DIE EU-DATENSCHUTZ-GRUNDVERORDNUNG

- EIN ÜBERBLICK -

Die EU Datenschutz-Grundverordnung

Grundsätzliches zur Datenschutzgrundverordnung

Überblick über wesentliche Inhalte

Überblick zur Datenschutzorganisation

Ziele der Datenschutz-Grundverordnung (DS-GVO)

- Betroffene erhalten **mehr Kontrolle** über ihre Daten
- **Globale Standards** für Datenschutz werden gesetzt
- Datenschutzregeln **passend für den digitalen Binnenmarkt**
  - **Harmonisiert** (EUR 2,3 Milliarden Einsparungen durch Vereinheitlichung unterschiedlicher Datenschutzregeln)
  - **Vereinfacht** (EUR 130 Millionen Einsparung durch Abschaffung von Meldepflichten)
  - **Kein „Forum-Shopping“** (Datenverarbeitung in Mitgliedsstaat mit weniger strengem Datenschutzrecht)
  - **„One-Stop-Shop“** (eine zuständige Aufsichtsbehörde für Unternehmen in der Europäischen Union)
  - Effiziente **Kooperation** der Datenschutzaufsichtsbehörden
  - Mehr **Konsistenz** der Anwendung des Datenschutzrechts

Wirkungen der DS-GVO

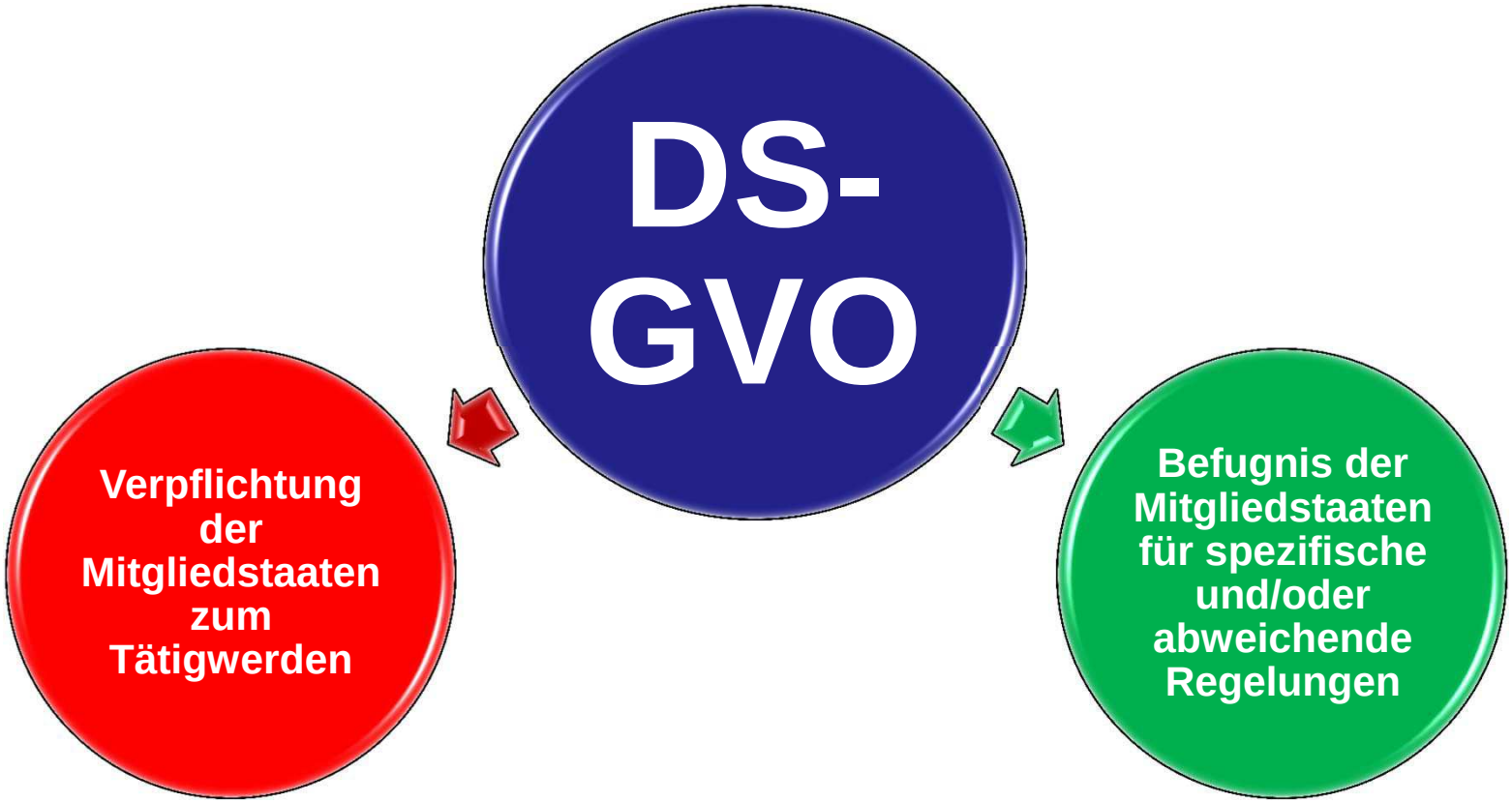
Art. 91:
„ … Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedsstaat.“

- Die DS-GVO ist eine allgemeine Regelung mit unmittelbarer innerstaatlicher Geltung

-> **„Durchgriffswirkung“**

- Grundsätzliche Vollharmonisierung im nicht-öffentlichen Bereich
- Ersetzt nationales Datenschutzrecht, führt grds. zur Unanwendbarkeit entgegenstehender nationaler Regelungen
- Öffnungsklauseln für nationalen Gesetzgeber in bestimmten Bereichen – Richtlinien-Charakter im öffentlichen Bereich
- Zweijährige Anpassungsphase für Rechtsbereinigung und Folgeänderungen

Öffnungsklauseln



Ca. 50 – 60 Öffnungsklauseln:

- bei Rechtsgrundlagen der Datenverarbeitung
- für spezifischere nationale Regelungen
- für Ausnahmen von Betroffenenrechten
- für andere Fälle

Auswirkung auf bestehende Regelungen

National

- **öffentlicher Bereich**: Fortbestand der wesentlichen allgemeinen und der bereichsspezifischen Regelungen
- **nicht-öffentlicher Bereich**: weitgehende Ersetzung durch DS-GVO
- Rechtsbereinigungsaufgaben im
  - BDSG
  - LDSG´s
  - bereichsspezifischen Datenschutzrecht wie Melderecht, Sozialrecht usw.
- Nicht betroffen sind z. B. (zunächst)
  - TMG ?
  - TKG
  - BetrVG
  - UWG

Europa

- EU-DS-Rili (RL 95/46/EG) wird aufgehoben
- E-Privacy-RL 2002/58 bleibt bestehen, aber Reformpflicht
- Reformpflicht der VO 45/2001
- Fortbestand (bis auf Widerruf) der
  - Angemessenheits-beschlüsse für Drittländer
  - BCR-Anerkennungen
  - Standardvertragsklauseln
  - Bestehenden Einwilligungen
- Aufbau des Europäischen Datenschutzausschusses

Anpassung in Deutschland

Insbesondere BDSG z. B.:

- DSB (§ 4f)
- Beschäftigten-datenschutz (§ 32)
- Aufsicht (§ 38)
- Sanktionen (§ 44)
- Zertifizierung
- …

Weitere gesetzliche Rege-lungen zum Datenschutz, insbesondere:

- Landesdaten-schutzgesetze
- SGB X
- Kirchliche DSG
- …

- Auch z. B. Datenschutz-kodex der Presse

Ausgestaltung / Überwachung

EuGH

- Auslegung der DS-GVO
- Kontrolle der Kommissionsentscheidungen

Kommission

- Überwachung der Umsetzung der DS-GVO
- Erlass delegierter Rechtsakte

DS-GVO

Europäischer Datenschutz-ausschuss

- Interpretation der DS-GVO
- Koordination der Zusammenarbeit

Nationale Gerichte

- Auslegung der DS-GVO und nationaler Datenschutz-Vorschriften

Mitgliedsstaaten

- Ergänzen und modifizieren den Rechtsrahmen

Aufsichtsbehörden

- Überwachung der Umsetzung des Datenschutzes (Zusammenarbeit)

Interpretation/Auslegung der Gesetze

DS-GVO

Keine gefestigte Interpretations- bzw. Auslegungshilfen:

- EuGH-Rechtsprechung bezieht sich auf Richtlinie 95/46/EG

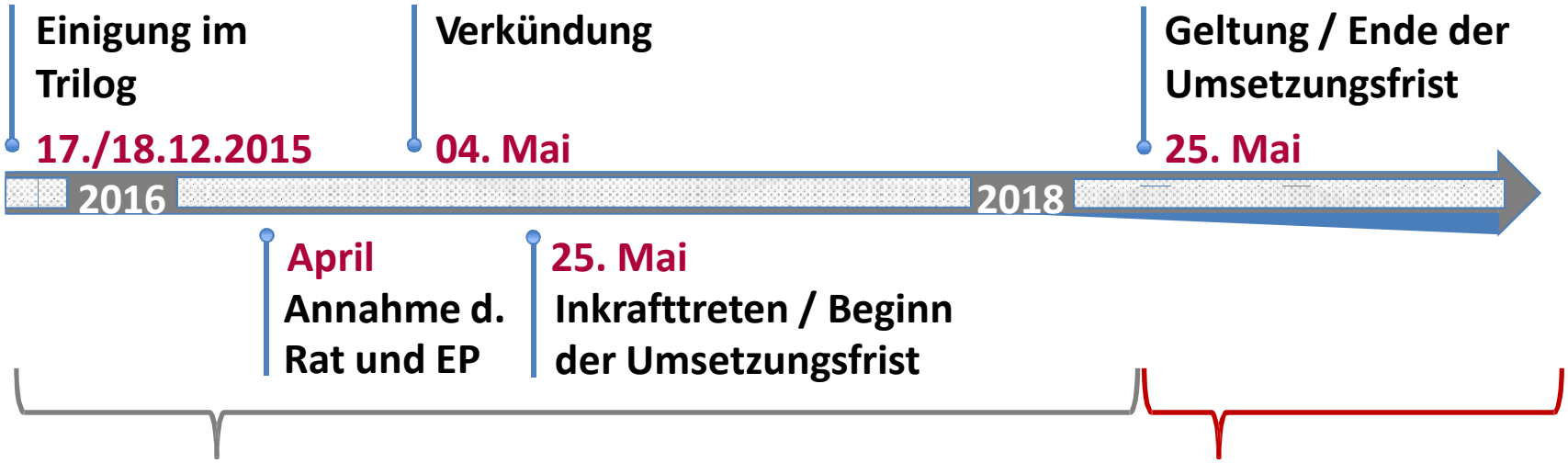
- Stellungnahmen/Orientierungshilfen des Europäischen Datenschutzausschusses müssen erst noch formuliert werden

- Kommentierungen aus der Literatur existieren noch nicht

➢ Unternehmen werden sich anfangs einer großen Rechtsunsicherheit bei der Auslegung der EU-DS-GVO stellen müssen.

➢ Eine Unterschiedliche Auslegungspraxis in den Mitgliedstaaten muss durch den Europäischen Datenschutzausschuss und den EuGH nivelliert werden.

Zeitliche Auswirkungen



- **BDSG gilt weiter**
- **Beginn der Umsetzungsfrist** (…Verarbeitungen, die zum Zeitpunkt des Inkrafttretens dieser Verordnung bereits begonnen haben, sollten innerhalb von zwei Jahren nach dem Inkrafttreten dieser Verordnung mit ihr in Einklang gebracht werden. … (EG 134))
- Ermächtigung der Kommission zum Erlass **delegierter Rechtsakte** (Art. 86 Abs. 2)

- **BDSG ist nicht mehr anwendbar**
- **Aufhebung** der EU-DS-Rili (RL 95/46/EG) (Art 88)
- **Verarbeitungen** müssen im Einklang mit der GVO sein
- **Ablauf** diverser Melde-/ Erklärungspflichten der Mitgliedsstaaten bezüglich nationaler Regelungen

Die EU Datenschutz-Grundverordnung

Grundsätzliches zur Datenschutzgrundverordnung

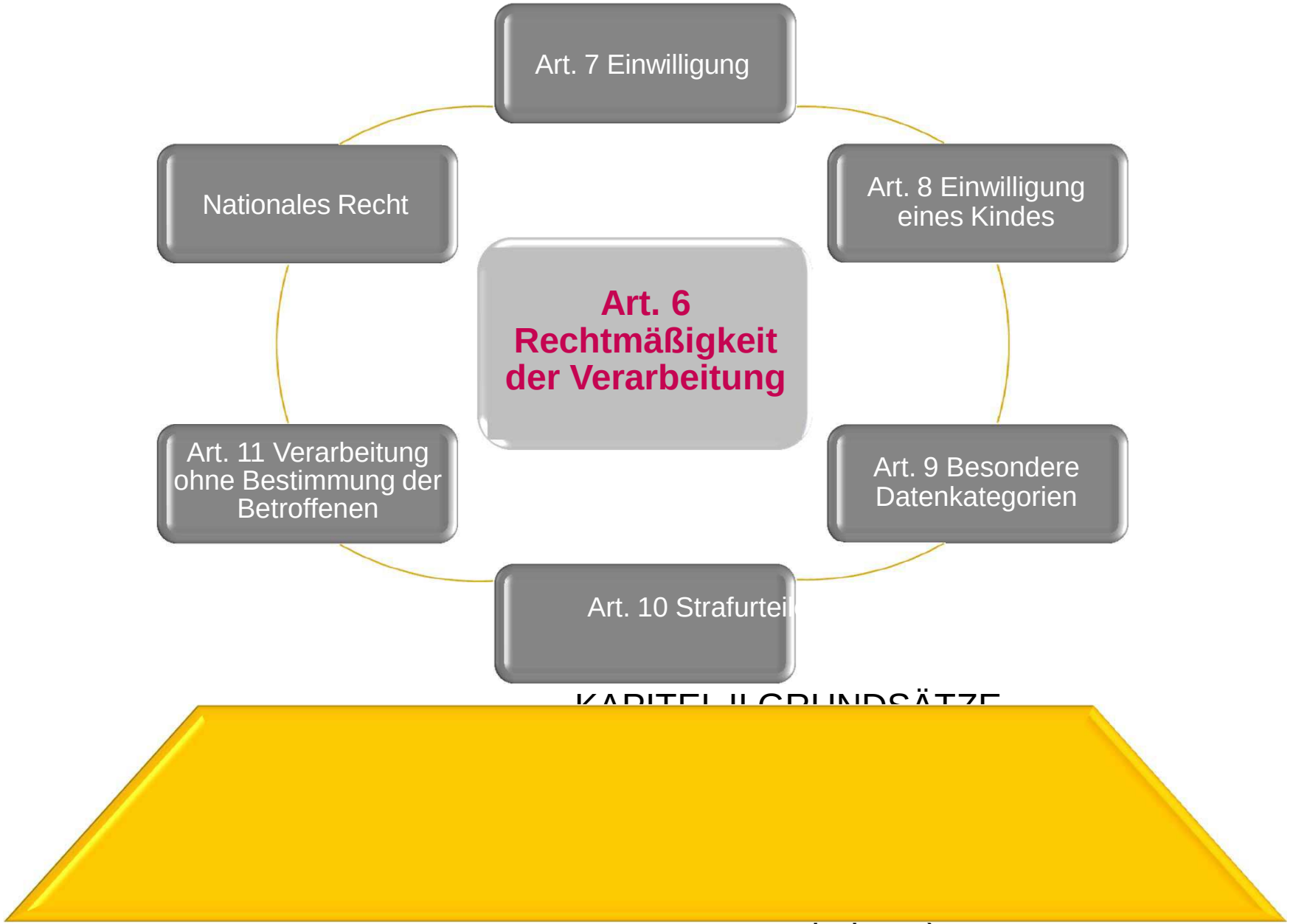
Überblick über wesentliche Inhalte

Überblick zur Datenschutzorganisation

Gliederung der DS-GVO

Kapitel I:	Allgemeine Bestimmungen Grundsätze
Kapitel II:	Rechte der betroffenen Person
Kapitel III:	Für die Verarbeitung Verantwortlicher und Auftragsverarbeiter
Kapitel IV:	Übermittlung personenbezogener Daten an Drittländer o. an internationale Organisationen
Kapitel V:	Unabhängigkeit der Aufsichtsbehörden Zusammenarbeit und Kohärenz Rechtsbehelfe, Haftung und Sanktionen
Kapitel VI:	Vorschriften für besondere Datenverarbeitungssituationen
Kapitel VII:	Delegierte Rechtsakte und Durchführungsrechtsakte
Kapitel VIII:	Schlussbestimmungen
Kapitel IX:	
Kapitel X:	
Kapitel XI:	

Reduzierte Verarbeitungstatbestände



Prinzipien zur Datenverarbeitung – Art. 5

Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz	• Verarbeitung auf rechtmäßige Weise, nach dem Grundsatz von Treu und Glauben und in einer für den Betroffenen nachvollziehbaren Weise
Zweckbindung	• Erhebung für festgelegte, eindeutige und rechtmäßige Zwecke und Verbot der Weiterverarbeitung in einer mit diesen Zwecken nicht zu vereinbarenden Weise
Datenminimierung	• Beschränkung auf das für den Zweck der Verarbeitung angemessene und sachlich relevante sowie notwendige Maß
Richtigkeit	• sachlich richtige und ggf. aktuellste Daten, Vorsehen von Maßnahmen zur unverzüglichen Löschung oder Berichtigung von unzutreffenden Daten
Speicherbe-grenzung	• Speicherung mit Personenbezug höchstens so lange, wie es für die Verarbeitungszwecke erforderlich ist;
Integrität und Vertraulichkeit	• geeignete TOM zum angemessenen Schutz der Daten insbes. vor unbefugter oder unrechtmäßiger Verarbeitung, zufälligem Verlust, zufälliger Zerstörung oder Schädigung

Rechenschafts-pflicht (Account-ability):

- Verantwortung und
- Nachweispflicht

für die Einhaltung der Prinzipien

Datenportabilität

Art. 20

- Erweiterung des Auskunftsrechts: Recht auf Erhalt einer Kopie seiner Daten
- Erweiterung durch Portierbarkeit der Daten zu einem Wettbewerbsdienst
- Eine Kopie kann vom Betroffenen herausverlangt werden als strukturiertes, gängiges und maschinenlesbares Format

– „Strukturiert“ bedeutet Datenbankformat (XML; komma-separierte Liste, SQLite usw.)

- hinderungsfreie Übermittlung an andere Stelle, ggf. Direktübermittlung (Abs. 2a)
- Gilt nur bei Verarbeitung aufgrund Einwilligung oder Vertrag.
- **AUSNAHME:** Die Portierung beeinträchtigt Rechte und Freiheiten anderer Personen
- **ACHTUNG:** Im Text keine Beschränkung auf Internetdienste!

Schnittstellen für die Datenportabilität müssen vorhanden sein

„Recht auf Vergessenwerden“

Art. 17 Abs. 2

- Vom Verantwortlichen veröffentlichte Daten sind nach den Vorgaben des Art. 17 Abs. 1 zu löschen (vorbehaltlich der Ausnahmen nach Art. 17 Abs. 3).
- **Zudem:** Information anderer für die Datenverarbeitung Verantwortlicher über das Verlangen des Betroffenen zur Löschung
  - aller Links zu diesen personenbezogenen Daten oder
  - von Kopien oder Replikationen dieser Daten
- Berücksichtigung der verfügbaren Technologie und der Implementierungskosten
- Vergleichbar § 35 VII

Die EU Datenschutz-Grundverordnung

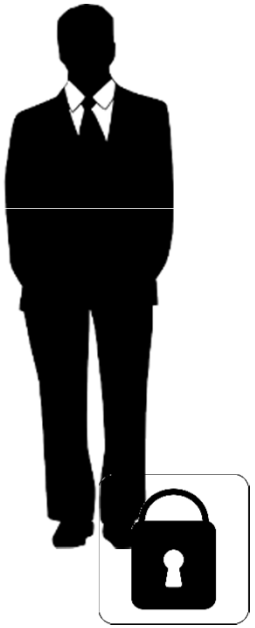
Grundsätzliches zur Datenschutzgrundverordnung

Überblick über wesentliche Inhalte

Überblick zur Datenschutzorgnisation

Schutzkonzept

DSB: Evolution der Aufgabenstellung



Sicherstellungsauftrag

(§ 29 Abs. 1 BDSG 1977 /
§ 37 Abs. 1 BDSG 1990)

Hinwirkungsauftrag

(§ 4g Abs. 1 BDSG 2001)

Überwachungsauftrag

(Art 39 Abs. 1 DS-GVO 2016)

Datenschutzbeauftragter – Bestellpflicht – Art. 37

Verpflichtend

- Öffentliche Stellen
- Unternehmen

→ *Kerntätigkeit besteht aus Verarbeitungs- vorgängen, welche auf Grund ihres Wesens, ihres Umfangs und/oder ihrer Zwecke eine regelmäßige und systematische Beobachtung [monitoring] von betroffenen Personen erforderlich machen*

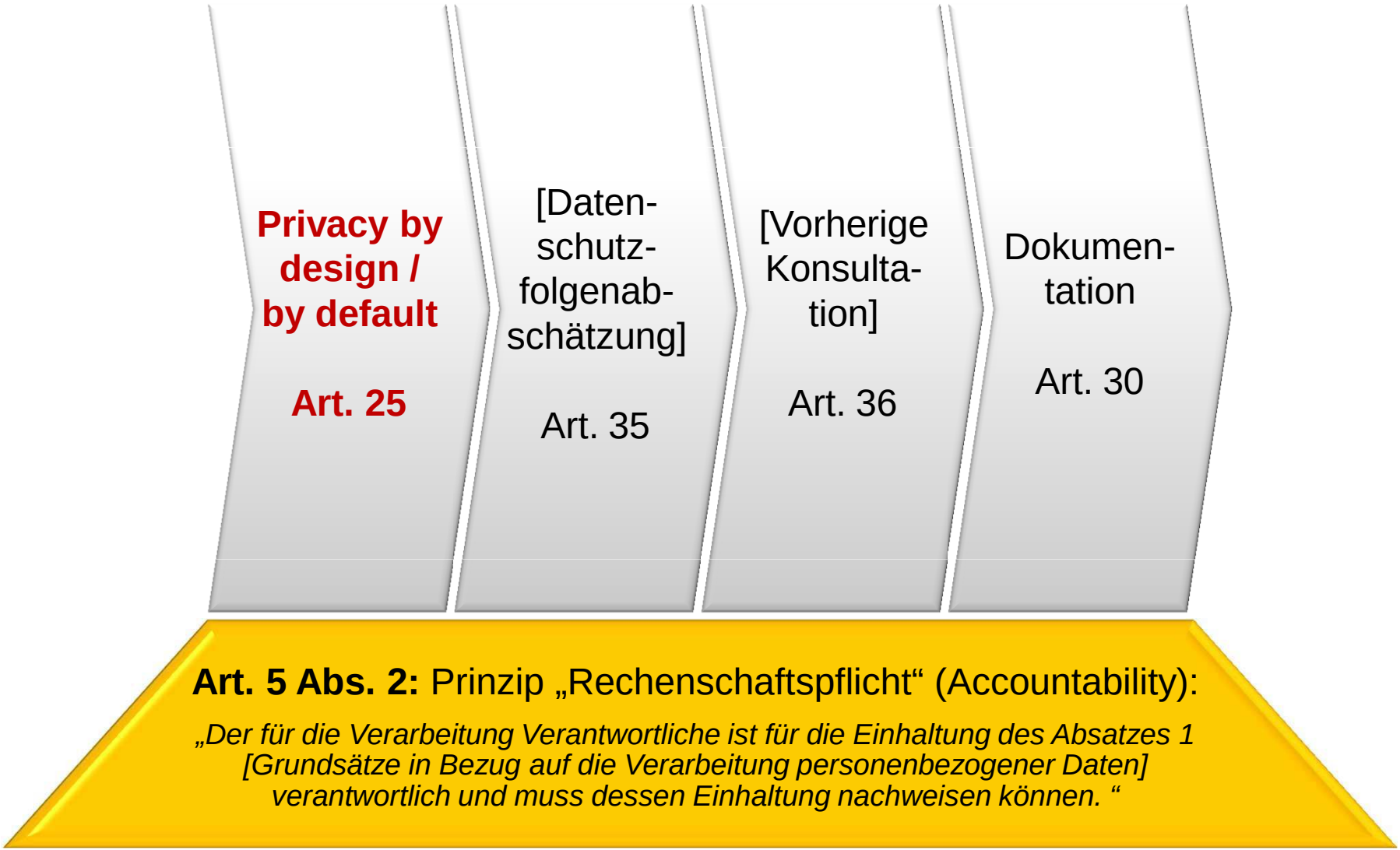
→ *Datenverarbeiter, deren Kerntätigkeit aus der Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 und 9a der DS-GVO in großem Umfang besteht*

- Nationale Öffnungsklausel: Nachfolgeregelung zu § 4f

Freiwillig

- Alle übrigen für die Verarbeitung Verantwortlichen

Verarbeitungen / Prozesse



Privacy by design / Privacy by default

Privacy by design

Unter Berücksichtigung des Stands der Technik … angemessene technische und organisatorische Maßnahmen …, mit denen die **wirksame Umsetzung der Datenschutzgrundsätze** wie etwa Datenminimierung und die Aufnahme der notwendigen Garantien in die Verarbeitung **erreicht werden sollen**, ...

Privacy by default

Der für die Verarbeitung Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass ***durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden***; …

Nachweis durch Zertifizierung nach Art 42 möglich

Möglichkeiten müssen in der Software implementiert sein Produkt-Zertifizierung ist möglich

Datenschutz-Folgenabschätzung

Art. 35

3. Die Folgenabschätzung enthält zumindest Folgendes:

(a)eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem für die Verarbeitung Verantwortlichen verfolgten berechtigten Interessen;

(b)eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;

(c)eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1;

(d)die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht werden soll, dass die Bestimmungen dieser Verordnung eingehalten werden, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

Ausreichende Dokumentationen hierzu müssen vorhanden sein

Sicherheit der Verarbeitung – Art. 32

- Angemessen, unter Beachtung insbes. des „Stands der Technik“, Risikoadäquat
- Fokussierung auf die IT-Sicherheitsziele:
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit
- Sicherheitsmanagement

Als Dienstleister müssen ausreichende Nachweise zur Verfügung gestellt werden können

Verzeichnis von Verarbeitungstätigkeiten - Art. 30

- Verantwortlicher:

„Verzeichnis aller Verarbeitungstätigkeiten”

- Auftragsverarbeiter:

Kundenbezogene Aufzeichnung der “durchgeführten Tätigkeiten …”

- Nicht öffentlich / Einsicht für Aufsichtsbehörden
- Dokumentation ähnlich Verfahrensverzeichnis
- Zusätzlich aufzunehmen: Beurteilung und Garantien bei Drittlandsübermittlungen gemäß Art. 49 Abs. 1 (g)
- Ausnahmen für Unternehmen unter 250 MA – häufig nicht einschlägig
- **Achtung:** Daneben bestehen weitere Dokumentationspflichten

Dokumentations- und Nachweispflichten

Dokumentationspflichten z. B.

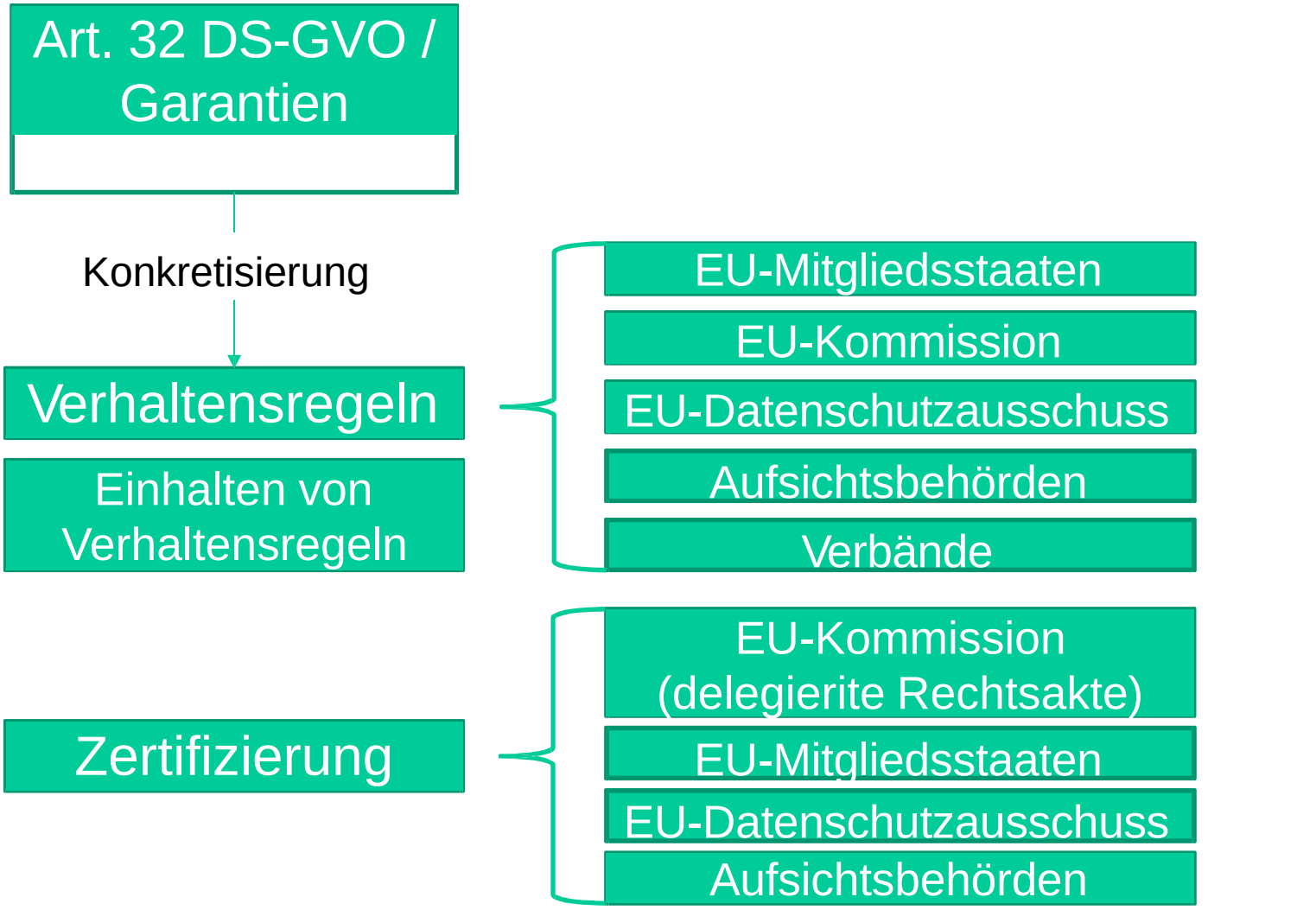
- Art 30 2 (a)
  - Dokumentierte Weisungen
  - Dokumentierte Weisung für Verarbeitung im Drittland
- Art 30: Verzeichnis von Verarbeitungstätigkeiten
- Art 33: Dokumentation aller Verletzungen des Schutzes personenbezogener Daten
- Art 46 Abs. 5: Dokumentation von Abwägungen und Garantien bei Drittlandübermittlungen

Nachweispflichten z. B.

- Art 5 Abs. 2: Nachweis der Einhaltung der Verarbeitungsprinzipien
- Art 7: Nachweis der Einwilligung
- Art 12: Nachweis der Unbegründetheit des Antrags
- Art 22: Nachweis für die Erforderlichkeit der Verarbeitung
- Art 24: Nachweis für die rechtmäßige Verarbeitung
- Art 26: Nachweis im Rahmen der Kontrolle
- Art 35: Nachweis zur Einhaltung der DS-GVO

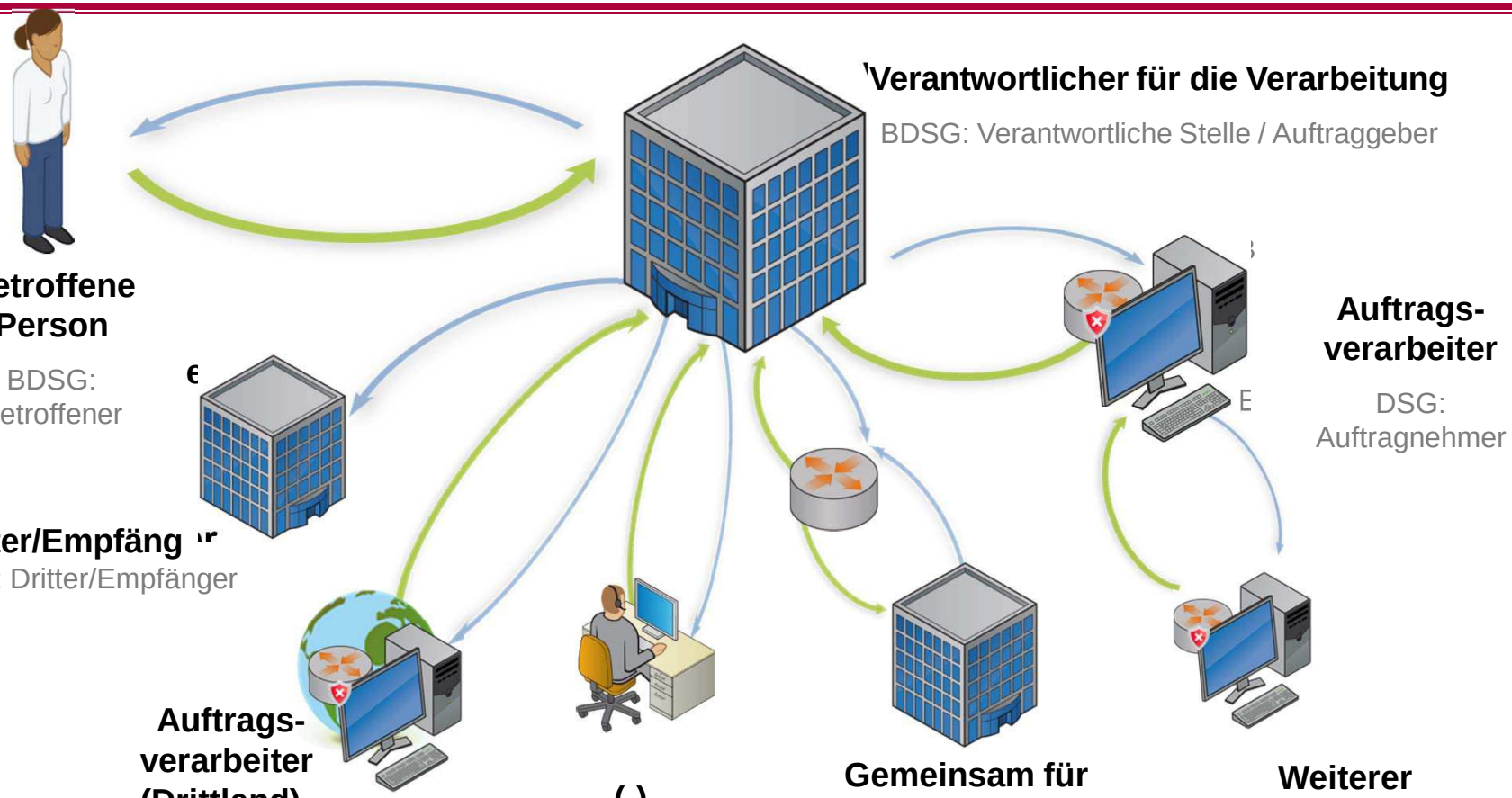
Viele Dokumentationen und Nachweise müssen erbracht werden können

Nachweis der IT-Sicherheit



Viele Nachweise können über Zertifizierung erbracht werden
ISO- Zertifikate etc. entsprechen dem (bisher) nicht

Zusammenarbeit mit Dienstleistern



Der Dienstleister ist selbst Normadressat
Eigene Pflichten gegenüber Unterauftragnehmern
…

Sanktionen - Systematik

Rechtswege:

- Beschwerde **bei** Aufsichtsbehörde
- Gerichtsverfahren **gegen** Aufsichts-behörde
- Gerichtsverfahren gegen Verantwort-lichen für die Verar-beitung / Auftrags-verarbeiter

Vertretung:

- Vertretung des Betroffenen durch einen Verband
- Verbandsklage-recht

(nach nationalem Recht)

Sanktionen:

- Schadensersatz
- Bußgeld
- Strafe (nach nationalem Recht)

Verschärfung der Bußgeldvorschriften, Art. 83 Abs. 4, 5, 6

o Bis zu 10.000.000 EUR oder im Fall eines Unternehmens bis zu 2 % seines weltweiten Jahresumsatzes, je nach dem, was höher ist	Pflichten gemäß den Artikeln 8, 11, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 42 und 43;	Verantwortliche; Auftragsverarbeiter
	42, 43	Zertifizierungsstelle
	41 Abs. 4	Überwachungsstelle
o Bis zu 20.000.000 EUR oder im Fall eines Unternehmens bis zu 4 % seines weltweiten Jahresumsatzes, je nach dem, was höher ist	Verstöße gegen die folgenden Bestim-mungen: Artikel 5, 6, 7 und 9, 12-22, 44-49, 58 Abs. 1, 2,	Verantwortliche, Auftragsverarbeiter

Berücksichtigung erschwerender und erleichternder (z. B. Zertifizierung) Tatsachen aber:
In jedem Fall
“wirksam, verhältnismäßig und abschreckend”

Vielen Dank für Ihre Aufmerksamkeit!