EU-Datenschutz-Grundverordnung

EU-Datenschutzgrundverordnung

daten schutz

Überblick

1) Rechtsgrundlagen…1
2) Anwendungsbereich…2
3) Begriffsbestimmungen…3
4) Verarbeitungsgrundsätze…4
5) Rechtsgrundlagen für die Datenverarbeitung…6
6) Einwilligung…9
7) Verarbeitung besonderer Kategorien personenbezogener Daten…11
8) Auftragsverarbeitung…14
9) Betroffenenrechte allgemein…15
10) Informationspflichten…17
11) Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung etc.…18
12) Widerspruchsrecht…20
13) Automatisierte Einzelentscheidung…22
14) Technisch-organisatorische Maßnahmen, Privacy by Design, Privacy by Default…23
15) Dokumentation…24
16) Meldung von Datenschutzverstößen…25
17) Datenschutzfolgenabschätzung…26
18) Betriebliche/Behördliche Datenschutzbeauftragte…27
19) Verhaltensregelungen und Zertifizierung…29
20) Internationaler Datenverkehr…30
21) Aufsichtsbehörde…32
22) Zusammenarbeit und Kohärenzverfahren…33
23) Europäischer Datenschutzausschuss…34
24) Rechtsbehelfe und Sanktionen…35
25) Besondere Datenverarbeitungssituationen…37

Rechtsgrundlagen

„Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.16 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der RL 95/46/EG (DSGVO)“

Geltung ab 25.05.18
Unmittelbar geltendes Recht in allen Mitgliedstaaten → Harmonisierung des Datenschutzrechts in der EU
Aber: Öffnungsklauseln und Regelungsaufträge für den nationalen Gesetzgeber
Öffnungsklauseln, z.B.:

- Datenverarbeitung durch öffentliche Stellen (Art. 6 Abs. 2, 3) → NDSG
- Pflicht zur Bestellung eines betr. Datenschutzbeauftragten (Art. 37 Abs. 4) → „BDSG neu“
- Datenverarbeitung im Beschäftigungskontext (Art. 88) → „BDSG neu“
- Ausnahmen zu den Betroffenenrechten (Art. 23) → „BDSG neu“

Regelungsaufträge, z.B.:

- Errichtung der Aufsichtsbehörden (Art. 51 ff.) → „BDSG neu“
- Rechtsschutz (Art. 83) → „BDSG neu“

→ neben GVO: neues Bundesdatenschutzgesetz und bereichsspezifische Datenschutzgesetze
→ Anpassung der bestehenden Datenschutzgesetze an die GVO

Anwendungsbereich

Persönlicher Schutzbereich – Art. 1 (1), (2)

- natürliche Personen
- unabhängig von Staatsangehörigkeit und Aufenthalt

Sachlicher Schutzbereich – Art. 1 (2)

- pb Daten (Art. 4 Nr. 1)
- ganz od teilweise automatisierte Verarbeitung (Art. 4 Nr. 2)
- nicht-automatisierte Verarbeitung, soweit in Dateisystem (Art. 4 Nr. 6) gespeichert
- Ausnahmen: Abs. 2 (Bsp: lit. c ->„ausschließlich persönliche oder familiäre Tätigkeit“)

Räumlich – Art. 3

Niederlassungsprinzip, Abs. 1

- Niederlassung (Erw. 22) ≠ Hauptniederlassung (Art. 4 Nr. 16)
  Sitz: stets als Niederlassung zu qualifizieren (EuGH)

Marktortprinzip, Abs. 2

- wenn sich Verarbeitung außereuropäischer Unternehmen gezielt auf Personen in EU bezieht
- Fälle: lit. a – Waren/Dienstleistungen; lit. b – Verhaltensbeobachtung

Begriffsbestimmungen

Art. 4

Legaldefinition der wichtigsten Datenschutzbegriffe

Keine wesentlichen inhaltlichen Änderungen gegenüber der EU-Datenschutzrichtlinie

Neue Definitionen wie „Profiling“, „genetische Daten“, „biometrische Daten“, „Gesundheitsdaten“, „Unternehmen“, „verbindliche unternehmensinterne Datenschutzvorschriften“

Zentrale Definitionen:

- „Personenbezogene Daten“
- „Verarbeitung“ (neu: weiter Begriff, umfasst jeden Vorgang im Zusammenhang mit pb Daten)
- „Verantwortlicher“
- „Dritter“
- „Einwilligung“
- „Verletzung des Schutzes personenbezogener Daten“

Verarbeitungsgrundsätze I

Art. 5 Abs. 2 – Verantwortlicher hat ***Rechenschaftspflicht*** bzgl. in Abs. 1 genannter Grundsätze

Art. 5 Abs. 1

a) Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz (transparent = in nachvollziehbarer Weise)

b) Zweckbindung:

- für festgelegte, eindeutige und legitime Zwecke erhoben
- nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet (Weiterverarbeitung für im öffentl. Interesse liegende Archivzwecke, für wiss. od. hist. Forschungszwecke od. für statistische Zwecke gilt nicht als unvereinbar mit den ursprünglichen Zwecken; Art. 89 Abs. 1)

c) Datenminimierung:

- dem Zweck angemessen und erheblich
- auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt

Verarbeitungsgrundsätze II

d) Richtigkeit:

- sachlich richtig; erforderlichenfalls auf dem neuesten Stand
- bei Unrichtigkeit im Hinblick auf Zwecke sind alle angemessenen Maßnahmen zur unverzüglichen Löschung bzw. Berichtigung zu treffen

e) Speicherbegrenzung:

- Speicherung in Form, die Identifizierung nur so lange ermöglicht, wie für Verarbeitungszwecke erforderlich
- länger, soweit Verarbeitung ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gem. Art. 89 (1) verarbeitet werden (vorbehaltlich Durchführung geeigneter toM, wie sie von DS-GVO gefordert werden)

f) Integrität und Vertraulichkeit:

- Gewährleistung angemessener Sicherheit der personenbezogenen Daten
- inkl. Schutz vor unbefugter od. unrechtmäßiger Verarbeitung, unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung od. unbeabsichtigter Schädigung (> geeignete toM)

Art. 6

Grundsatz: Verbot mit Erlaubnisvorbehalt

Rechtsgrundlagen für Datenverarbeitung aus der GVO:

- Einwilligung (Art. 6 Abs. 1 a, s. auch Art. 7, Definition in Art. 4 Nr. 11
- Erfüllung eines Vertrages oder Durchführung einer vorvertraglichen Maßnahme (Art. 6 Abs. 1 b)
- Erfüllung einer rechtlichen Verpflichtung (Art. 6 Abs. 1 c)
- Schutz lebenswichtiger Interessen (Art. 6 Abs. 1 d)
- Erfüllung öffentlicher Aufgaben (Art. 6 Abs. 1 e)
- Wahrung berechtigter Interessen (Art. 6 Abs.1 f)

Öffnungsklausel (Art. 6 Abs. 2, 3): Für Datenverarbeitung durch öffentliche Stellen speziellere Rechtsgrundlagen nach nationalem Recht möglich → NDSG, SGB etc.

Art. 6

Insbesondere: Wahrung berechtigter Interessen (Art. 6 Abs. 1 f)

„Die Verarbeitung ist rechtmäßig, wenn die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt."

→ Interessenabwägung

→ berechtigtes Interesse des Verantwortlichen oder eines Dritten: z.B. Direktwerbung (EG 47), Übermittlung innerhalb verbundener Unternehmen (EG 48)

→ Rechtsgrundlage für Videoüberwachung Privater, für Werbung, für Adresshandel

→ gilt nicht für Behörden, Art. 6 Abs. 1 S. 2

Art. 6

Weiterverarbeitung zu Sekundärzwecken, Art. 6 Abs. 4:

Einmal rechtmäßig erhobene Daten dürfen unabhängig von der ursprünglichen Rechtsgrundlage zu einem anderen Zweck weiter verarbeitet werden, sofern die Weiterverarbeitung zu einem Zweck erfolgt, der mit dem ursprünglichen Erhebungszweck vereinbar ist. Kriterien der Prüfung der Vereinbarkeit der Zwecke (soweit nicht Einwilligung bzw. Rechtsvorschrift nach Art. 23 einschlägig): z.B. Verbindung zwischen den Zwecken, Zusammenhang der Erhebung, Art der Daten (s. Art. 6 Abs. 4 a) bis e).

→ keine gesonderte Rechtsgrundlage erforderlich (vgl. auch EG 50)

→ Aufweichung des Zweckbindungsgrundsatzes

→ Öffnungsklausel für nationalen Gesetzgeber (s. „BDSG neu“)

Einwilligung I

Definition: Art. 4 Nr. 11: „jede **freiwillig** für den **bestimmten Fall**, in **informierter Weise** und **unmissverständlich abgegebene** Willensbekundung in Form einer **Erklärung** oder einer **sonstigen eindeutigen bestätigenden Handlung**, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist“

- Freiwillig: echte Wahl muss gegeben sein (nicht nur „ohne Drohung“); nicht der Fall z.B. bei Überrumpelung, Koppelung etc.
- Bestimmter Fall: nicht pauschal; es muss erkennbar welche Daten zu welchem Zweck und durch wen verarbeitet werden
- Informiert: Kenntnisnahme des Inhalts ist zumutbar möglich, d.h. die Erklärung ist verständlich (inhaltlich, sprachlich) und hervorgehoben
- Erklärung oder sonstige Handlung:

➢ in jeder Form möglich; auch elektronisch (Erw. 32 – mit weiteren Anforderungen)

➢ konkludent, durch schlüssiges Handeln; z.B. aktiver Mausklick in Kästchen (≠ „Dulden“ bei opt-out) – gilt nicht bei besonderen personenbezogenen Daten!! (Art. 9)

Einwilligung II

Allgemeine Anforderungen an Einholung und Ausgestaltung

Art. 7 – vier Absätze, vier Punkte

(1) Nachweisbarkeit
(2) Klare Sprache
(3) Widerrufbarkeit
(4) Freiwilligkeit

Art. 8 – Spezialregelung für speziell an Unter-16-Jährige gerichtete „Dienste der Informationsgesellschaft" (*in etwa: Telekommunikation und Telemedien)*

(1) Durch Erziehungsberechtigte oder mit deren Einverständnis
(2) Vergewisserung („angemessene Anstrengungen")

Verarbeitung besonderer Kategorien personenbezogener Daten I

Art. 9, 10

Besondere Kategorien pb Daten:

- Rassische Herkunft
- Ethnische Herkunft
- Politische Meinungen
- Religiöse oder weltanschauliche Überzeugungen
- Gewerkschaftszugehörigkeit
- Genetische Daten (Def. in Art. 4 Nr. 14)
- Biometrische Daten (Def. in Art. 4 Nr. 15)
- Gesundheitsdaten (Def. in Art. 4 Nr. 16)
- Daten zum Sexualleben oder zur sexuellen Orientierung

Grundsatz: Verarbeitung dieser Daten verboten, Art. 9 Abs. 1

Verarbeitung besonderer Kategorien personenbezogener Daten II

Art. 9, 10

Ausnahmen, Art. 9 Abs. 2:

- Ausdrückliche Einwilligung der betroffenen Person, Art. 9 Abs. 2 a
- Wahrnehmung von arbeits- und sozialrechtlichen Rechten und Pflichten des Verantwortlichen, Art. 9 Abs. 2 b (z.B. im Arbeitsverhältnis erforderliche Verarbeitung von Gesundheitsdaten wie Beschäftigungsverbot, nur mit rechtlicher Grundlage und „geeigneten Garantien“)
- Schutz lebenswichtiger Interessen, Art. 9 Abs. 2 c (wenn betroffene Person selbst nicht einwilligen kann)
- Zweckgebundene interne Verarbeitung durch bestimmte politisch, religiös, weltanschaulich oder gewerkschaftlich ausgerichtete Organisationen, Art. 9 Abs. 2 d
- Von der betroffenen Person offensichtlich veröffentlichte Daten, Art. 9 Abs. 2 e
- Verfolgung rechtlicher Ansprüche, Art. 9 Abs. 2 f
- Erhebliches öffentliches Interesse, Art. 9 Abs. 2 g (auf rechtlicher Grundlage, verhältnismäßige Anwendung)
- Maßnahmen für die individuelle Gesundheit, Art. 9 Abs. 2 h (medizinische Behandlungen, unter Voraussetzungen des Art. 9 Abs. 3, insbesondere Verpflichtung zur Geheimhaltung)
- Öffentliches Gesundheitswesen, Art. 9 Abs. 2 i (öffentliches Interesse im Zusammenhang mit Gefahrenabwehr im Gesundheitsbereich und zur Qualitätssicherung bei der Gesundheitsversorgung)
- Archivzwecke, Forschung, Statistik, Art. 9 Abs. 2 j (auf rechtlicher Grundlage und mit angemessenen Schutzmaßnahmen)

Allgemeine Öffnungsklausel für eigene nationale Regelungen bezüglich genetischen, biometrischen und Gesundheitsdaten, Art. 9 Abs. 4 (s. „BDSG neu“)

Verarbeitung besonderer Kategorien personenbezogener Daten III

Art. 10

Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten, Art. 10:

- Verarbeitung nur zulässig unter behördlicher Aufsicht
- Verarbeitung nur zulässig auf rechtlicher Grundlage mit „ geeigneten Garantien“
- Gilt nur für die Person des Täters (nicht Zeugen, Opfer)

Auftragsverarbeitung

Definition: Art. 4 Nr. 8: eine natürliche oder juristische Person, Behörde, Einrichtung od. andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet

Art. 28 (1): **Anforderungen** an **toM** beim Auftragsverarbeiter (AV)

- Müssen Garantien bieten, dass Verarbeitung in Einklang mit DSGVO und Betroffenenrechte gewährleistet

Art. 28 (2): keine „**weiteren AV**" ohne schriftliche Genehmigung des Verantwortlichen

Art. 28 (4): **weitere AV** treffen die **gleichen datenschutzrechtlichen Pflichten** wie den AV; Haftung des AV für weitere AV gegenüber dem Verantwortlichen

Art. 28 (3): AV muss auf Grundlage eines Vertrages oder anderen Rechtsinstruments der EU oder eines Mitgliedstaates erfolgen

- Inhalt: Gegenstand und Dauer; Art und Zweck; Art der Daten; Kategorien der betroffenen Personen; Pflichten und Rechte des Verantwortlichen; sowie ein nicht abschließender Katalog konkreter Inhalte
- Form: schriftlich oder elektronisch (Abs. 9)

Art. 82: verschärfte **Haftung** für Verantwortliche

- verschuldensunabhängig mit Exkulpationsmöglichkeit (1,3)
- AV haftet nur selbst wenn nach DSGVO auferlegten Pflichten nicht nachgekommen oder Nichtbeachtung von/Handeln entgegen rechtmäßig erteilter Anweisungen (2)

Betroffenenrechte – Modalitäten (Art. 12)

1) Transparenz, Art. 12 Abs. 1

Verpflichtung des Verantwortlichen, geeignete Maßnahmen zu ergreifen, um Informationen und Mitteilungen im Zusammenhang mit der Ausübung der Betroffenenrechte übermitteln zu können.

2) Form der Informationen und Mitteilungen, Art. 12 Abs. 1

- Präzise, transparente, verständliche und leicht zugängliche Form
- In klarer und einfacher Sprache, insbes. bei Kindern
- Schriftlich, elektronisch oder mündlich, wenn Identität nachgewiesen

3) Verweigerungsrecht des Verantwortlichen, Art. 12 Abs. 2 S. 2

- Wenn betroffene Person nicht mehr identifiziert werden kann, es sei denn, betroffene Person bringt zusätzliche Informationen zur Identifizierung bei

4) Unterrichtung über ergriffene Maßnahmen, Art. 12 Abs. 2, 3

- Grundsätzlich unverzüglich, spätestens innerhalb eines Monats, Fristverlängerung möglich
- Auch Unterrichtung über Untätigkeit, innerhalb eines Monats, mit Begründung und Hinweis auf Beschwerderecht

5) Unentgeltlichkeit, Art. 12 Abs. 5

- Aber bei exzessiven oder offenkundig unbegründeten Anträgen angemessenes Entgelt oder Verweigerung des Tätigwerdens (Verweigerungsrecht neu)

Betroffenenrechte – Beschränkungen (Art. 23)

Öffnungsklausel für nationales Recht:

- Beschränkungen der Betroffenenrechte zulässig für bestimmte wichtige Rechtsgüter wie nationale Sicherheit, öffentliche Sicherheit, Verhütung oder Aufdeckung von Straftaten sonstige wichtige Ziele des allgemeinen öffentlichen Interesses etwa im Haushalts- und Steuerbereich oder im Bereich der öffentlichen Gesundheit (Art. 23 Abs. 1)
- Nur erlaubt, wenn notwendig und verhältnismäßig
- Mindestinhalt beschränkender Gesetze vorgegeben, z.B. Garantien gegen Missbrauch und Speicherfristen (Art. 23 Abs. 2)
- → s. „BDSG neu“

Informationspflichten

Art. 13, 14

1) Informationspflicht bei Erhebung der Daten bei der betroffenen Person, Art. 13
2) Informationspflicht, wenn die Daten nicht bei der betroffenen Person erhoben wurden, Art. 14

- ✓ Informationen z.B.: Name und Kontaktdaten des Verantwortlichen, Kontaktdaten des Datenschutzbeauftragten, Zweck und Rechtsgrundlage der Verarbeitung, Empfänger, Dauer der Speicherung, Betroffenenrechte
- ✓ Informationen in präziser, verständlicher Sprache
- ✓ Ausschluss der Informationspflicht z.B. wenn Informationen der betroffenen Person schon bekannt sind oder bei unverhältnismäßigem Aufwand, insbesondere bei Datenverarbeitung zu Forschungszwecken
- ✓ Bußgeldbewehrt nach Art. 83 Abs. 5 b)
- ✓ Öffnungsklausel für nationalen Gesetzgeber für weitere Beschränkungen (Art. 23, s. „BDSG neu“) und für Ausnahmen für Datenverarbeitung zu journalistischen sowie zu wissenschaftlichen oder künstlerischen Zwecken (Art. 85 Abs. 2)

Betroffenenrechte – alte Bekannte

Art. 15 – Auskunftsrecht

- **(1) HS. 1: „ob"** personenbezogene Daten verarbeitet werden
- **(1) HS. 2: Auskunftsinhalt**
- **(2)**: wenn Übermittlung an **Drittstaaten** oder internationale Organisationen Information zu geeignete Garantien (Art. 46)
- **(3), (4)**: *NEU* – Zurverfügungstellung einer **Kopie** (ggf in gängigem elektronischen Format), soweit dadurch keine Rechte und Freiheiten anderer Personen beeinträchtigt werden

Art. 16 – Recht auf **Berichtigung**

- **S. 1**: bei unrichtigen Daten
  - „unverzüglich" (wohl ca. 2 Wochen, vgl. Art. 12 Abs. 4)
- **S. 2**: bei unvollständigen Daten (bezogen auf Zweck)
  - *wohl auch unverzüglich*

Art. 17 – (allg.) Recht auf Löschung

- **(1):** „unverzüglich" (wohl ca. 2 Wochen, vgl. Art. 12 Abs. 4); Katalog von **Gründen** (*NEU* - Recht auf Löschung im Fall von Erhebung aufgrund Art. 8 (1) > Kinder)
- **(3)**: **Ausnahme**: entgegenstehende (höhere) Interessen

Art. 18 – Recht auf **Einschränkung** der Verarbeitung („Sperrung")

- **(1):** Katalog von **Gründen**
- **(2): Folge**: Verarbeitung nur noch zu genannten Zwecken
- **(3)**: **Unterrichtung** der betroffenen Person durch Verantwortlichen vor Aufhebung der Sperre

Betroffenenrechte – öfter mal was Neues

Art. 17 (2) – „Recht auf **Vergessenwerden**"

entstanden nach EuGH-Urteil „Google Spain"; geht aber darüber hinaus

- durch Verantwortlichen veröffentlichte Daten oder
- Pflicht zur Löschung nach (1)

➢ „unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art" treffen, um (andere) Verantwortliche zu informieren, dass betroffene Person Löschung „aller Links" od. „Kopien" od. „Replikationen" verlangt hat

- **(3)**: **Ausnahme**: entgegenstehende (höhere) Interessen

Art. 20 – Recht auf **Datenübertragbarkeit**

- **(1):** Bereitstellung und Übermittlung die Person betreffende Daten, die sie selbst bereitgestellt hat, wenn Verarbeitung auf Einwilligung (Art. 6 (1) lit. a/Art. 9 (2) lit. a) oder Vertrag (Art. 6 (1) lit. b) beruht und Verarbeitung mithilfe automatisierten Verfahrens erfolgt

➢ strukturiertes, gängiges und maschinenlesbares Format

➢ (selbst) ohne Behinderung durch Verantwortlichen an anderen Verantwortlichen übermitteln

- **(2)**: Recht dass Verantwortlicher **direkt** an anderen Verantwortlichen übermittelt, wenn „technisch machbar"
- **(3)**: nicht zugleich Löschpflicht
- **(4)**: Grenze: Rechte und Freiheiten anderer

Widerspruchsrecht I

Art. 21

1) Widerspruchsrecht in Fällen des Art. 6 Abs. 1 e und f, Art. 21 Abs. 1

- Verarbeitung zur Wahrnehmung öffentlicher Aufgaben oder zur Wahrung berechtigter Interessen des Verantwortlichen
- Widerspruchsgründe, die sich aus der besonderen Situation der betroffenen Person ergeben (atypische Konstellationen)
- Ausnahmen: a) zwingende schutzwürdige, überwiegende Gründe für die Verarbeitung oder b) Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (Art. 21 Abs. 1 S. 2)

→ Verarbeitungsverbot, Art. 21 Abs. 1 S. 2

→ Löschung der Daten, Art. 17 Abs. 1 c

2) Widerspruchsrecht gegen Direktwerbung, Art. 21 Abs. 2, 3

- ohne Angabe von Gründen
- Keine Ausnahmen

→ Verarbeitungsverbot bezüglich Direktwerbung, Art. 21 Abs. 3

→ Löschung der Daten, Art. 17 Abs. 1 c

Widerspruchsrecht II

Art. 21

3) Widerspruchsrecht gegen zu Forschungs- und Statistikzwecken erfolgende Verarbeitungen, Art. 21 Abs. 6

- Verarbeitung zu Forschungs- oder Statistikzwecken
- Widerspruchsgründe, die sich der besonderen Situation der betroffenen Person ergeben (atypische Konstellationen)
- Ausnahme: Verarbeitung ist erforderlich zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe, Art. 21 Abs. 6 Hs. 2

→ Verarbeitungsverbot bezüglich Forschungs- oder Statistikzwecken

→ Öffnungsklausel für nationalen Gesetzgeber für weitere Einschränkungen, Art. 89 Abs. 2, 3

4) Hinweispflicht, Art. 21 Abs. 4

- Bzgl. Widerspruchsrecht nach Abs. 1 und 2
- Spätestens bei Erhebung der Daten bzw. erster Kommunikation
- Ausdrücklicher, verständlicher Hinweis, getrennt von anderen Informationen

5) Sanktionierung, Art. 83 Abs. 5 b

- Bußgeldbewehrt

Automatisierte Einzelentscheidung (inkl. Profiling)

Art. 22 (1) – Grundsatz: Recht des Einzelnen, **nicht Objekt** einer **ausschließlich** auf **automatisierter** Verarbeitung beruhenden Entscheidung zu werden

Ausnahmen:

Abs. 2 *(Rückausnahme Daten nach Art. 9 (1); (4))*

lit. a – erforderlich für Abschluss eines **Vertrages** zw. Verantwortlichem u. betroffener Person

lit. c – mit ausdrücklicher **Einwilligung** der betroffenen Person

lit. b – aufgrund von **Rechtsvorschriften** der EU/Mitgliedstaaten

- denen Verantwortlicher unterliegt
- die angemessene Maßnahmen zur Wahrung der Rechte, Freiheiten und berechtigten Interessen betroffener Person enthalten

(3): angemessene **Maßnahmen** des Verantwortlichen zur Wahrung Rechte, Freiheiten und berechtigten Interessen betroffener Person;

mindestens:

- Recht auf Erwirkung des Eingreifen Person seitens Verantwortlichem
- Recht auf Darlegung eigenen Standpunktes
- Anfechtung Entscheidung

Technisch-organisatorische Maßnahmen, Privacy by Design, Privacy by Default

Art. 24: **technisch-organisatorische Maßnahmen (toM)**

- zur Sicherstellung und Erbringung des Nachweises (> Art. 5 (2); Art. 30), dass die Verarbeitung gemäß der DS-GVOerfolgt
- gemeint sind alle Handlungen die dem dienen: Ausrichtung technischer Systeme, Instruktion des Personals, Notfallpläne (Bspe. in Erw. 78)
- „**geeignet**" unter Berücksichtigung von (=„**risk based approach**")

  Art (Art. 4 Nr. 2), **Umfang** (Menge der Daten über Personen und Menge der Personen deren Daten einfließen, Erw. 75), **Umstände** (Kontext, örtlich, zeitlich) und **Zweck** (Art. 5 (1) lit. b))

  (gleichwertige Faktoren der Gesamtabwägung; Parameter zur Bestimmung von Wahrscheinlichkeit und Risiko)

  sowie

  Eintrittswahrscheinlichkeit (statistischer Erwartungswert) und **Schwere der Risiken** (Gewicht des bedrohten Rechts; mögliche materielle und immaterielle Schäden durch Verarbeitung, Erw. 75) für **Rechte** und **Freiheiten** (europäische Primär- und Sekundärrecht) betroffener Personen

⇒ *Risiko = Schadensschwere x Eintrittswahrscheinlichkeit*

- Pflicht zur regelmäßigen **Überprüfung** ((1) S. 2)

Art. 25: **Privacy by Design**, **Privacy by Default**

- Konkretisierung des Art. 24; gerichtet an Verantwortliche (vgl. Erw. 78) – *nicht Hersteller…*
- Datenschutz durch Technikgestaltung (Abs. 1); Datenschutz durch datenschutzfreundliche Voreinstellungen (Abs. 2)

„Dokumentation“

Art. 30 – Verzeichnis von *Verarbeitungstätigkeiten*

- „alle Verarbeitungstätigkeiten des Verantwortlichen“ – Bspe.: „Videoüberwachung“, „Telefonanlage“ etc.
- Sinn der Vorschrift: Erfüllung materieller Anforderungen verfahrensrechtlich absichern; Ansatzpunkt für Aufsicht – soll vorläufige RMK-Prüfung erlauben

- **(1)**: Pflicht für Verantwortliche; Mindestinhalt lit. a-g;
- **(2)**: *NEU* auch Pflicht für AV bzgl. „alle[r] Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung“; Mindestinhalt lit. a-d; insb.: dem jeweils Verantwortlichen zuzuordnen (vgl. li. b)
- **(3)**: Schriftform (auch elektronisch)
- **(4)**: Zurverfügungstellen gegenüber der Aufsichtsbehörde
- **(5)**: **Ausnahmen** und **Rückausnahmen**

- Nicht für „KMU“ *(weniger als 250 Mitarbeiter),*
- *außer*

– *von ihnen vorgenommene Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Personen*
– *Verarbeitung nicht nur gelegentlich, oder*
– *Verarbeitung (auch) von Daten gemäß Art.9 (1) bzw. gem. Art. 10*

Meldung von Datenschutzverstößen

Art. 33, 34

Verletzung des Schutzes personenbezogener Daten → Definition in Art. 4 Nr. 12

1) Pflicht des Verantwortlichen zur Meldung an die Aufsichtsbehörde, Art. 33

- Unverzüglich, möglichst binnen 72 Stunden ab Bekanntwerden, Art. 33 Abs. 1 S. 1
- Inhalt der Meldung: Beschreibung der Datenschutzverletzung und ungefähre Zahl der betr. Datensätze, Name und Kontaktdaten des DSB, Folgenbeschreibung, Beschreibung ergriffener oder vorgeschlagener Maßnahmen, Art. 33 Abs. 3
- Ausnahmen: voraussichtlich kein Risiko für Rechte und Freiheiten, Art. 33 Abs. 1 letzter HS
- Bußgeldbewehrt, Art. 83 Abs. 4 a

2) Pflicht des Auftragsverarbeiters zur Meldung an den Verantwortlichen, Art. 33 Abs. 2

3) Pflicht des Verantwortlichen zur Benachrichtigung der Betroffenen, Art. 34

- Voraussichtlich hohes Risiko für Rechte und Freiheiten, Art. 34 Abs. 1
- Unverzüglich, Art. 34 Abs. 1
- Inhalt der Meldung: Namen und Kontaktdaten des DSB, Folgenbeschreibung, Beschreibung ergriffener oder vorgeschlagener Maßnahmen, Art. 34 Abs. 2
- In klarer und einfacher Sprache, Art. 34 Abs. 2
- Ausnahmen: geeignete technische oder organisatorische Sicherheitsvorkehrungen getroffen (so dass Daten unzugänglich sind) oder andere nachfolgende Maßnahmen getroffen (so dass sich aller Wahrscheinlichkeit nach Risiko nicht mehr realisiert) oder einzelne Benachrichtigung bedeutet unverhältnismäßigen Aufwand (dann öffentliche Bekanntmachung), Art. 34 Abs. 3
- Bußgeldbewehrt, Art. 83 Abs. 4 a

Datenschutz-Folgenabschätzung

Art. 35

WANN

Wenn eine Verarbeitungsform ein ***hohes Risiko*** für die Rechte und Freiheiten natürlicher Personen darstellt; zu beurteilen anhand: Art, Umfang, Umständen, Zwecken (vgl. Folie zu toM); zeitlich: „*vorab*“ **(1)**

„Insbesondere“ in **(3)**

a) Systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen basierend auf automatisierter Verarbeitung, wenn dies Grundlage für rechtswirksame Entscheidungen

b) Umfangreiche Verarbeitung von Daten nach Art. 9 Abs. 1/Art. 10

c) Systematische und umfangreiche Überwachung öffentlich zugänglicher Bereiche

Ggf. ***Ausnahme*** **(10)**

WAS

Mindestanforderungen **(7)**

a) systematische Beschreibung der Verarbeitungsvorgänge und -zwecke (ggf berechtigtes Interesse des Verantwortlichen darzulegen),

b) Bewertung von Notwendigkeit und VHM in Bezug auf den Zweck,

c) Bewertung der Risiken für Rechte und Freiheiten gem. Abs. 1,

d) geplante Abhilfemaßnahmen einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren zur Bewältigung der Risiken

WER

der ***Verantwortliche*** (*NEU*) nicht der bDSB); Einholung Rat bDSB, sofern benannt **(1, 2)** ggf Einholung Standpunkt Betroffener **(9)**

Art. 37

I) Benennung, Art. 37

1) Pflicht zur Benennung

- Datenverarbeitung durch Behörde oder öffentliche Stelle, Art. 37 Abs. 1 a
- Durchführung von Verarbeitungsvorgängen, die umfangreiche, regelmäßige und systematische Überwachung erfordern, Art. 37 Abs. 1 b (z.B. Auskunfteien)
- umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten, Art. 37 Abs. 1 c (z.B. Krankenhäuser)
- Nach nationalen Vorschriften (Öffnungsklausel), Art. 37 Abs. 4 S. 1 HS 2

2) Anforderungen, Art. 37 Abs. 5

- Berufliche Qualifikation und Fähigkeit zur Erfüllung der Aufgaben des DSB
- Fachwissen auf dem Gebiet des Datenschutzes

3) Rechtsverhältnis zum Verantwortlichen

- Interner oder externer DSB (auch bei Behörden), Art. 37 Abs. 6
- Gemeinsamer DSB bei Unternehmensgruppen oder Behörden, Art. 37 Abs. 2, 3

4) Veröffentlichungs- und Mitteilungspflicht, Art. 37 Abs. 7

Art. 38 – 39

II) Stellung des DSB, Art. 38

- Einbindung des DSB in relevante Verarbeitungsvorgänge, Art. 38 Abs. 1
- Unterstützungspflicht des Verantwortlichen, Art. 38 Abs. 2
- Unabhängigkeit des DSB, Art. 38 Abs. 3 S. 1
- Abberufungs- und Benachteiligungsverbot, Art. 38 Abs. 3 S. 2 (kein Kündigungsschutz nach GVO)
- Kein Interessenkonflikt, Art. 38 Abs. 6

III) Aufgaben, Art. 39

- Mindest-Aufgaben
- Z.B. Beratung, Überwachung, Zusammenarbeit mit Aufsichtsbehörde

IV) Sanktionen

- Bußgeldbewehrt, Art. 83 Abs. 4 a

V) Öffnungsklausel für nationales Recht → s. „BDSG neu“

Verhaltensregelungen – Zertifizierungen

Art. 40 – **Verhaltensregeln**

(1): **Förderungsverpflichtung** – Mitgliedstaaten, Aufsichtsbehörden, EDSA und KOM

(2): vorlageberechtigte **Institutionen**: Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder ADV vertreten („Repräsentationserfordernis");
Inhalte: Beispiele zu präzisierender Bereichen (a-k)

(3): mögliche „geeignete Garantie" für **Übermittlung** in **Drittstaat**, wenn sich Empfänger vertraglich oder rechtlich an die Verhaltensregeln bindet (i.V.m. Art. 46 (2) lit. e)

(4): Vorgaben zu **Überwachungsverfahren** (durch Stellen nach Art. 41)

(5): Vorlage bei und Genehmigung durch Aufsichtsbehörde (Art. 55)

- Im Übrigen: verschiedene Vorgaben für Geltung in einem Mitgliedstaat oder mehreren ((5)-(9)); Veröffentlichungs- und Registerpflichten (10, 11)

Art. 42 – **Zertifizierungsverfahren**, **Datenschutzsiegel** und –**prüfzeichen**

(1): **Förderungsverpflichtung** – Mitgliedstaaten, Aufsichtsbehörden, EDSA und KOM

(2): mögliche auch solche Instrumente als „geeignete Garantie" für **Übermittlung** in **Drittstaat** zu schaffen, wenn sich Empfänger vertraglich oder sonst rechtlich an sie bindet (i.V.m. Art. 46 (2) lit. f)

(3, 4, 6): Freiwilligkeit, transparentes **Verfahren**; Weitergeltung DS-GVO; Kooperation

(5): Erteilung (durch Stellen nach Art. 43 oder Aufsichtsbehörde)

(7): Gültigkeitsdauer, Widerruf und Überprüfung

(8): Prüfzeichenregister

Internationaler Datenverkehr I

Art. 44 – 49

Allgemeine Grundsätze, Art. 44

- Verbot mit Erlaubnisvorbehalt
- Drittländer: alle Nicht-EU-Staaten
- Übermittlung als solche muss erlaubt sein (2-Stufen-Prüfung)

Erlaubnis-Tatbestände:

- Angemessenheitsbeschluss der KOM, Art. 45 (auch EU-US-Privacy Shield)
- Rechtlich bindende und durchsetzbare Dokumente zwischen Behörden, Art. 46 Abs. 2 a
- Verbindliche unternehmensinterne Datenschutzvorschriften (BCR), Art. 46 Abs. 2 b
- Standarddatenschutzklauseln, Art. 46 Abs. 2 c, d
- Daten importierendes Unternehmen verfügt über genehmigte Verhaltensregeln gemäß Art. 40, Art. 46 Abs. 2 e
- Daten importierendes Unternehmen verfügt über genehmigte Zertifizierung gemäß Art. 42, Art. 46 Abs. 2 f
- Genehmigte Vertragsklauseln, Art. 46 Abs. 3 a
- Genehmigte Verwaltungsvereinbarungen (ohne rechtliche Verbindlichkeit) zwischen Behörden, Art. 46 Abs. 3 b

Internationaler Datenverkehr II

Art. 44 – 49

Ausnahme-Tatbestände, Art. 49:

- Einwilligung des Betroffenen, Art. 49 Abs. 1 a (gilt nicht für Behörden, Art. 49 Abs. 3)
- Erforderlich zur Vertragserfüllung, Art. 49 Abs. 1 b (gilt nicht für Behörden, Art. 49 Abs. 3)
- Erforderlich zur Vertragserfüllung mit einem Dritten im Interesse des Betroffenen, Art. 49 Abs. 1 c (gilt nicht für Behörden, Art. 49 Abs. 3)
- Notwendig aus wichtigen Gründen des öffentlichen Interesses, Art. 49 Abs. 1 d
- Erforderlich zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen, Art. 49 Abs. 1 e
- Erforderlich zum Schutz lebenswichtiger Interessen, Art. 49 Abs. 1 f
- Übermittlung aus einem Register zur Information der Öffentlichkeit, Art. 49 Abs. 1 g
- Erforderlich zur Wahrung berechtigter Interessen des Verantwortlichen (keine wiederholte Übermittlung, begrenzte Zahl von Betroffenen, keine überwiegenden Schutzinteressen und geeignete Garantien, Meldung an Aufsichtsbehörde und Betroffene), Art. 49 UAbs. 2 (gilt nicht für Behörden, Art. 49 Abs. 3)

Aufsichtsbehörden

„Jeder Mitgliedstaat sieht vor, dass eine oder mehrere **unabhängige Behörden** für die **Überwachung** der Anwendung dieser **Verordnung** zuständig sind, damit die **Grundrechte** und **Grundfreiheiten** natürlicher Personen bei der Verarbeitung **geschützt** werden und der **freie Verkehr personenbezogener Daten** in der Union **erleichtert** wird (im Folgenden „Aufsichtsbehörde“).“ (Art. 51 (1))

➢ „Ausgestaltung“: Unabhängig (Art. 52), allg. Bedingungen für Ernennung Mitglieder (Art. 53), Vorgaben zu nationalen Rechtsvorschriften und Verschwiegenheitspflicht (Art. 54)

Zuständigkeit, Art. 55/56

- ***sachlich***: „Erfüllung der **Aufgaben** und die Ausübung der **Befugnisse**“ die durch **DS-GVO** übertragen sind (Art. 55 (1)); nicht für Gerichte soweit „justizielle Tätigkeit“ (Art. 55 (3))
- ***örtlich***:

– Art. 55 (1); Art. 56: „**Federführung**“ wenn Hauptniederlassung oder einzige Niederlassung in eigenem Hoheitsgebiet

– „**betroffen**“ bei Beschwerden aus, bzw. Verstößen im eigenen Hoheitsgebiet (dann: Unterrichtung federführende Behörde, (3)-(6)), Ausnahme: bei Art. 6 (1) lit. c/e nur betroffener Mitgliedstaat (Art. 55 (2))

Aufgaben, Art. 57

- Verweis auf **DS-GVO** und ergänzend/zusammenfassend **Katalog** (a-v), **(1)**
- **Modalitäten: (2)-(4)**: (z.B. auch) elektronisches Beschwerdeformular bereithalten; Unentgeltlichkeit ggü Betroffenen („ggf“ ggü DSB), Gebühr bei offenkundig unbegründeten oder exzessiven Anfragen möglich; jährlicher Tätigkeitsbericht

Befugnisse, Art. 58

(1): **Untersuchung**sbefugnisse; z.B. Datenschutzüberprüfungen, Zugang erhalten

(2): **Abhilfe**befugnisse; z.B. Verwarnen, Anweisen zu Benachrichtigung über data breach, Geldbuße verhängen

(3): **Genehmigung**sbefugnisse; z.B. zu Datenschutzfragen an Öffentlichkeit wenden, Zertifizierung erteilen

➢ Ausübung nach nationalem Recht; das geeignete Rechtsbehelfe und ordnungsgemäße Verfahren bieten muss, (4)

➢ National Möglichkeit schaffen, gerichtliches Verfahren einzuleiten *(ohne Einschränkung)*, (5)

Art. 60

→ verpflichtendes Verfahren der Zusammenarbeit verschiedener Aufsichtsbehörden bei grenzüberschreitendem Datenverkehr

→ gilt nicht für Einzelfälle im öffentlichen Bereich, Art. 55 Abs. 2 S. 1, 2

1) Grenzüberschreitender Datenverkehr, Art. 4 Nr. 23:
   - Erfolgt in mehr als einem Mitgliedstaat
   - Betrifft Personen in mehreren Mitgliedstaaten

2) Federführende/betroffene Aufsichtsbehörde:
   - Federführende Aufsichtsbehörde = Aufsichtsbehörde der Hauptniederlassung des Verantwortlichen, Art. 56 Abs. 1
   - Betroffene Aufsichtsbehörde = Aufsichtsbehörde einer Niederlassung des Verantwortlichen in einem Mitgliedstaat oder Aufsichtsbehörde für betroffene Personen in einem Mitgliedstaat, Art. 4 Nr. 22

3) Kohärenzverfahren im Einzelnen: Art. 60
   (1) Entscheidungsentwurf der federführenden Aufsichtsbehörde
   (2) Information an die betroffenen Aufsichtsbehörden
   (3) Abstimmung über den Beschlussentwurf (4 Wochen Frist)
   (4) Ggf. Vorlage an den EDSA
   (5) Ggf. Entscheidung durch den EDSA
   (6) Ausführung der Entscheidung durch die federführende Aufsichtsbehörde

Europäischer Datenschutzausschuss

Art. 68 ff Europäischer Datenschutzausschuss (EDSA, „**Ausschuss**")

Stellung, Art. 68

(1): Einrichtung der EU mit eigener ***Rechtspersönlichkeit***

(2): Besetzung

- **Vertreter**: ein ***Vorsitz***, zwei Stellvertreter, zu wählen durch Mitglieder (Art. 73, 74)
- **Mitglieder**: Leiter der Aufsichtsbehörden + EDPS (bzw. jeweilige Vertreter); die KOM ist teilnahmeberechtigt (kein Stimmrecht) und wird unterrichtet (5)

- ***Unabhängig*** und weisungsungebunden (Art. 69)
- eigene ***Geschäftsordnung*** (Art. 72 (2), 74 (2)), Beratungen „erforderlichenfalls" vertraulich (Art. 76 (1))

Aufgaben, Art. 70

(1): „Sicherstellung der ***einheitlichen Anwendung*** der DSGVO", durch…

(2): …abschließenden Katalog (a-y) – wesentliche ***Instrumente***: Beratung der und Stellungnahmen für die KOM, Ausarbeitung/Bereitstellung/Überarbeitung von Leitlinien, Empfehlungen und bewährten Verfahren;

Jahresberichterstattung (Art. 72) an Europäisches Parlament, Europäischen Rat und KOM

Sekretariat, Art. 75

(1): gestellt vom EDPS

(2): aber Weisung des Vorsitzes unterstellt

- „analytische, administrative und logistische Unterstützung" für EDSA, z.B. Tagesgeschäft, innere u äußere Kommunikation, Vor- u Nachbereitung Sitzungen (Abs. 5/6)

Art. 77 – 82

I) Rechtsbehelfe der betroffenen Person

- Beschwerde bei einer Aufsichtsbehörde, Art. 77
  - Pflicht zur Unterrichtung über Stand und Ergebnisse der Beschwerde, Art. 77 Abs. 2
  - Bei Aufsichtsbehörde der Wahl, Beteiligung der zuständigen Aufsichtsbehörde, aber „Single Point of contact“ für Beschwerdeführer
  - Keine Bearbeitungspflicht bei offenkundig unbegründeten o. exzessiven Beschwerden, Art. 57 Abs. 4
- Gerichtlicher Rechtsbehelf gegen die Aufsichtsbehörde, Art. 78
  - gegen rechtsverbindliche Beschlüsse der Aufsichtsbehörde, Art. 78 Abs. 1 oder
  - bei Untätigkeit der Aufsichtsbehörde, Art. 78 Abs. 2
- Gerichtlicher Rechtsbehelf gegen den Verantwortlichen oder Auftragsverarbeiter, Art. 79
  - bei Verletzung eigener Datenschutzrechte der betroffenen Person
- Schadensersatz, Art. 82

II) Verfahrens- und Prozessvertretung, Art. 80 Abs. 1

- Nach Beauftragung durch die betroffenen Person
- Einrichtung, Organisation oder Vereinigung ohne Gewinnerzielungsabsicht, im Bereich Datenschutz tätig
- Vertretung bzgl. Rechten nach Art. 77 – 79 und 82

III) Verbandsbeschwerde bzw. –klagerecht, Art. 80 Abs. 2

- Nach nationalem Recht (Öffnungsklausel)

Art. 83, 84

I) Allgemeines

- Geldbußen sollen wirksam, verhältnismäßig und abschreckend sein, Art. 83 Abs. 1
- Geldbußen sind neben oder anstelle von Abhilfemaßnahmen der Aufsichtsbehörde möglich, Art. 83 Abs. 2 S. 1
- Kriterien für die Verhängung und die Bemessung von Geldbußen: z.B. Schwere des Verstoßes, Vorsatz oder Fahrlässigkeit, Umfang der Zusammenarbeit mit der Aufsichtsbehörde, Art. 83 Abs. 2 a – k
- Öffnungsklausel für Geldbußen gegen Behörden nach nationalem Recht, Art. 83 Abs. 7
- Öffnungsklausel für strafrechtliche Sanktionen nach nationalem Recht, Art. 84 → s. „BDSG neu“

II) Bußgeldtatbestände und Bußgeldrahmen

- Verstöße gegen Pflichten eines Verantwortlichen oder Auftragsverarbeiters, Art. 83 Abs. 4: z.B. bzgl. technisch-organisatorischen Maßnahmen, Dokumentationspflicht, Meldung von Datenschutzverletzungen → bis zu 10 000 000 Euro oder bis zu 2 % des Jahresumsatzes eines Unternehmens
- Verstöße gegen Rechte der Betroffenen, Art. 83 Abs. 5: z.B. bzgl. Rechtsgrundlage, Grundsätze der GVO, Betroffenenrechte → bis zu 20 000 000 Euro oder bis zu 4 % des Jahresumsatzes eines Unternehmens
- Verstöße gegen Anweisung einer Aufsichtsbehörde, Art. 83 Abs. 6 → bis zu 20 000 Euro oder bis zu 4 % des Jahresumsatzes eines Unternehmens

Besondere Verarbeitungssituationen

- Meinungsfreiheit, Presse- und Informationsfreiheit, Wissenschaft, Kunst und Literatur, Art. 85
  - *Soweit „erforderlich"; Mitteilung an Kommission*
- Informationsfreiheit, Art. 86
  - *Amtliche Dokumente; wohl Fortgeltung Informationsfreiheits-/zugangsgesetze*
- Nationale Kennziffern, Art. 87
- Beschäftigtendatenschutz, Art. 88
  - *Mitteilung an Kommission bis 25.05.2018*
- Archiv, Wissenschaft, Forschung und Statistik, Art. 89
  - *Ausnahmen, soweit für spezifische Zwecke notwendig*
- Zuständigkeit LfD für Berufsgeheimnisträger, Art. 90
  - *Soweit „notwendig und verhältnismäßig"; Mitteilung an Kommission bis 25.05.2018*
- Kirchen und religiösen Gemeinschaften, Art. 91
  - *Fortgeltung eigener Regelungen soweit im Einklang mit DS-GVO*