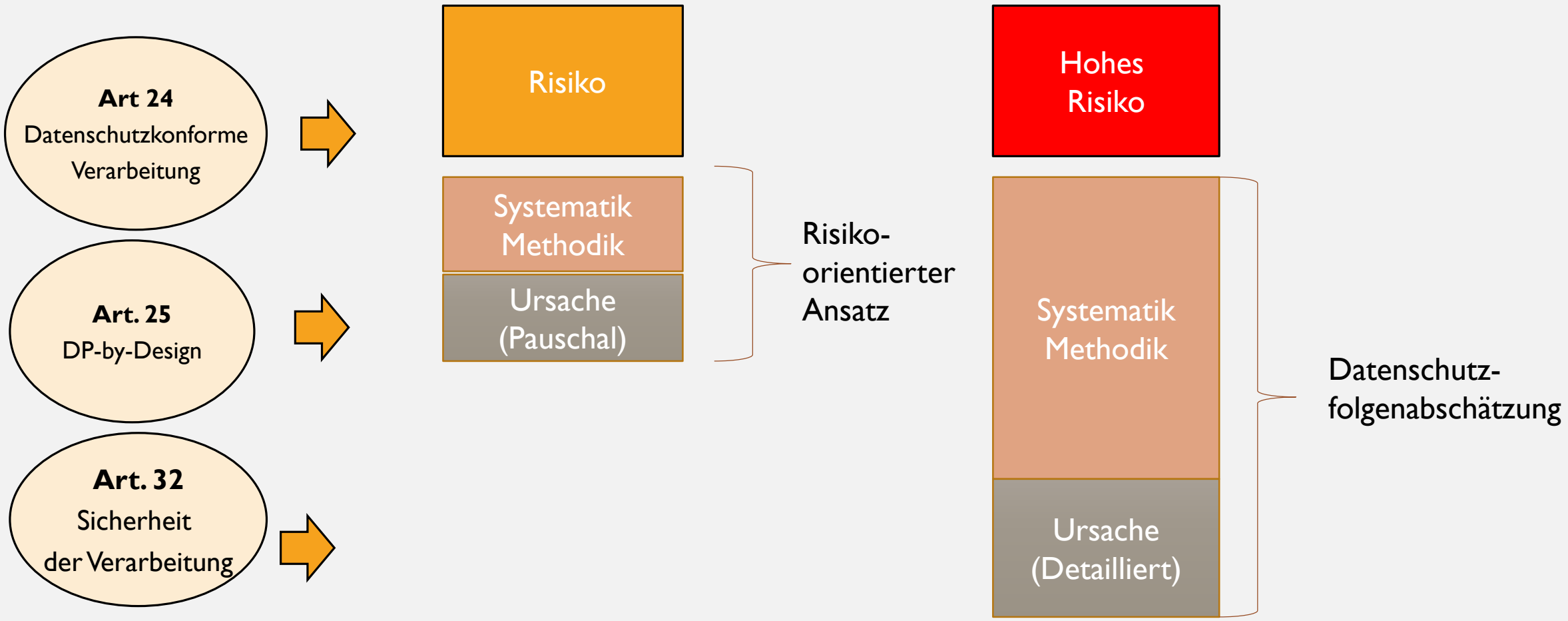
TECHNISCHER DATENSCHUTZ

Gemeinsame Elemente

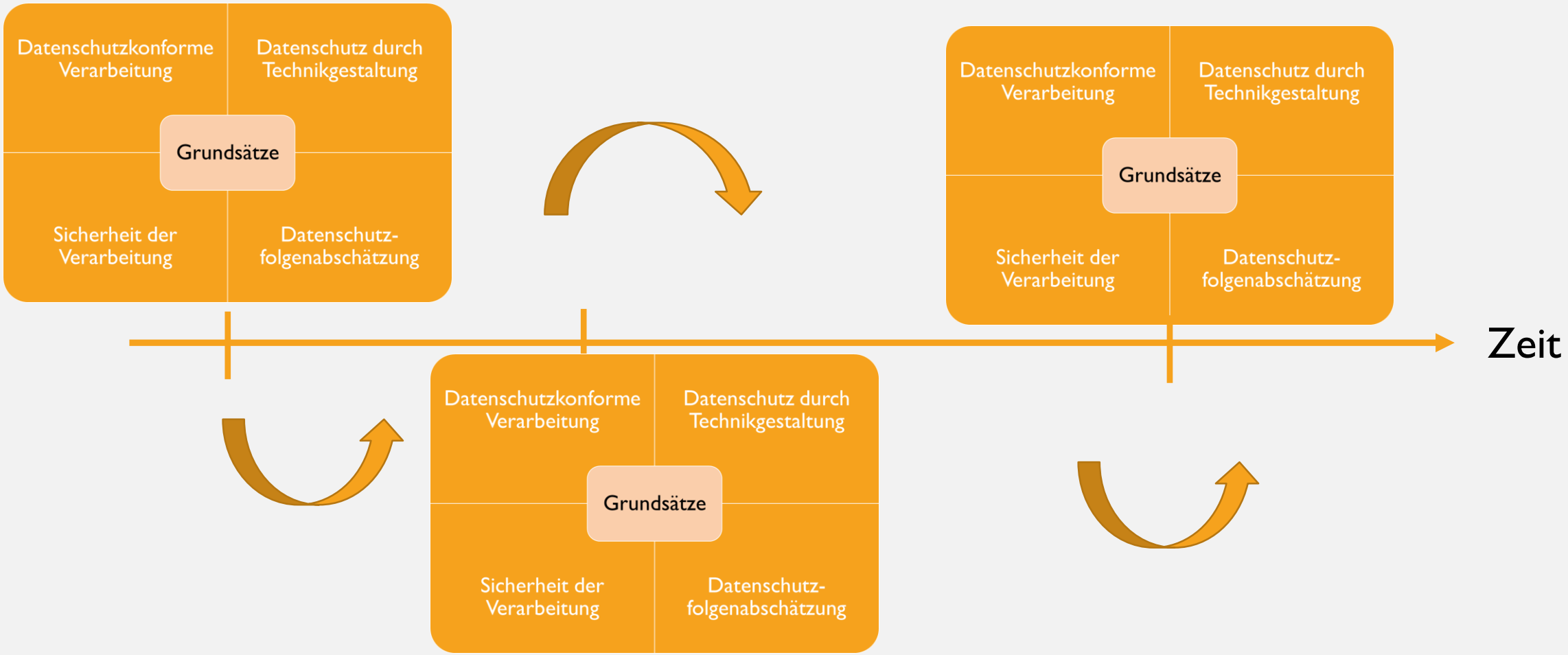
- Risikobasierter Ansatz
- Technische und organisatorische Maßnahmen
- Wirksamkeit
- Nachweisbarkeit
- Evtl. Zertifikate



RISKO VS. DATENSCHUTZFOLGENABSCHÄTZUNG



PRIVACY BY DESIGN



3 HAUPTBEREICHE UMSETZEN

- Datenschutzkonforme Verarbeitung
- Sicherstellung der Betroffenenrechte
- Meldung von Datenschutzverletzungen

INFORMATIONSPFLICHTEN

Transparente Information, Kommunikation und Modalitäten
Art. 12

Erhebung beim Betroffenen
Art. 13

Erhebung bei Drittem
Art. 14

Bildet **Basis** für die Ausübung der **Betroffenenrechte** (z.B. Recht auf Auskunft)

Zwei Zielsetzungen:
Ziel 1: Allgemeine Informationen (Art. 13 Abs. 1)
Ziel 2: Umsetzung der fairen und transparenten Verarbeitung (Art. 13 Abs. 2)

Bei Dritten: Zusätzlich Datenkategorien und Quelle der Informationen angeben

BETROFFENENRECHTE

Transparente Information, Kommunikation und Modalitäten
Art. 12

Auskunft
Art. 15

Berichtigung, Löschung, Einschränkung
Art. 16 - 19

Datenübertragbarkeit
Art. 20

Widerspruch
Art. 21

Automatisierte Entscheidungen
Art. 22

Widerruf der Einwilligung
Art. 7 Abs. 3

RECHT AUF AUSKUNFT (Z.B.)

- **Auskunft muss sich beziehen auf:**
  - Verarbeitungszwecke
  - Kategorien personenbezogener Daten
  - Empfänger oder Kategorien von Empfängern
  - Speicherdauer, mindestens Kriterien für Speicherdauer
  - Beschwerderecht bei Aufsichtsbehörde
  - Information über Herkunft der Daten
  - Wenn automatisierte Entscheidungsfindung: involvierte Logik
  - Wenn Übermittlung in Drittland: Info über geeignete Garantien

- **Frist für Auskunft:**
  - Unverzüglich
  - Jedenfalls innerhalb eines Monats
  - Verlängerung um zwei Monate bei Komplexität
- **Form der Auskunft:**
  - Kopie der personenbezogenen Daten (erste Kopie kostenlos)

RECHT AUF LÖSCHUNG (Z.B.)

- **Löschverlangen** begründet bei:
  - Wegfall des Zwecks
  - Wegfall der Rechtsgrundlage
  - Widerspruch und keine Gründe für weitere Verarbeitung
  - Unrechtmäßigkeit der Verarbeitung
  - Spezielleres Gesetz fordert Löschung
  - Widerruf der Einwilligung eines Kindes

- **Keine Pflicht zur Löschung** bei:
  - Recht auf freie Meinungsäußerung
  - Erfüllung einer rechtlichen Verpflichtung
  - Öffentliches Interesse
  - Archiv- oder Forschungszwecke
  - Geltendmachung von Rechtsansprüchen

Achtung:

Dass Software Löschung „nicht kann“, ist kein Grund für Nichtlöschung

RECHT AUF DATENÜBERTRAGBARKEIT (Z.B.)

- Betroffene Person kann vom Verantwortlichen **verlangen**, dass sie Daten, die sie ihm bereitgestellt hat,
  - in einem strukturierten, gängigen und maschinenlesbaren Format erhält und
  - ohne Behinderung durch den Verantwortlichen einem anderen Verantwortlichen übermitteln kann (soweit „technisch machbar“, kann sogar verlangt werden, dass der Verantwortliche die Daten gleich direkt an den neuen Verantwortlichen übermittelt).

- **Keine Pflicht** zur Übermittlung u.a.:
  - Für Erkenntnisse aus bereitgestellten Daten
  - Bei Verletzung Rechte Dritter
  - Verarbeitung im öffentlichen Interesse

3 HAUPTBEREICHE UMSETZEN

- Datenschutzkonforme Verarbeitung
- Sicherstellung der Betroffenenrechte
- Meldung von Datenschutzverletzungen

DATENSCHUTZVERLETZUNG

- Eine Verletzung des Schutzes personenbezogener Daten (kurz „Datenschutzverletzung“) ist gemäß Art. 4 Nr. 12 eine **Verletzung der Sicherheit**, die

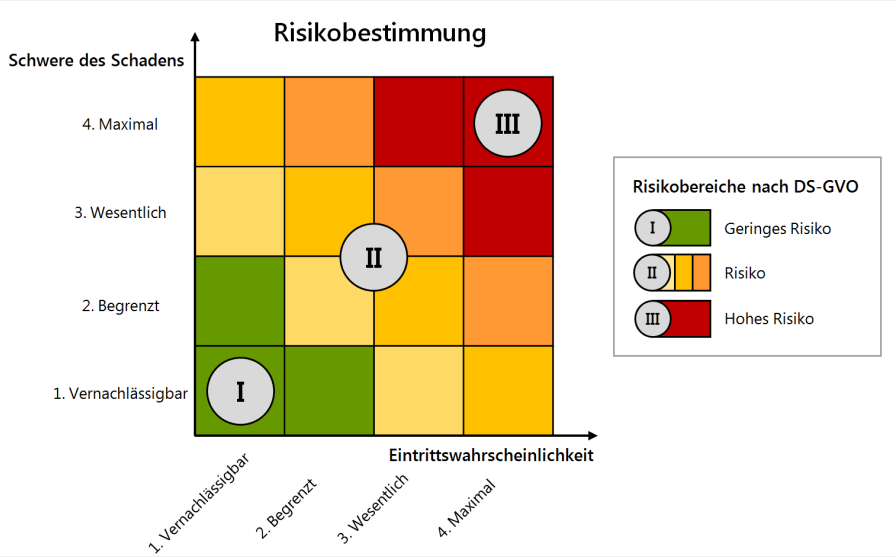
  - ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust oder zur Veränderung (**Verlust der Verfügbarkeit bzw. Integrität**) oder
  - zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten (**Verlust der Vertraulichkeit**)

  führt.

MELDUNG AN AUFSICHTSBEHÖRDE

- **Grundsatz**:
  Im Falle einer Verletzung des Schutzes personenbezogene
  Verantwortliche diese der zuständigen Aufsichtsbehörde
  1.

- **Ausnahme**:
  Der Verantwortliche stellt feststellt, dass die Verletzung v
  zu einem Risiko für die Rechte und Freiheiten von nat
  führt (was zu dokumentieren ist).

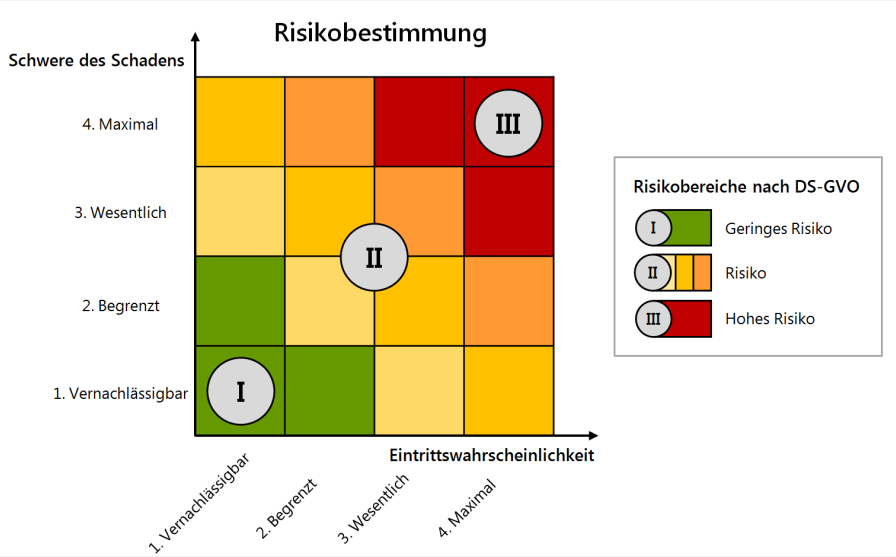


MELDUNG AN AUFSICHTSBEHÖRDE

- **Frist**: „unverzüglich und möglichst binnen 72 Stunden“
- **Inhalt**:
  - Kontaktdaten DSB
  - Beschreibung von: (Ergänzung möglich)
    - Art der Verletzung,
    - Kategorien, Anzahl Personen und Datensätze
    - Wahrscheinliche Folgen der Verletzung
    - Vom Verantwortlichen ergriffene bzw. geplante Maßnahmen
- **Dokumentation** der Verletzung

MELDUNG AN BETROFFENEN

- **Voraussetzung:** Hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen
- **Frist**: unverzüglich
- **Inhalt**: (*in klarer und einfacher Sprache*)
  - Beschreibung von:
    - Art der Verletzung,
    - Name und Kontaktdaten DSB
    - Wahrscheinliche Folgen der Verletzung
    - Vom Verantwortlichen ergriffene bzw. geplante Maßnahmen



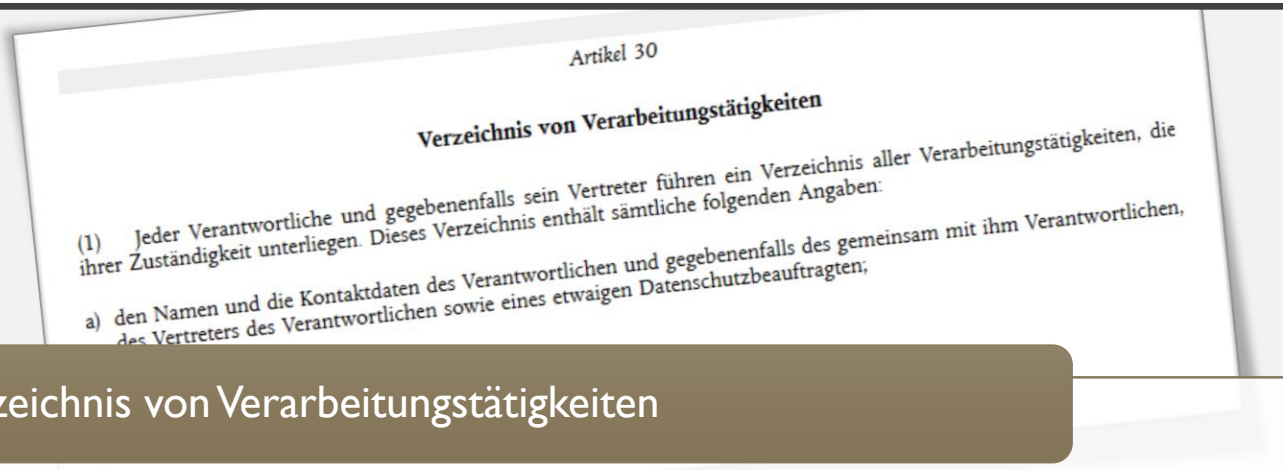
MELDUNG AN BETROFFENEN

- **Vorbereitung auf Meldung wegen Datenschutzverletzungen**

  - ErwGr. 87: *Es sollte festgestellt werden, ob alle geeigneten technischen Schutz- sowie organisatorischen Maßnahmen getroffen wurden, um sofort feststellen zu können, ob eine Verletzung des Schutzes personenbezogener Daten aufgetreten ist, und um die Aufsichtsbehörde und die betroffene Person umgehend unterrichten zu können.*

  - Daraus folgt: **Pflicht zur Vorbereitung** auf Datenschutzverletzungen!

VERZEICHNIS DER VERARBEITUNGSTÄTIGKEITEN



Artikel 30

Verzeichnis von Verarbeitungstätigkeiten

(1) Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgenden Angaben:

a) den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;

Verzeichnis von Verarbeitungstätigkeiten

- Gehört zu den **Pflichten** der Verantwortlichen und Auftragsverarbeiter (Kapitel IV DS-GVO)
- Fokus: **Verarbeitungstätigkeiten**
- Es ist ein Verzeichnis aller Verarbeitungstätigkeiten **schriftlich** zu führen (auch elektronisch möglich)
- Verzeichnis wird der **Aufsichtsbehörde** auf Anfrage zur Verfügung gestellt

VERZEICHNIS DER VERARBEITUNGSTÄTIGKEITEN

BDSG	DS-GVO	Änderungen
(Muss nicht immer erstellt werden)	(faktisch immer)	(KMUs müssen evtl. keines mehr erstellen. Nur wenn z.B. kein Risiko)
Name Verantwortliche Stelle	Name und Kontaktdaten der Verantwortliche Stelle	Kontaktdaten
-	Name und Kontaktdaten des Datenschutzbeauftragten	Neu
Zweckbestimmung der Datenerhebung, -verarbeitung und -nutzung	Zwecke der Verarbeitung	Keine
Beschreibung der betroffenen Personengruppen	Beschreibung der Kategorien betroffener Personen	Keine
Beschreibung der Daten(-kategorien)	Beschreibung der Kategorien personenbezogener Daten	Keine
Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können	Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind	Keine
(geplante) Datenübermittlung in Drittstaaten	Übermittlungen an ein Drittland (samt Name des Landes)	Keine
Löschfristen	Löschfristen für Datenkategorien	Keine
Beschreibung der technischen und organisatorischen Maßnahmen	Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen	Keine

VERZEICHNIS DER VERARBEITUNGSTÄTIGKEITEN

Neu: Verzeichnis von Auftragsverarbeitern

- Alle Kategorien von Tätigkeiten, die im Auftrag durchgeführt werden

Inhalt:

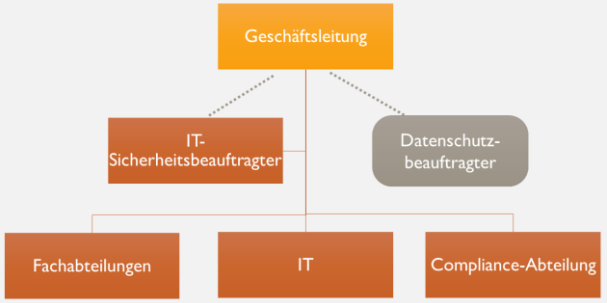
- Name/Kontaktdaten des Auftragsverarbeiters
- Name/Kontaktdaten **jedes Verantwortlichen**, in dessen Auftrag Tätigkeiten durchgeführt werden
- Name/Kontaktdaten des Datenschutzbeauftragten des Auftragverarbeiters und des jeweiligen Verantwortlichen
- Kategorien von Verarbeitungen, die im Auftrag durchgeführt werden
- Übermittlungen an ein Drittland (samt Name des Landes)
- Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen

VERARBEITUNGSVERZEICHNIS+

Erweiterung jeder Verarbeitung um:	Rechtsgrundlage der Verarbeitung
	Dokumentation, dass Einwilligung erteilt wurde
	Dokumentation, dass Verarbeitung für Betroffenen transparent erfolgt
	Dokumentation, dass Informationspflichten eingehalten werden
	Dokumentation, dass Datenschutz durch Technik eingehalten wird
	Dokumentation des Prozesses für Auskunft, Berichtigung und Löschung
	Umsetzung Speicherbegrenzung
	Umsetzung der Sicherheit der Verarbeitung
	Gemeinsame Verantwortlichkeiten
	Auflistung alle Auftragsdatenverarbeiter (inkl. Internationaler Datentransfer mit Rechtsgrundlagen)
	Umgang mit Datenschutzverletzungen
	Darstellung der Meldepflicht an Aufsichtsbehörden
	Verwendung von Werkzeug Zertifizierung
	Verwendung von Werkzeug Code of Conduct
	Risikobewertung / Datenschutzfolgeabschätzung
	Dokumentation durchgeführter Audits
	Dokumentation von Awareness-Maßnahmen
	Datenportabilität

„FORMEL“ ZUR RECHENSCHAFTSPFLICHT

AUFBAUORGANISATION



3 HAUPTBEREICHE UMSETZEN

- Datenschutzkonforme Verarbeitung
- Sicherstellung der Betroffenenrechte
- Meldung von Datenschutzverletzungen

\+ Dokumentation + Audit = Rechenschafts-pflicht

FRAGEN?