IWM Workshop „Grundlagen Datenschutzrecht + Datenschutz in der Praxis“ - (EU-DS-GVO + Privacy by Design/ Privacy by Default)

30.11.2017 Tübingen

Wer?

- Professur für **Medienrecht und Medienpolitik** in der digitalen Gesellschaft, Hochschule der Medien (HdM) Stuttgart
- Institut für Digitale Ethik (IDE), Hochschule der Medien Stuttgart
- Zuvor: Rechtsanwalt
- Vorsitzender des Wissenschaftlichen Beirats der Gesellschaft für Datenschutz und Datensicherheit (GDD)
- Aktuelle Forschungs- und Veröffentlichungsprojekte: Kooperative Fahrer-Fahrzeug-Interaktion (KoFFI); Learning Analytics für Prüfungsleistungen und Studienerfolg (LAPS)
- Kommentierung Art. 25 DS-GVO, in:

GDD
Gesellschaft für Datenschutz und Datensicherheit e.V.

IDE

HOCHSCHULE DER MEDIEN

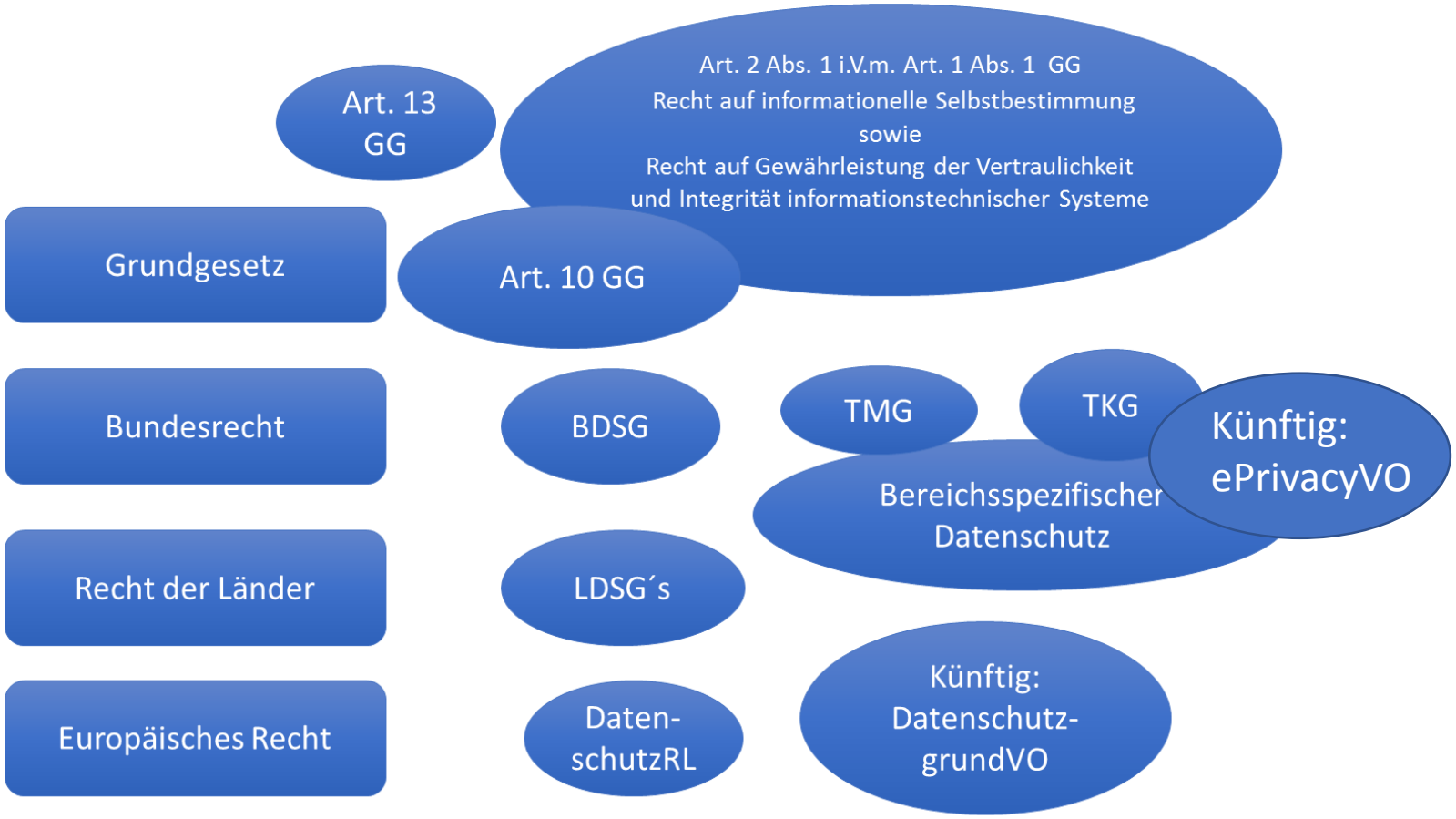
Agenda

- **Teil I:**
  - **Überblick Datenschutzrecht**
  - **Europäische Vorgaben: von der Richtlinie zur Verordnung**
  - **DS-GVO: Grundlagen, Prinzipien, Neuerungen**
- **Teil II**
  - **Details Privacy by Design (Artikel 25 Abs. 1 DS-GVO)**
  - **Details Privacy by Default (Artikel 25 Abs. 2 DS-GVO)**

Teil I: Überblick DS-GVO

Hintergrund, Rechtscharakter, Grundprinzipien

Überblick Datenschutzrecht - Rechtsquellen



Hintergrund zur DSGVO - Basisdaten

Titel: Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG
Kurz: Datenschutz-Grundverordnung (DSGVO)

Rechtsnatur: Verordnung (unmittelbar geltend) *mit Öffnungsklauseln*

Geltungsbereich: Europäische Union

Zeitliche Abfolge:

1995	2011	2016	2018
Dezember	November	Mai	25. Mai
Inkrafttreten der Datenschutz-Richtlinie	Erster Entwurf der DSGVO	Veröffentlichung + Inkrafttreten der DSGVO	Verbindliche Anwendung der DSGVO

Von der Richtlinie zur Verordnung - Ausgangssituation

- Datenschutz-Richtlinie 95/46: Umsetzung „bunt“:
  - Nationale Sonderregelungen bspw. zur Werbung, Adresshandel, Scoring
- Datenschutz-Richtlinie **95**/46

DS-GVO – Ziele/Ideen

Modernisierung des Datenschutzrechts

EU-weite *einheitliche Standards* zum Datenschutz

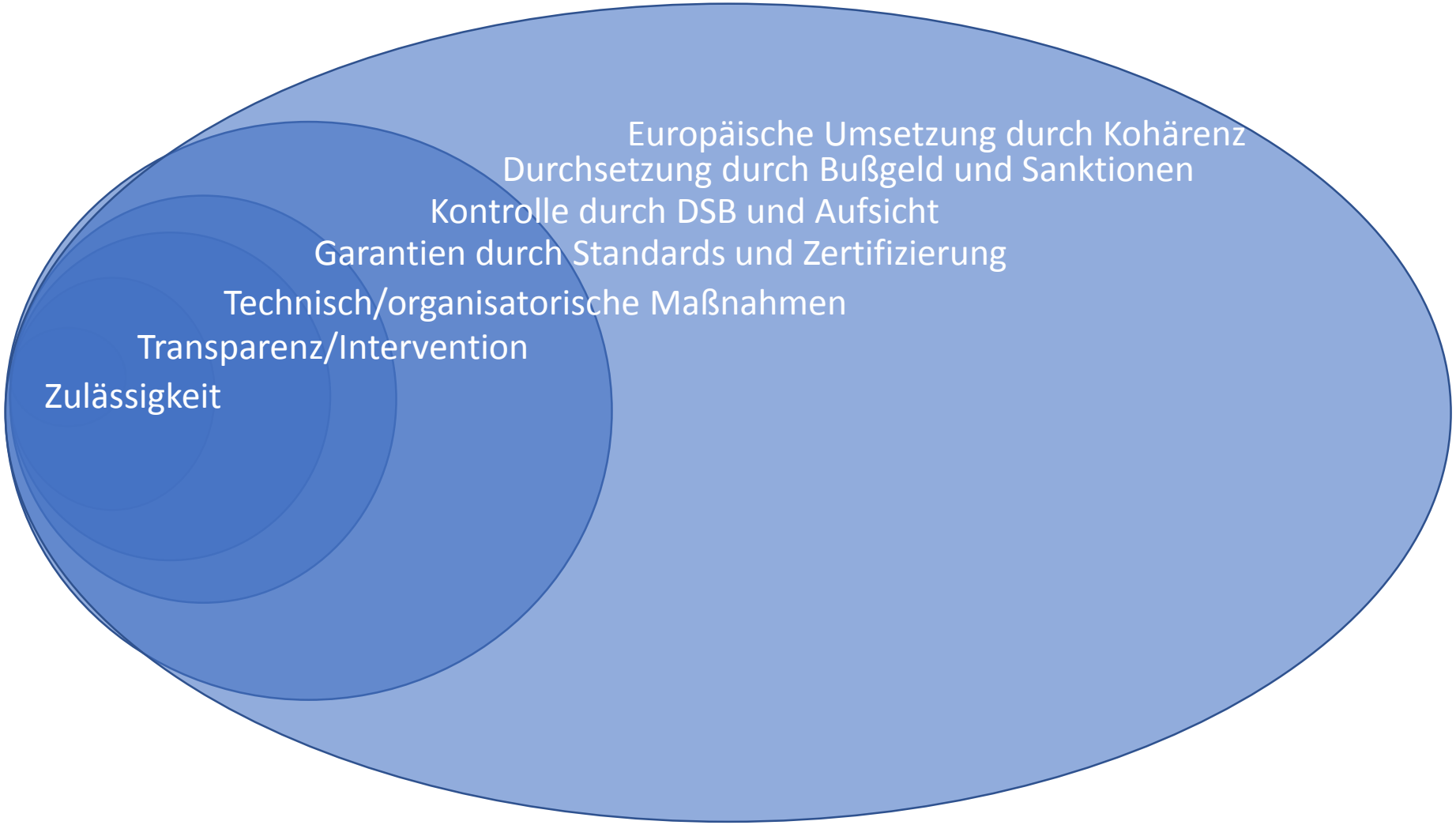
EU-weite *Stärkung* des Datenschutz

EU-weite *Kooperationen der Aufsichtsbehörden*

Verordnung - Rechtscharakter

- DS-GVO: allgemeine Regelung mit unmittelbarer Geltung (Verordnungen müssen nicht wie Richtlinien umgesetzt werden)
- Grundsatz: Vollharmonisierung im nicht-öffentlichen Bereich
- Ersetzt grds. nationales Datenschutzrecht, führt zur Unanwendbarkeit entgegenstehender nationaler Regelungen
- ABER: Öffnungsklauseln (Richtlinien-Charakter im öffentlichen Bereich)

DS-GVO: Übersicht



Grundprinzipien der DSGVO

Artikel 1
Gegenstand und Ziele

- Schutz der Grundrechte und Grundfreiheiten natürlicher Personen
- insbesondere deren Recht auf Schutz personenbezogener Daten und
- der freie Verkehr personenbezogener Daten

Artikel 5
Grundsätze für die Verarbeitung

- Rechtmäßigkeit
- Datensparsamkeit
- Zweckbindung
- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit

Artikel 2
Sachlicher Anwendungsbereich

- Ganz oder teilweise Automatisierte Verarbeitung personenbezogener Daten
- Nichtautomatisierte Verarbeitung von personenbezogener Daten

Artikel 6
Rechtmäßigkeit der Datenverarbeitung

Erfüllung mind. einer Bedingung:

- Einwilligung
- Erfüllung/Verarbeitung eines Vertrages
- Schutz lebenswichtiger Interessen

Grundprinzipien der DSGVO

Artikel 3
Räumlicher Anwendungsbereich
new

Artikel 51-62
Unabhängige Aufsichtsbehörden (One-Stop-Shop)
new

Artikel 12-21
Rechte der betroffenen Person
new

Artikel 63
Kohärenzverfahren
new

Artikel 83
Allgemeine Bedingungen für die Verhängung von Geldbußen
new

Grundprinzipien der DSGVO

Artikel 3
Räumlicher Anwendungsbereich
new

Artikel 12-21
Rechte der betroffenen Person
new

Artikel 83
Allgemeine Bedingungen für die Verhängung von Geldbußen
new

Grundprinzipien der DSGVO – Artikel 3

Räumlicher Anwendungsbereich – „Marktortprinzip“

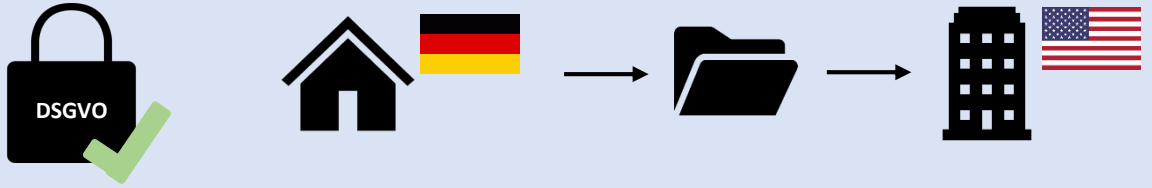
- Die DSGVO ist nicht nur für die in der Europäischen Union niedergelassenen Unternehmen relevant (sog. Marktortprinzip, Art. 3 Abs. 2).
- Voraussetzung ist, dass sich ein Angebot von (unentgeltlichen) Waren oder Dienstleistungen an einen **nationalen Markt in der EU** richtet (lit. a), oder eine Datenverarbeitung zur **Verhaltensbeobachtung** betroffener Personen in der EU erfolgt (lit. b).
- **Der Anwendungsbereich erstreckt sich also grds. auch auf außereuropäische Unternehmen, die auf dem europäischen Markt agieren, selbst wenn Sie keine eigenständige Niederlassung im Gebiet der europäischen Union unterhalten (z.B. auch Facebook oder Google).**
- Dadurch sollen **gleiche Wettbewerbsbedingungen** für alle Unternehmen geschaffen werden, nachdem das BDSG lediglich „im Inland“ erhobene Daten dem deutschen Datenschutzrecht unterwarf (§ 1 Abs. 5 Satz 2 BDSG) und insoweit Unklarheiten bezgl. dessen Anwendbarkeit entstanden sind.

Quelle: BfDI – Info 6

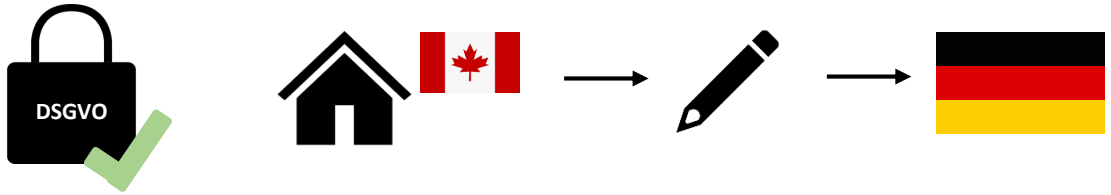
Grundprinzipien der DSGVO – Artikel 3

Räumlicher Anwendungsbereich – „Marktortprinzip“

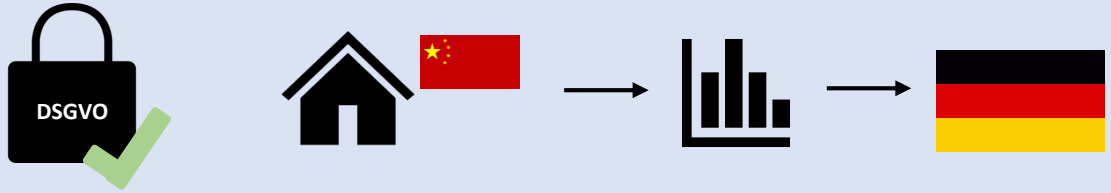
Kundendaten des deutschen Handelsunternehmens werden von Mutterkonzern in den USA gespeichert.



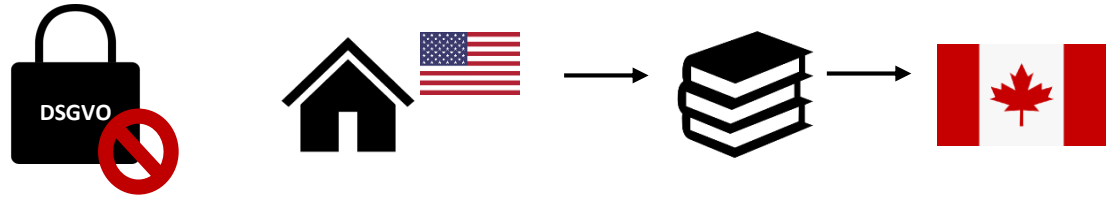
Kanadisches Handelsunternehmen verkauft über das Internet Stiftehalter in Deutschland.



Chinesisches Unternehmen beobachtet das Einkaufsverhalten von Personen aus Deutschland mithilfe eines Analysetools.



Amerikanisches Handelsunternehmen verkauft Bücher über das Internet in Kanada.



Artikel 4: Definitionen

1. “personenbezogene Daten” alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden “betroffene Person”) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;

Artikel 4: Definitionen

2. “Verarbeitung” jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

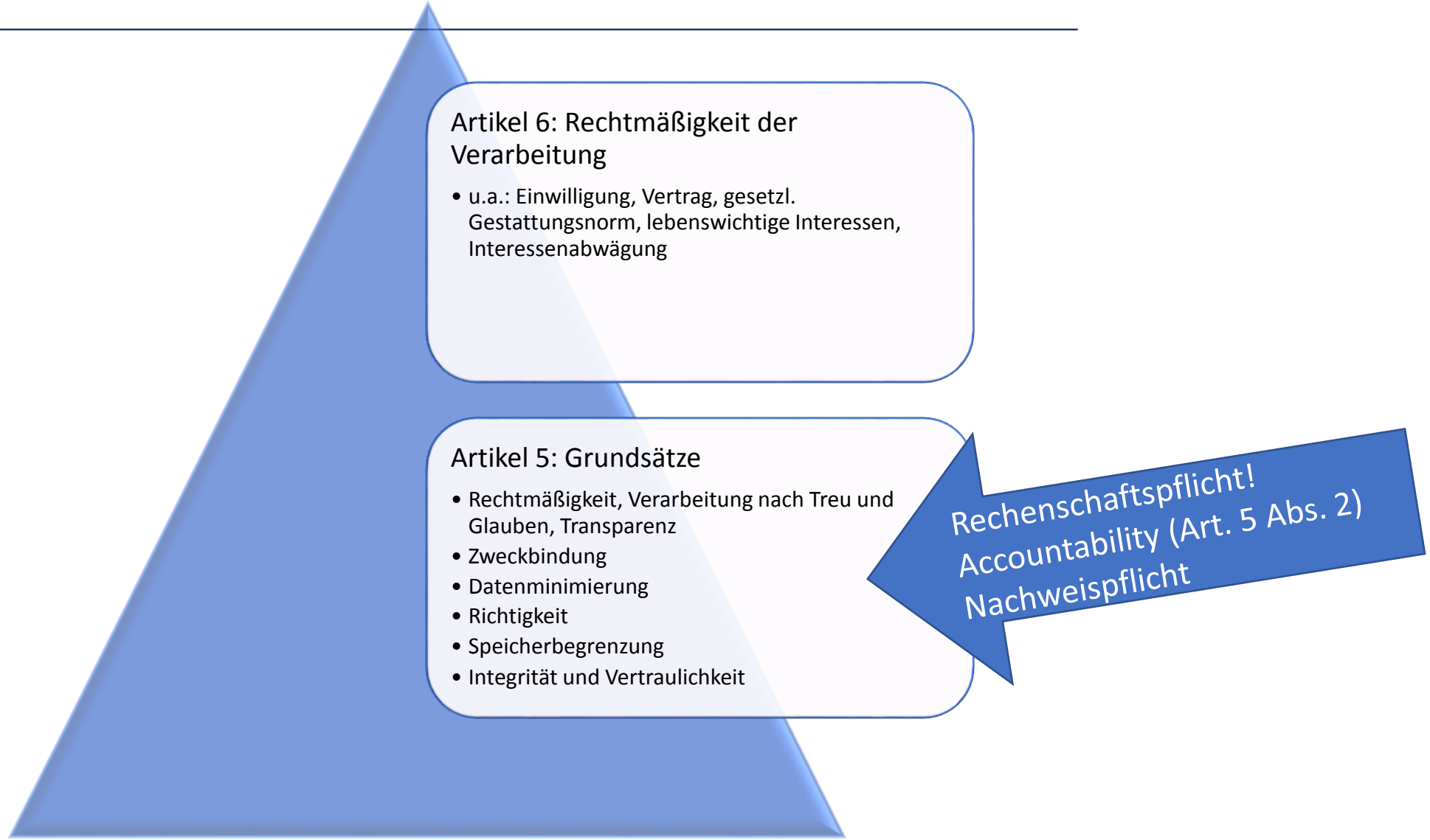
Artikel 4: Definitionen

5. “Pseudonymisierung” die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden;

Artikel 4: Definitionen

7. „Verantwortlicher“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden

Artikel 5 und 6 DS-GVO



Artikel 6: Rechtmäßigkeit der Verarbeitung

- u.a.: Einwilligung, Vertrag, gesetzl. Gestattungsnorm, lebenswichtige Interessen, Interessenabwägung

Artikel 5: Grundsätze

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit

Rechenschaftspflicht!
Accountability (Art. 5 Abs. 2)
Nachweispflicht

Artikel 5 und 6 Details

- Verarbeitung von Daten ist nur rechtmäßig, wenn eine **Einwilligung** oder eine andere in dieser Vorschrift normierte Ausnahme vorliegt (Art. 5 Abs. 1 lit. a i.V.m. Art. 6 Abs. 1), d.h. wenn
  - die Verarbeitung für die **Erfüllung eines Vertrags** erforderlich ist (Art. 6 Abs. 1 lit b), oder
  - die Verarbeitung zur Erfüllung einer **rechtlichen Verpflichtung** erforderlich ist (lit. c), oder
  - die Verarbeitung erforderlich ist, um **lebenswichtige Interessen** der betroffenen Person zu schützen (lit. d), oder
  - die Verarbeitung zur Erfüllung **hoheitlicher Aufgaben** erforderlich ist (lit. e), oder
  - zur Wahrung **berechtigter Interessen** des Verantwortlichen oder eines Dritten erforderlich ist (lit. f).
- Generell muss die Verarbeitung der personenbezogenen Daten **dem Zweck angemessen** sein (Art. 5 lit. b u. c).
- Auch **Prinzip der Datensparsamkeit** („Datenminimierung“) genannt, Art. 5 lit. c).

DS-GVO und ihre „Umsetzung“ im nationalen Recht

- Die DS-GVO gilt in den Mitgliedstaaten unmittelbar und braucht daher nicht in nationales Recht umgewandelt werden (sog. **Anwendungsvorrang, Art. 288 Abs. 2 AEUV**).
- Mitgliedstaaten können jedoch eigene, ergänzende Regelungen setzen (jedoch lediglich dort, wo durch DSGVO gesetzl. vorgesehen, sog. „**Öffnungsklauseln**“, s.o.).
- In der Bundesrepublik Deutschland erfolgte diese Rechtsetzung z.B. durch das Datenschutz-Anpassungs-Umsetzungs-Gesetz (**DSAnpUG-EU**), insbes. in Hinblick auf **Datenverarbeitung öffentlicher Stellen (Art. 86)** sowie im Beschäftigtenkontext (Art. 88).
- Die DS-GVO ersetzt nicht nur das Bundesdatenschutzgesetz (BDSG), sondern auch viele weitere Bundesgesetze, die Regelungen zum Datenschutz beinhaltet haben (z.B. SGB, TKG, TMG, etc.). Diese sind hiervon (inhaltlich oder auch formell) betroffen und werden von dieser überlagert (z.B. datenrechtliche Regelungen des § 11 ff. TMG; hierbei auch geplante **E-PrivacyVO** zu beachten).

DS-GVO und DSAnpUG zusammen lesen: Arbeitshilfe der GDD

www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_6.pdf

Prüfungsraster

- Gibt es eine datenschutzrechtliche Regelung in der DS-GVO?
- Lässt diese Regelung den Mitgliedstaaten einen Regelungsspielraum?
- Wurde der Regelungsspielraum in Deutschland genutzt?
- Wurden die Grenzen des mitgliedstaatlichen Spielraums beachtet?

Grundprinzipien der DSGVO

Artikel 3
Räumlicher Anwendungsbereich
new

Artikel 12-21
Rechte der betroffenen Person
new

Artikel 83
Allgemeine Bedingungen für die Verhängung von Geldbußen
new

Grundprinzipien der DSGVO – Artikel 12-21

Rechte der betroffenen Person - Übersicht

Information:
- Zweck & Rechtsgrundlage der Verarbeitung
- Name und Kontaktdaten des Verantwortlichen

Transparenz:
- Präzise, verständlich und leicht zugänglich
- Klare und einfache Sprache

Auskunft:
- Verarbeitungszweck
- (Geplante) Dauer der Verarbeitung
- Offenlegung gegenüber Dritten

Einschränkung:
- Unrechtmäßigkeit der Verarbeitung
- Bestritt der Richtigkeit

Datenübertragbarkeit: new
- Übermittlung der Daten

Widerspruch:
- Direktwerbung

Vervollständigung

Berichtigung

Löschung („Recht auf Vergessenwerden“): new
- Unrechtmäßigkeit der Verarbeitung
- Zweck der Erhebung nicht mehr notwendig

Rechte der betroffenen Person

Details

- Art. 12 DSGVO normiert die Anforderungen an die **Transparenz,** die Art der **Kommunikation** sowie die **Modalitäten** für die Ausübung der Rechte der betroffenen Person. Beispiele:
  - Betroffene müssen in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form über die Verarbeitung ihrer Daten informiert werden (Art. 12 Abs. 1 Satz 1).
  - Verantwortliche müssen betroffener Person die Ausübung ihrer Rechte erleichtern (Abs. 2).
- Art. 13 f. DSGVO sehen einen umfangreichen Katalog **proaktiver Benachrichtigungspflichten** vor, wobei danach differenziert wird, ob die Daten bei der betroffenen Person (Art. 13 DSGVO) oder bei Dritten (Art. 14 DSGVO) erhoben werden. Beispiele:
  - Zum Zeitpunkt der Erhebung muss die betroffene Person über Namen und Kontaktdaten des Verantwortlichen und den Zweck der Verarbeitung informiert werden (Art. 13 Abs. 1 lit. a, c).
  - Darüber hinaus über die Dauer der Speicherung (Abs. 2 lit. a), das Recht auf Auskunft/Berichtigung/Löschung/Einschränkung (lit. b) oder ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben ist (lit. e).

Rechte der betroffenen Person

Details

- Nach Art. 15 DSGVO hat die betroffene Person ein **Recht auf Auskunft,** ob und welche Daten, insbesondere zu welchem Zweck (Abs. 1 lit. a) die Daten erhoben werden.
- Nach Art. 16 DSGVO hat die betroffene Person ein **Recht auf Berichtigung** unrichtig erhoberner Daten.
- Nach Art. 17 DSGVO hat die betroffene Person unter bestimmten Voraussetzungen das Recht, die **Löschung** ihrer Daten (sog. „**Recht auf Vergessenwerden**“)zu verlangen.
  - Dabei besteht auch die Pflicht eines Datenverantwortlichen, der die Daten veröffentlicht hat, datenverarbeitende Dritteh über das Löschbegehren des Betroffenen zu informieren (Abs. 2).
- Art. 18 DSGVO normiert das **Recht auf Einschränkung der Verarbeitung**, z.B. wenn die Richtigkeit der Daten in Frage steht für die Dauer der Überprüfung (Abs. 1 lit.a).
- Das **Recht auf Datenübertragbarkeit** (Art. 20) gibt betroffenen Personen unter bestimmten Voraussetzungen einen Anspruch, eine Kopie der sie betreffenden personenbezogenen Daten in einem üblichen und maschinenlesbaren Dateiformat zu erhalten (z.B. um den Wechsel zu einem **anderen Anbieter** zu erleichtern).

Technischer und organisatorischer DS

Artikel 25
Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen
new

Artikel 35
Datenschutz-Folgenabschätzung
new

Artikel 40 und Artikel 42
Zertifizierung und Verhaltensregeln
new

Artikel 37
Benennung eines Datenschutzbeauftragten

Pflicht, wenn:
- Öffentliche Stelle
- Datenverarbeitung als Kerntätigkeit

Hauptaufgabe:
Überwachung der Einhaltung datenschutzrechtlicher Vorschriften

Technischer und organisatorischer DS

Artikel 25
Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen
new

Artikel 35
Datenschutz-Folgenabschätzung
new

Artikel 40 und Artikel 42
Zertifizierung und Verhaltensregeln
new

Artikel 37
Benennung eines Datenschutzbeauftragten

Pflicht, wenn:
- Öffentliche Stelle
- Datenverarbeitung als Kerntätigkeit

Hauptaufgabe:
Überwachung der Einhaltung datenschutzrechtlicher Vorschriften

Technischer und organisatorischer DS – Artikel 25 Abs. 1

Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

Privacy by Design: „Datenschutz durch Technikgestaltung“

Ergreifen technischer und organisatorischer **Maßnahmen** (TOMs) zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung (im **Entwicklungsstadium**), z.B.

- Pseudonymisierung
- Verschlüsselung
- Nutzerauthentifizierung

⬇

Unter Berücksichtigung:

Stand der Technik + Implementierungskosten	*Art, Umfang und Zwecke der Verarbeitung*	*Eintrittswahrscheinlichkeit und Schwere des Risikos*

Technischer und organisatorischer DS – Artikel 25 Abs. 2

Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

Privacy by Default: „Datenschutz durch datenschutzfreundliche Voreinstellungen“

Verarbeitung grundsätzlich nur personenbezogener Daten, deren Verarbeitung für den **jeweiligen bestimmten Verarbeitungszweck erforderlich** ist (= Werkeinstellungen datenschutzfreundlich ausgestalten)

Ziel: Nutzer schützen, die weniger technikaffin sind („Privacy Paradox“)

Was tun bei Unsicherheit mit Artikel 25?

Ein genehmigtes **Zertifizierungsverfahren** gemäß Artikel 42 DSGVO kann als Faktor herangezogen werden!

Technischer und organisatorischer DS

Artikel 25
Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen
new

Artikel 35
Datenschutz-Folgenabschätzung
new

Artikel 40 und Artikel 42
Zertifizierung und Verhaltensregeln
new

Artikel 37
Benennung eines Datenschutzbeauftragten

Pflicht, wenn:
- Öffentliche Stelle
- Datenverarbeitung als Kerntätigkeit

Hauptaufgabe:
Überwachung der Einhaltung datenschutzrechtlicher Vorschriften

Technischer und organisatorischer DS

Artikel 25
Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen
new

Artikel 35
Datenschutz-Folgenabschätzung
new

Artikel 40 und Artikel 42
Zertifizierung und Verhaltensregeln
new

Artikel 37
Benennung eines Datenschutzbeauftragten

Pflicht, wenn:
- Öffentliche Stelle
- Datenverarbeitung als Kerntätigkeit

Hauptaufgabe:
Überwachung der Einhaltung datenschutzrechtlicher Vorschriften

Technischer und organisatorischer DS – Artikel 40-42

Zertifizierung und Verhaltensregeln

Zertifizierung von Verarbeitungsvorgängen

Nachweis der Aufsichtsbehörde/einer akkreditierten Stelle, dass die DSGVO bei Verarbeitungsvorgängen eingehalten wird

Ziele:

- Vereinfachung der Kontrolle

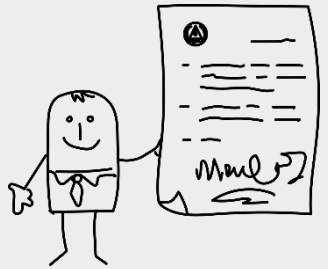
Informationen zur Zertifizierung via BayLFDI
https://www.lda.bayern.de/media/baylda_ds-gvo_2_certification.pdf

Verhaltensregeln: „Code of Conduct“

Verbindliche Vorgaben eines (Branchen-) Verbands oder einer anderen Vereinigung, die datenschutzrechtliche Verhaltensweisen der jeweiligen Mitglieder festlegen

Ziele:

- Präzisierung/Konkretisierung der Anforderungen der DSGVO
- Branchenspezifische Standards



Technischer und organisatorischer DS – Artikel 35

Datenschutz-Folgenabschätzung

Instrument des „Risikomanagements“:
Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch systematische Beschreibung der geplanten Verarbeitungsvorgänge

Notwendig, wenn:

- Verarbeitung besonders sensibler Daten
- Voraussichtlich hohes Risiko für Rechte und Freiheiten natürlicher Personen durch Verarbeitung (insb. bei Verwendung neuer Technologien)

Technischer und organisatorischer DS – Artikel 35

Datenschutz-Folgenabschätzung

Artikel 35 Abs. 1 DS-GVO
Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

Folgenabschätzung durchführen – wann genau?

Art. 29 Gruppe WP 248

- Nach der Leitlinie gilt es als je wahrscheinlicher, desto mehr der aufgelisteten Kriterien vorliegen. Als Faustregel soll gelten, dass eine Folgenabschätzung bei Erfüllung von zwei oder mehr Kriterien durchgeführt werden muss.
- Die Kriterien sind: (1) Scoring, Profiling, Evaluation, z. B. Einschätzung der Kreditwürdigkeit, Behavioral Marketing etc., (2) automatisierte Einzelfallentscheidungen, (3) systematische Überwachung, (4) Verarbeitung sensibler Daten, (5) umfangreiche Datenverarbeitungen (bezogen auf die Anzahl betroffener Personen und Datenkategorien, die Dauer der Verarbeitung, die geographische Ausdehnung), (6) das Zusammenführen oder Abgleichen von Datenbeständen, wenn Betroffene nicht damit rechnen können, (7) die Verarbeitung von Daten besonders schutzbedürftiger Personen, (8) Neuartigkeit von Verarbeitungsvorgängen, Verwendung neuer Technologien (bspw. Fingerabdrucksensoren oder Gesichtserkennung), (9) Verarbeitungen, die es betroffenen Personen erschweren, ihre Rechte auszuüben oder eine Leistung in Anspruch zu nehmen, z.B. die Beurteilung der Kreditwürdigkeit durch eine Bank vor der Vergabe eines Darlehens

Grundprinzipien der DSGVO

Artikel 3
Räumlicher Anwendungsbereich
new

Artikel 12-21
Rechte der betroffenen Person
new

Artikel 83
Allgemeine Bedingungen für die Verhängung von Geldbußen
new

Grundprinzipien der DSGVO – Artikel 83

Allgemeine Bedingungen für die Verhängung von Geldbußen

Geldbußen nach Art. 83 Abs. 4 DSGVO

- *Art. 33 DSGVO: Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde*
- *Art. 35 DSGVO: Datenschutz-Folgenabschätzung*

Geldbußen von bis zu **10 000 000 EUR** oder bis zu **2 %** des gesamten **weltweit erzielten Jahresumsatzes** (höherer Betrag)

Geldbußen nach Art. 83 Abs. 5 DSGVO

- *Art. 6 DSGVO: Rechtmäßigkeit der Verarbeitung*
- *Art. 12-21 DSGVO: Rechte der Betroffenen*

Geldbußen von bis zu **20 000 000 EUR** oder bis zu **4 %** des gesamten **weltweit erzielten Jahresumsatzes** (höherer Betrag)

Grundprinzipien der DSGVO – Artikel 83

Allgemeine Bedingungen für die Verhängung von Geldbußen

- Gegen **Behörden und sonstige öffentliche Stellen** des Bundes können auch in Zukunft keine Geldbußen verhängt werden (vgl. Art. 83 Abs. 7 i.V.m. bislang fehlender nationaler Regelung).
- Bußgeld zukünftig auch gegen Hochschulen?
- Auf jeden Fall Befugnisse nach Art. 58 DSGVO:
- Verwarnung (lit. a und b),
- Anweisungs- und Anordnungsbefugnisse (lit. c, d, e, g und h) und die Sanktionsbefugnisse (lit. f, h, i und j)

Aus Verfahrensverzeichnis wird Verarbeitungsverzeichnis

Praxisrelevant: das Verfahrensverzeichnis des BDSG wird abgelöst durch das „Verzeichnis von Verarbeitungstätigkeiten“ (Art. 30 EU-DSGVO).

Muster BayLDA
https://www.projekt29.de/datenschutzblog29/muster-fuer-verzeichnis-der-verarbeitungstaetigkeiten-nach-art-30-dsgvo

Teil II: Artikel 25 DSGVO

Privacy by Design und Privacy by Default – was bedeutet das in der Praxis?

Privacy by Design

Artikel 25 Absatz 1 DS-GVO

Artikel 25 Absatz 1 DS-GVO: PbD

Normtext

Art. 25 DSGVO Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen – wie z. B. Pseudonymisierung – trifft, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

Artikel 25 Absatz 1 DS-GVO: PbD

Normtext

Art. 7
Achtung des Privat- und Familienlebens

Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation.

Art. 8
Schutz personenbezogener Daten

(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
(2) 1 Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. 2Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.
(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

PbD Basics

- Idee: Technik im Dienst der Rechtsdurchsetzung (Code is law, Lessig, Cavoukian Mitte der 90‘er: PETS)
- Cavoukian „739“ (7 Grundprinzipien, 3 Verantwortungsbereiche, 9 Anwendungsfelder)
  - 7 Grundprinzipien: 1. Proactive not Reactive; Preventative not Remedial; 2. Privacy as the Default Setting; 3. Privacy Embedded into Design; 4. Full Functionality – Positive-Sum, not Zero-Sum; 5. End-to-End Security – Full Lifecycle Protection; 6. Visibility and Transparency – Keep it Open; 7. Respect for the User – Keep it User-Centric.

  - 3 Verantwortungsbereiche: 1) IT systems; 2) accountable business practices; and 3) physical design and networked infrastructure.

  - 9 Anwendungsfelder: 1.CCTV/Surveillance Cameras in Mass Transit Systems; 2.Biometrics Used in Casinos and Gaming Facilities; 3.Smart Meters and the Smart Grid; 4.Mobile Devices & Communications; 5.Near Field Communications (NFC); 6.RFIDs and Sensor Technologies; 7.Redesigning IP Geolocation Data; 8.Remote Home Health Care; 9.Big Data and Data Analytics.

PbD Basics

- Bei Artikel 25 geht es nicht nur darum, Datenvermeidung und Datenminimierung proaktiv und technisch-organisatorische Steuerungsmechanismen zu adressieren.
- Es geht auch um Nachhaltigkeit in der Datenwirtschaft, um vertrauensbildende Maßnahmen in einem hochtechnisierten, vernetzten Umfeld.

- (Auch, bzw. vor allem?): öffentliche Stellen haben Vorbildfunktion!

- Beispiel: Landesdatenschutzbeauftragte BaWü führt auf Grundage vorab kommunizierter Richtlinie Folgenabschätzung (Art. 35 DS-GVO) durch, bevor die Institution „twittert“

- https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2017/11/2017.11.02._Richtlinie-zur-Nutzung-sozialer-Netzwerke-durch-öff.-Stellen.pdf#

- https://www.baden-wuerttemberg.datenschutz.de/twitter-datenschutzfolgenabschaetzung/

PbD Details

Die einzelnen Tatbestandsmerkmale des Art. 25 Abs. 1 DS-GVO

- Adressat: Verantwortliche (Art. 4 Nr. 7 DS-GVO) NICHT Hersteller (letztgenannte werden nur „ermutigt“ in ErwG 78)
- Maßgeblicher Zeitpunkt: sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung – letztlich: das „gesamte Lebenszyklusmanagement personenbezogener Daten“.
- TOM
  - Unter technischen Maßnahmen werden im Allgemeinen Vorkehrungen verstanden, die sich entweder physisch auf den Vorgang der Verarbeitung von Daten erstrecken, oder solche, die den Software- oder Hardwareprozess der Verarbeitung (logisch) steuern. Organisatorische Maßnahmen richten sich auf die äußeren Rahmenbedingungen zur Gestaltung des technischen Verarbeitungsprozesses.
- Pseudonymisierung (allein reicht nicht!)
  - PRAXISHINWEIS: Die Fokusgruppe Datenschutz der Plattform Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft hat im Rahmen des Digital-Gipfels 2017 ein Whitepaper mit Leitlinien für die rechtssichere Nutzung von Pseudonymisierungslösungen unter Berücksichtigung der Vorgaben der DS-GVO veröffentlicht. Dort werden die Rahmenbedingungen der Pseudonymisierung, Verfahren und technisch-organisatorische Anforderungen in verschiedenen Anwendungszenarien eingehend erörtert.

PbD Details

Maßnahmen neben der Pseudonymisierung

„ErwG 78er“ Maßnahmen

Der Verantwortliche soll „interne Strategien“ festlegen und Maßnahmen ergreifen, die „unter anderem darin bestehen können, dass die Verarbeitung personenbezogener Daten minimiert wird, personenbezogene Daten so schnell wie möglich pseudonymisiert werden, Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten hergestellt wird, der betroffenen Person ermöglicht wird, die Verarbeitung personenbezogener Daten zu überwachen, und der Verantwortliche in die Lage versetzt wird, Sicherheitsfunktionen zu schaffen und zu verbessern.“

Daraus folgt: Grundsätze der Transparenz, der Intervenierbarkeit, Löschkonzept, Tagging (Sicherung zweckentsprechender Datenverarbeitung) implementieren

PbD Details

Stand der Technik

„Stand der Technik“

Der Stand der Technik bezeichnet das obere Ende des technisch möglichen, aber praktisch Bewährten zu einem bestimmten Zeitpunkt.

Weil es sich um ein dynamisches Konzept handelt, folgt aus dem Gesagten für die Praxis, dass die Beachtung (noch praktizierter) nationaler oder internationaler Normen (Bspw. ISO 27001) allein noch nicht ausreicht!

PbD Deteils

Kosten

„Implementierungskosten“

Einigkeit besteht in der Kommentarliteratur weitgehend dahingehend, dass Implementierungskosten dem insoweit klaren Wortlaut folgend **nur initial entstehende, nicht aber auch laufende Betriebs- und Folgekosten** erfassen können.

PbD Details

„Risikoanalyse“ wie geht das?

1. Lies: Erwägungsgrund 75, 76

2. Solange (auch) für die Risikoanalyse im Sinne des Art. 25 Absatz 1 zertifizierte Verfahren und Leitlinien des Europäischen Datenschutzausschusses im Sinne des Art. 70 Abs. 1 lit. d fehlen, wird man sich an Methodik und den Modellen der ENISA, des BSI und des im Auftrag der Datenschutzkonferenz entwickelten Standard-Datenschutzmodells (SDM) orientieren können.
Hilfreich sind ferner das in der Literatur entwickelte LINDDUN-Modell sowie Papiere der französischen Aufsichtsbehörde für Informatik und Freiheiten (CNIL), der Aufsichtsbehörde des Vereinigten Königreichs ICO, sowie der spanischen AGPD, die zum Teil mehrteilige Dossiers mit „Good Practices“ erarbeitet haben.

3. Eine Risikoanalyse ist auch Bestandteil der im Rahmen der Mindestanforderungen einer Datenschutzfolgenabschätzung zu dokumentierenden Aspekte (Artikel 35 Absatz 7 lit. c). Daher können die im Rahmen des Artikels 35 entwickelten Ansätze fruchtbar gemacht werden. Sachgerecht erscheint vor diesem Hintergrund, als die Schwere des Risikos potentiell mitbestimmenden Faktor den Umstand zu bewerten, dass neue Technologien bzw. Verarbeitungsmethoden zum Einsatz gelangen, was ausweislich der Wertung in ErwG 89 ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen bedingen kann.

PbD Details

Mit Blick auf das Abwägungsergebnis der Verhältnismäßigkeitsprüfung (Angemessenheit) und die Auswahl der konkreten Maßnahme (Entscheidungs- und Gestaltungsspielraum) wird dem Verantwortlichen in Artikel 25 Absatz 1 DSGVO ein erheblicher Spielraum zugestanden. Insoweit lassen sich die für TOM i.S.d. § 9 BDSG angestellten Überlegungen übertragen, wonach nicht „mit Kanonen auf Spatzen geschossen werden muss“.

Andererseits handelt es sich nicht um einen freien, d.h. aufsichts- , bzw. gerichtsfesten Beurteilungsspielraum, sondern konzeptionell um eine Ermessensentscheidung.

Privacy by Default

Artikel 25 Absatz DS-GVO

Privacy by Default - Hintergrund

- Mit der Regelung wird erstens dem Umstand Rechnung getragen, dass es (auch unter dem Aspekt der Datensicherheit) einen Unterschied macht, ob Daten nur nicht verwendet oder gar nicht erst erhoben werden.

- Zweitens haben Studien gezeigt, dass Nutzer vom System vorgegebene Einstellungen üblicherweise beibehalten (sog. "status quo bias"), was gerade im Rahmen der Profileinstellungen bei Sozialen Netzwerken, auf die die Vorschrift in erster Linie zugeschnitten ist, eine wichtige Rolle spielt.

Privacy by Default - Details

- Adressat der Regelung ist (wie auch bei Abs. 1) der für die Verarbeitung personenbezogener Daten Verantwortliche und nicht der Hersteller.

- Nach Artikel 25 Absatz 2 Satz 1 hat der Verantwortliche geeignete TOM zu ergreifen um sicherzustellen, dass durch Voreinstellungen grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.

- Ausgangspunkt ist demnach der datenschutzrechtliche Zweckbindungs- und Erforderlichkeitsgrundsatz (Art. 5 Abs. 1 lit b) und c). Nur diejenigen Datenarten, die für die jeweils konkret festgelegten Verarbeitungszwecke (Art. 30 Abs. 1 lit. b) erforderlich sind, sollen erhoben werden.

Privacy by Default - Details

- Artikel 25 Absatz 2 Satz 2 konkretisiert weiter dahingehend, dass sich die Erforderlichkeit auf die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit bezieht.
  - Umfang: (in Abgrenzung zur Menge) die Tiefe der Verarbeitung, beispielsweise durch Erstellung von Persönlichkeitsprofilen. Da der Verantwortliche den Verarbeitungszweck festlegt, entscheidet er zugleich über den Umfang der dafür erforderlichen Daten.
  - Die Speicherfrist für personenbezogene Daten muss nach Erwägungsgrund 39 auf das unbedingt erforderliche Mindestmaß beschränkt bleiben. Im Zuge dessen hat der Verantwortliche Fristen für ihre Löschung vorzusehen (Löschkonzept).
- BEISPIEL: Unzulässig nach Art. 25 Absatz 2 Satz 1 und 2 wäre die ohne gesonderte Einwilligung des Betroffenen erfolgende Weitergabe der bei ihm gespeicherten Adressdaten im Rahmen des Anmeldeverfahrens für ein soziales Netzwerk ebenso, wie eine diesbezügliche Einwilligung nicht durch ein standardmäßig angekreuztes Kästchen erklärt werden kann.

Privacy by Design: bad, better, best Practice

„Smartes“ Spielzeug

Caya, Hello Barbie, VaiKai