Datenschutzrecht

Auftragsverarbeitung,
aktuelle Forschungsfragen im Datenschutz

1. Juni 2026

Harald Zwingelberg

Ansprechpartner Vorlesungsreihe: Benjamin Bremert

Vertretene Auffassungen sind solche des Referenten bzw. teilweise Ergebnisse aus Projekten und nicht keine Positionierung des ULD.

Ankündigungen

- Gesetzestexte für Vorbereitung und Klausur:
  - DSGVO (insbesondere Art. 1-40)
  - https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32016R0679
  - Druckfassung bereitgestellt: https://www.datenschutzzentrum.de/uploads/vorlesungen/cau/Gesetzessammlung.pdf

- Soweit nicht anders gekennzeichnet, sind alle genannten Artikel solche der DSGVO.

Agenda

- Wiederholung
- Auftragsverarbeitung
- Transparenz

Wiederholung

Grundlagen

Wiederholung

- Wo sind die Grundprinzipien des Datenschutzes geregelt?
  - Art. 5 DSGVO

- Nennen sie die Grundprinzipien und deren Kerninhalt
  1. Rechtmäßigkeit, Art. 5 I a
  2. Zweckbindung, Art. 5. I b
  3. Erforderlichkeit, Art. 5 I b, c (u.a. Datenminimierung)
  4. Transparenz, Art. 5 I a (Auskunft, …)
  5. Integrität und Vertraulichkeit Art. 5 I f (Datensicherheit)
  6. Rechenschaftspflicht, Art. 5 II

*Wiederholung *)*
Sechs Goldene Regeln des Datenschutzes

Welche Grundsätze des Datenschutzes kennen Sie?

- Rechtmäßigkeit
  - Gesetz, Einwilligung, Vertrag, Dienst- oder Betriebsvereinbarung
- Zweckbindung
  - Weiterverarbeitung nur für einem mit Erhebungszweck vereinbaren Zweck
- Datenminimierung und Speicherbegrenzung
  - Verarbeitung nur soweit für Erhebungszweck erforderlich
- Transparenz und Betroffenenrechte
  - Unterrichtung über Verwendung, Auskunfts-/Berichtigungs-/Löschrechte
- Integrität und Vertrautlichkeit
  - Technische und organisatorische Maßnahmen, Integrität und Vertraulichkeit
- Kontrolle
  - Interner / externer Datenschutzbeauftragter

*) Zum ganzen siehe Vorlesungsfolien von B. Bremert „Einführung Datenschutzrecht I und II"
Ausführlich zu Data Protection Principles, B. Bruegger, http://guidelines.panelfit.eu/the-gdpr/main-principles/
und als Vortragsfolien (CC-by-Lizenz) https://www.datenschutzzentrum.de/uploads/projekte/anomed/GDPR-Principles.pdf

AnoMed
PANELFIT

Wiederholung
Art. 6 DSGVO: Zentrale Befugnisnorm

- Datenverarbeitung ist (nur!) rechtmäßig, wenn:
  - **Einwilligung**
  - **Vertragserfüllung**
  - **Erfüllung rechtlicher Verpflichtung**
  - Lebenswichtige Interessen
  - Ausübung öffentliche Gewalt
  - **Wahrung berechtigter Interessen, sofern Interessen des Betroffenen nicht überwiegen *)**

*) Ausführlich zur Verarbeitung für berechtigte Interessen nach Art. 6 I f DSGVO:
Robrahn/Bremert, Interessenskonflikte im Datenschutzrecht, ZD 2018, 291ff.
Autorenversion frei verfügbar :
https://www.datenschutzzentrum.de/uploads/projekte/itesa/Robrahn-Bremert-Artikel6abs1fDSGVO.pdf

Wiederholung
Besondere Kategorien personenbez. Daten

- Art. 9 (1) DSGVO:
  Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer nat. Person ist untersagt.

- Art 9 (2) DSGVO: Ausnahmen vom Verbot u.a. für Behanldung und Forschung

Auftragsverarbeitung

Auftragsverarbeitung als rechtliche Gestaltungsmöglichkeit

Anforderungen, Umfang, Rechtsfolgen

Auftragsdatenverarbeitung Anwendungsbereich, Bedeutung

Problemstellung

- Relevante Grundsätze des Datenschutzrechts:
  - Rechtmäßigkeit, Art. 5 (1) DSGVO daher sind erforderlich:
    - Einwilligung, Art. 6 (1) (a) oder
    - anderweitige gesetzliche Rechtsgrundlage, Art. 6 (1) …
  - Datensicherheit

Folge

- Bei jedem Datenfluss ist grundsätzlich zu prüfen, ob es einer Rechtsgrundlage (RGL) für die Übermittlung bedarf und die Sicherheit der Verarbeitung ist zu gewährleisten.
- Erhebung durch Dritten bedarf eigener RGL für Empfänger.

Auftragsdatenverarbeitung Anwendungsbereich, Bedeutung

- Typische Anwendungsbereiche der Auftragsverarbeitung
  - Hosting (insbesondere mit Webshop und Kundendaten),
  - externe Datensicherung,
  - IT-Betreuung, soweit Zugriff auf personenbez. Daten besteht,
  - Aktenvernichtung,
  - Druck- und Versandleistungen (Lettershop),
  - Lohnbuchhaltung,
  - Callcenter,
  - Kundenservice durch Service-Partner
  - SaaS
  - …

Auftragsdatenverarbeitung Definitionen

Begriffsbestimmungen für Akteure der Datenverarbeitung

- Art. 4 (7) DSGVO: ***Verantwortlicher*** ist die [Einrichtung], die allein oder gemeinsam mit anderen Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet… (Engl.: controller)

- Art. 4 (8) DSGVO: ***Auftragsverarbeiter*** ist eine [Einrichtung] die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (Eng.: processor)

- Art. 26 (1) DSGVO: ***Gemeinsam Verantwortliche***: Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke und die Mittel zur Verarbeitung fest, sind sie gemeinsam Verantwortliche. (Engl.: joint controllers)
  - Zentraler Punkt in jüngeren EuGH-Urteilen: Gemeinsam Verantwortliche sind ein Webseitenbetreiber, der mittels Einbindung eines Social-Media-Plugins auf der eigenen Webseite (EuGH 2019, Fashion ID, C-40/17, Rn. 81) oder mittels Nutzung eine Fanpage (EuGH 2018, Wirtschaftsakademie, C-210/16, Rn. 39) Datenflüsse an den Plattformbetreiber veranlasst.

Auftragsdatenverarbeitung Voraussetzungen

Voraussetzungen Art. 28 DSGVO

- völlige Weisungsabhängigkeit des Auftragsverarbeiters
- Vertrag mit bestimmten Mindestinhalten, Art. 28 (3) – Teil 1
  - Art und Zweck der Verarbeitung, Dauer, Art der personenbezogenen Daten, Kategorien betroffener Personen
  - Bindung des Auftragsverarbeiters an Weisungen des Verantwortlichen
  - Pflichten und Rechte des Verantwortlichen gegenüber dem Auftragsverarbeiter
  - Verarbeitung nur auf Basis dokumentierter Weisung des Verantwortlichen Besteht ausnahmsweise eine Rechtspflicht des Auftragsverarbeiters zur Übermittlung an Dritte muss der Auftragsverarbeiter diese rechtlichen Rahmenbedingungen vor der Verarbeitung dem verantwortlichen mitteilen. lit. a)
  - Mitarbeiter des Auftragsverarbeiters müssen zur Vertraulichkeit verpflichtet werden. lit b)

Auftragsdatenverarbeitung Voraussetzungen

Voraussetzungen Art. 28 DSGVO

- Vertrag mit bestimmten Mindestinhalten, Art. 28 (3) – Teil 2 (Fortsetzung)
  - Erforderliche techn.-org. Maßnahmen nach Art. 32 sind zu bestimmen. lit c)
  - Auflagen bei der Inanspruchnahme von (Unter-)Auftragsverarbeitern durch den Auftragsverarbeiter. lit. d)
  - Unterstützung des Verantwortlichen bei der Gewährung von Betroffenenrechten
  - Löschung oder Rückgabe aller Daten nach Abschluss der Verarbeitung
  - Überlassen der nötigen Informationen, um die Einhaltung der Vorschriften auch gegenüber Prüfern nachzuweisen
- Form: Textform genügt, Unterschrift ist nicht notwendig.
- Verantwortlicher muss Auftragsverarbeiter risikoangemessen auswählen und während der gesamten Dauer des Auftragsverhältnisses überwachen (Art. 28 Abs. 1, Art. 24 DSGVO).

Auftragsdatenverarbeitung
Art. 28 als RGL für Übermittlung und DV

Art. 28 als eigenständige Rechtsgrundlage?

Muss neben Art. 28 zusätzlich eine Rechtsgrundlage aus Art. 6 für den Datentransfer zum Auftragsverarbeiter gegeben sein?

- Antwort: Nein, Art. 28 ist Rechtsgrundlage für die Übermittlung und die Verarbeitung im Rahmen des Auftrags.
  Grund: Auftragnehmer wird als quasi-interne Stelle des Verantwortlichen behandelt. Die Trennung macht nur Sinn, wenn mit Einhalten der Anforderungen nicht zusätzlich eine RGL bestehen müsste. Ansonsten würde ja bereits die RGL den Datenfluss ohne Extra-Aufwand gestatten.

- Der Verantwortliche braucht weiterhin eine eigene RGL und muss die weiteren Voraussetzungen der DSGVO einhalten, z.B. für technisch-organisatorische Maßnahmen.

Auftragsdatenverarbeitung Pflichten

Pflichten / Aufgaben des Verantwortlichen

- Sorgfältige Auswahl und Überwachung nach Art. 28
- Vertragliche Bindung
- Bereitstellung der erforderlichen Informationen für den Auftragsverarbeiter

Pflichten des Auftragsverarbeiters

- Bei Sitz im Drittland – Bestellung eines Vertreters in der Union, Art. 27
- Eigenes Verzeichnis der Verarbeitungstätigkeiten, Art. 30 (2)
- Vornahme der erforderlichen techn.-org. Maßnahmen (TOMs)
- Meldung von Sicherheitsverstößen an den Verantwortlichen, sofort zwecks Einhaltung der 72-h-Meldefristen, Art. 33 (2)
- Unterstützung bei der Datenschutzfolgenabschätzung
- Benennung eines Datenschutzbeauftragten

Auftragsdatenverarbeitung Rechtsfolgen

Rechtsfolgen

- Datentransfer zum und Verarbeitung beim Auftragsverarbeiter ist privilegiert, d.h. sie bedarf keiner gesonderten Rechtsgrundlage neben dem Auftrag.

- Geldbußen wegen Verstoß gegen die eigenen Pflichten können gegen den Auftragsverarbeiter direkt verhängt werden.

- Ein fehlender Vertrag über die Auftragsverarbeitung ist für beide Parteien bußgeldbewährt, so dass Auftragnehmer einen solchen aus Eigeninteresse anbieten sollten.
  Hinweis: Gute Anbieter im DSGVO-Raum bieten diese Verträge proaktiv an.

Auftragsdatenverarbeitung

Rechtsstellung Auftragsverarbeiter

- Auftragsverarbeiter haftet nur für die Verletzung der speziellen Pflichten eines Auftragnehmers oder bei Verstoß gegen eine Weisung auf Schadensersatz, Art. 82 (2).

- Bei Überschreiten des Auftrags wird Auftragsverarbeiter mit allen Pflichten und Risiken zu einem Verantwortlichen.
  - D.h. er hat alle datenschutzrechtlichen Pflichten
  - D.h. nicht, dass die Daten da dann auch zu Recht verarbeitet werden, vielmehr wird regelmäßig eine unzulässige Verarbeitung, ggf. auch ein sanktionsfähiger Verstoß vorliegen.

Auftragsdatenverarbeitung Verstöße

Verstöße des Verantwortlichen

- Verantwortlicher hat nach Vertragsende Kontrollpflicht bezüglich der Löschung personenbezogener Daten beim Auftragnehmer.

  [OLG Dresden, 15.10.2024 - 4 U 422/24, https://openjur.de/u/2496904.html]

- Verantwortlicher muss Löschung nach Vertragsende sicherstellen. Andernfalls Haftung für data breach beim Auftragsverarbeiter. [BGH 11.11.2025 - VI ZR 396/24]

- Fehlerhafte Abgrenzung zwischen Auftrag und gemeinsamer Verantwortlichkeit: Falscher Vertrag ist Datenschutzverstoß. Bei Unsicherheit: Dokumentation transparent halten, sodass Korrekturen mit minimalem Aufwand möglich sind.

Gemeinsame Verantwortlichkeit

Abgrenzung von (gemeinsam) Verantwortlichen

- Verantwortlicher ist wer Zwecke und wesentliche Mittel der Verarbeitung bestimmt – wer nur nicht-wesentliche Mittel bestimmt, kann Auftragsverarbeiter bleiben.
  - Wesentliche Mittel (essential means): Zweckbestimmung, Datenkategorien, Personenkreis, Aufbewahrungsfristen, Zugriffsberechtigungen (Art. 4 Nr. 7 DSGVO)
  - Nicht-wesentliche Mittel: Technische Implementierung, Wahl der Software, Serverstandort, konkrete Sicherheitsmaßn.
  - Eingeschränkte Entscheidungsbefugnisse bei der Durchführung schließen eine Auftragsverarbeitung nicht automatisch aus

Näher dazu: EDPB Guidelines 07/2020 v2.1, Rn. 28 ff. https://www.edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf

Gemeinsame Verantwortlichkeit

Abgrenzung Auftrag und gemeinsame Verantwortlichkeit

- Indizien für Auftragsverarbeitung:
  - besonders ausführliche Weisungen,
  - engmaschige Überwachung
  - Auftragsverarbeiter weckt Eindruck, er gehöre organisatorisch zum Verantwortlichen.

- Indizien für (eigene) Verantwortlichkeit:
  - Gemeinsame Verantwortlichkeit möglich, auch ohne direkten Datenzugriff einer Partei [EuGH, IAB Europe, C-604/22, 7.3.2024]
  - Einige freie Berufe haben auf Grundlage der Berufsordnungen eigenständige Rechtsgrundlagen für die Verarbeitung, da diese nur Teil einer umfassenderen Beratungsfunktion gegenüber Ihren Kunden ist. Beispiele Rechtsanwälte, Steuerberater, Psychologen… Diese sind dann Verantwortliche.

Quellen: EDSA, Guidelines 07/2020.

Auftragsdatenverarbeitung in Drittstaaten

Ist Sitz des Auftragnehmers im Drittstaat möglich?

- Drittstaat = außerhalb des EWR (EU + Island, Liechtenstein und Norwegen), insbesondere USA
- DSGVO: Art. 27 (1) begründet auch für Auftragsverarbeiter die ausdrückliche Pflicht zur Bestellung eines Vertreters in der Union. Im Umkehrschluss: Auftragsverarbeitung in Drittstaaten ist nicht per se verboten.
- Ein Übermittlungsinstrument nach Art. 44 ff. DSGVO muss kumulativ zum AV-Vertrag nach Art. 28 DSGVO vorliegen

Übermittlungsinstrumente

- Angemessenheitsbeschluss der EU-Kommission (Art. 45 DSGVO): UK, JP, für USA: EU-US Data Privacy Framework nur für zertifizierte US-Unternehmen
- Standarddatenschutzklauseln (SCCs) der EU-Kommission (Art. 46 Abs. 2 lit. c DSGVO): SCCs 2021, Modul 2 (Verantwortlicher => Auftragsverarbeiter)
- Transfer Impact Assessment (TIA): Nach EuGH Schrems II (C-311/18) reicht SCC-Abschluss allein nicht. Zusätzlich: Pflicht zur Prüfung des tatsächlichen Schutzniveaus im Drittland vor dem Transfer (Klausel 14 SCCs 2021)

Auftragsdatenverarbeitung in Drittstaaten

KI-Dienste als Auftragsverarbeiter in Drittstaaten

Ausgangslage:

- Einsatz von KI-APIs (z. B. OpenAI, Google Gemini, Anthropic, AWS Bedrock) = typischerweise Auftragsverarbeitung nach Art. 28 DSGVO
- Anbieter mit Sitz in USA → automatisch Drittstaatentransfer: Art. 28 und Art. 44 ff. DSGVO müssen kumulativ erfüllt sein
- Selbst wenn API-Endpunkt in der EU liegt: Muttergesellschaft unterliegt US-Recht (CLOUD Act) → kein automatisch ausreichendes Schutzniveau

Bewertung des EDPB (Opinion 28/2024)

- KI-Anbieter, der Prompts/Ausgaben verarbeitet, ist i. d. R. Auftragsverarbeiter, sofern er keine eigene Zweckbestimmung vornimmt
- KI-Anbieter, der Modell mit den übermittelten Daten weitertrainiert, wird zum eigenständigen Verantwortlichen => AV-Vertrag allein reicht dann nicht
- Vertrag muss Trainingsverbot explizit regeln – Opt-out-Klausel genügt nicht bei Daten gem. Art. 9 DSGVO

Auftragsdatenverarbeitung in Drittstaaten

KI-Dienste als Auftragsverarbeiter in Drittstaaten

Prüfschritte bei KI-Einsatz in den USA:

1. Enthält der Prompt personenbezogene Daten?
   (Kundentexte, Nutzerprofile, Logs)
2. AV-Vertrag Art. 28 Abs. 3 DSGVO mit Trainingsverbot, Sub-Processor-Liste, Löschfristen
3. Übermittlungsinstrument:
   EU-US DPF (zertifizierte Anbieter, Art. 45 DSGVO) => kein TIA erforderlich
   SCCs 2021 Modul 2 (Art. 46 Abs. 2 lit. c DSGVO) => TIA nach Klausel 14 erforderlich
4. Transfer Impact Assessment (TIA): bei SCC / BCR ist CLOUD Act-Risiko zu bewerten, ergänzende Maßnahmen dokumentieren

(!) Der AV-Vertrag allein genügt nicht. Es müssen auch die Art. 44 ff DSGVO erfüllt sein (Übermittlungsinstrument und TIA).

Auftragsdatenverarbeitung in Drittstaaten

Besondere Risiken: Staatliche Zugriffe

- Mögliche Risiken staatlicher Zugriffe auf Daten in Rechenzentren in Drittstaaten, aber auch auf Auftragsverarbeiter mit Sitz in Drittstaaten (selbst bei Rechenzentrum in der EU) können dazu führen, dass der Schutz der Rechte betroffener Personen nicht gewährleistet ist (Art. 28 Abs. 1 DSGVO)
  - US CLOUD Act (2018), 18 U.S.C. § 2713: Verpflichtet US-Provider zur Herausgabe von Daten an US-Behörden — auch bei Serverstandort in der EU und auch wenn nur die Muttergesellschaft US-amerikanisch ist
  - Konsequenz: Ein EU-Rechenzentrum allein garantiert kein ausreichendes Schutzniveau, wenn der Betreiber einer US-Konzernmutter untersteht → ist im TIA und bei der Auswahl des Auftragsverarbeiters zu bewerten
  - US-Behörden oder Gerichte können nicht einfach Herausgabe anordnen. Das EU-Recht gilt vorrangig. Eine Übermittlung auf deren Basis ist ohne RGL aus Art 6 und Vereinbarkeit mit den Art. 44 ff. DSGVO unzulässig. Solche Sachverhalte sind Frage für die Rechtsabteilung!

Quelle: Art. 48 DSGVO; EDPB Leitlinien zu Artikel 48 DSGVO, 02/2024

Zusammenfassung Auftragsverarbeitung

- Sind mehrere an der Datenverarbeitung beteiligt ist deren Verhältnis zueinander zu klären.

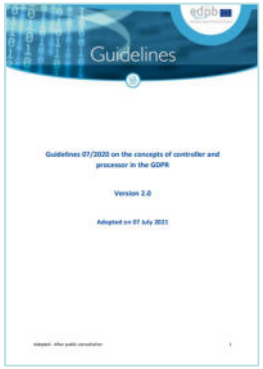
- Gemeinsame Verantwortlichkeit lässt die Notwendigkeit einer RGL nicht entfallen! Das Recht, die Daten zu verarbeiten / übermitteln, / auszutauschen, muss schon vorher vorhanden sein.

- Anders bei rechtmäßiger Auftragsverarbeitung. Diese ist für die Datenflüsse vom Verantwortlichen zum Auftragnehmer zugleich Rechtsgrundlage. Anforderungen, Rechte und Pflichten sowie Haftung sind in Art 28 DSGVO geregelt.

Weiterführendes

- DSK zur gemeinsamen Verantwortlichkeit
  https://www.datenschutzzentrum.de/uploads/dsgvo/kurzpapiere/DSK_KPNr_16_Gemeinsame-Verantwortliche.pdf

- Europäischer Datenschutzausschuss
  Guidelines 07/2020 on the concepts of controller and processor in the GDPR
  https://www.edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf



- LfD BaWü
  zusammenfassende FAQ zu Guidelines 7/2020 in deutscher Sprache
  https://www.baden-wuerttemberg.datenschutz.de/faq-zur-abgrenzung-der-verantwortlichkeiten-und-des-begriffs

Transparenz

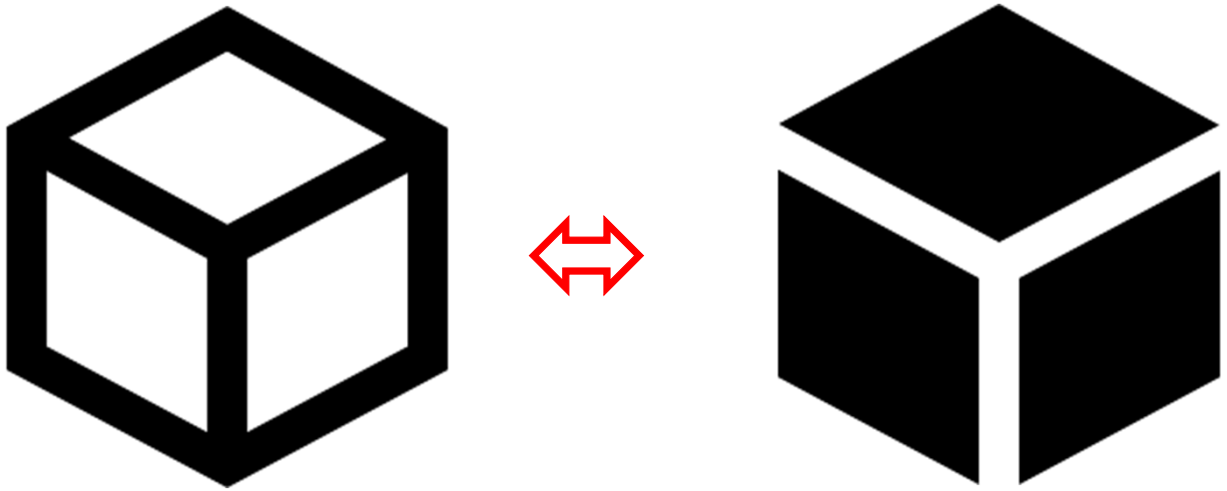
mittels Layered Policies

und

Transparency enhancing Technologies (TETs)

Vorab: zum Begriff Transparenz

Datenschützer ⇔ u.a. Kryptografen



In der Informatik (vor allem im US-Raum) wird Transparenz oft genau gegenteilig verstanden, nämlich als “Unsichtbarkeit” von Systemen und Prozessen um den Nutzer nicht mit Details zu belästigen

Warum Transparenz? Aus Sicht des Datenschutzrechts

- Nach DSGVO muss personenbezogene Datenverarbeitung **nachvollziehbar** sein, insbesondere in Bezug darauf,
  - welche Daten erhoben werden und in welchem Umfang
  - auf welche Art und Weise Information verarbeitet wird
  - zu welchen Zwecken und von wem

  - ➢ Transparenz ist zwingende Vorbedingung, um Betroffenenrechte wirksam ausüben zu können (u.a. Berichtigung).
  - ➢ Transparenz ist gesetzliche Pflicht aus Art. 5(1)(a) und nicht lediglich ein optionaler Service
  - ➢ Sie ist für den gesamten Lebenszyklus zu gewährleisten

Was? Worüber ist aufzuklären?

- Art 13: Siehe Katalog im Gesetzestext (Identität, Zwecke, berechtigte Interessen, Empfänger, Betroffenenrechte,…)

- Art 14: Wie 13 zusätzlich Kategorien der verarbeiteten Daten und Herkunft der Daten

- Art 7 für Einwilligung
  - Einwilligungsersuchen muss **klar unterscheidbar** von anderen Erklärungen sein
  - Verständliche, leicht zugängliche Form, einfache Sprache
  - Informiertheit ist Wirksamkeitsvoraussetzung: Mindestinhalt = Zweck + Verantwortlicher + Widerrufsrecht

Wie?
Anforderung genereller transparenter Information und Kommunikation

Artikel 12

Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person

(1) Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen gemäß den Artikeln 13 und 14 und alle Mitteilungen gemäß den Artikeln 15 bis 22 und Artikel 34, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln; dies gilt insbesondere für Informationen, die sich speziell an Kinder richten. Die Übermittlung der Informationen erfolgt schriftlich oder in anderer Form, gegebenenfalls auch elektronisch. Falls von der betroffenen Person verlangt, kann die Information mündlich erteilt werden, sofern die Identität der betroffenen Person in anderer Form nachgewiesen wurde.

Für wen? Adressaten

- Bei der Beurteilung, ob hinreichende Transparenz gegeben ist, ist zumeist die Perspektive des Betroffenen ausschlaggebend:

  - Art. 12 (1) …Maßnahmen, um der betroffenen Person alle Informationen […], in präziser, transparenter, verständlicher und leicht zugänglicher Form in" einfacher Sprache zu übermitteln.

  - Weitergehende Dokumentation kann sich demgegenüber an interne und externe Experten (Aufsichtsbehörden) richten, und dürfen technischer verfasst sein Art. 30

Informiertheit des Betroffenen (Einwilligung)

Art. 4 Nr. 11 - zusammen mit Art. 7 DSGVO - erfordert für eine wirksame Einwilligung:

- Freiwilligkeit
- Bestimmtheit (für einen oder mehrere feste Zwecke)
- Informiertheit
- Eindeutige Willensbekundung des Betroffenen
- Jederzeitige Widerrufbarkeit

Nach Art. 7 Abs. 1 DSGVO muss der Verantwortliche die wirksame Einwilligung nachweisen können!

Informiertheit des Betroffenen (Einwilligung)

- **Information**
  - Welche Daten werden verarbeitet?
  - Wer verarbeitet die Daten?
  - Zu welchem Zweck?

Art. 7 Abs. 2 DSGVO: Ersuchen um Einwilligung muss bei einer schriftlichen Erklärung, die noch andere Sachverhalte betrifft,

  - in verständlicher und leicht zugänglicher Form
  - in einer klaren und einfachen Sprache
  - von anderen Sachverhalten klar unterscheidbar sein

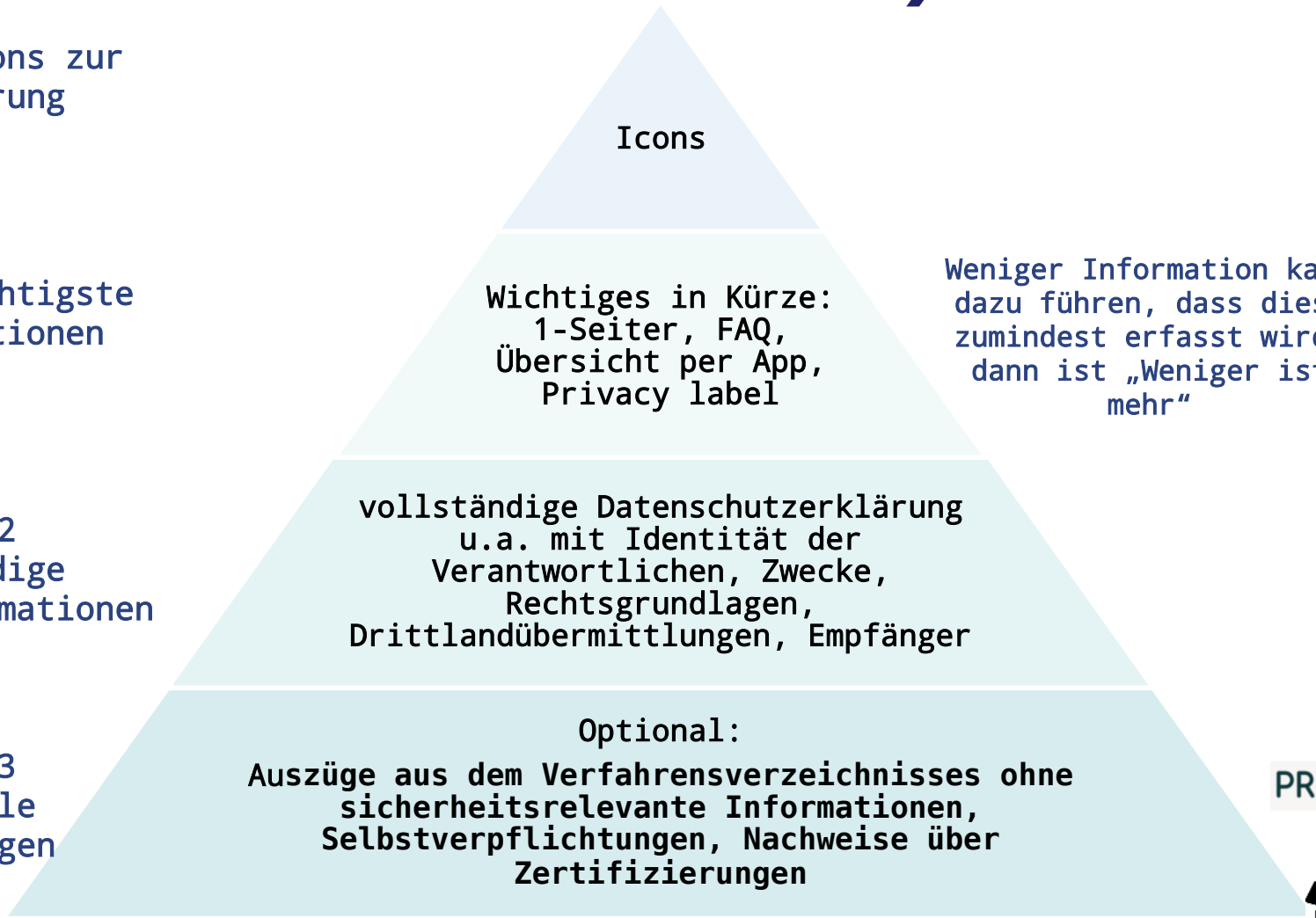
Layerd Policies

Ebene 0: Icons zur Orientierung

Ebene 1: wichtigste Kerinformationen

Ebene 2 Vollständige Pflicht-informationen

Ebene 3 Optionale Ergänzungen



Weniger Information kann dazu führen, dass diese zumindest erfasst wird, dann ist „Weniger ist mehr“

PRIMA

Transparenz im Internet of Things

- Problemstellung: Wie kann im Internet of Things die erforderliche Transparenz für alle hergestellt werden?

- Lösungsidee: Privacy Label
- Bewertungsmetrik für Datenschutzeigenschaften u.a. für Kaufentscheidungen
- Verständliche und bildliche Darstellung

- Folgeproblem: Beschaffung der Informationen?
  - Produktbeschreibungen
  - Pflichtangaben nach Data Act, Cyber-Resiliance Act u.a.
  - Hersteller / Importeure
  - Dokumentation der Einstellungsoptionen
  - Webtraffic-Analyse, Funktionen und Verhalten des Geräts
  - Firmware-Analyse

Figure 1: "Privacy facts" label for IoT devices.

Projekt Unboxing.IoT.Privacy, Bildquelle: A. Railean, Privacy&Us-Projekt

Transparenz und Auftragsvearbeitung im Internet of Things

- IoT-Geräte bedingen meist Datenverarbeitung bei Dritten, daher gilt
  - Sorgfältige Auswahl der Anbieter
  - Transparenz für andere Personen im Haushalt, Betrieb,…
    - Wer ist (mit-)verantwortlich? Was wird von wem zu welchen Zwecken wo verarbeitet? Informationsquelle?
- Data Act verpflichtend ab Sept. 2025
  - Ziel: Zugänglichkeit von Daten aus vernetzten Geräten für die Nutzer
  - Voraussetzung dafür: Information vor Anschaffung über Datenarten, Frequenz, Zugriffsmöglichkeit, durch Hersteller, Verkäufer und Dienstanbieter wird Pflicht, vgl. Art. 3-4 DA.

Zusammenfassung Transparenz

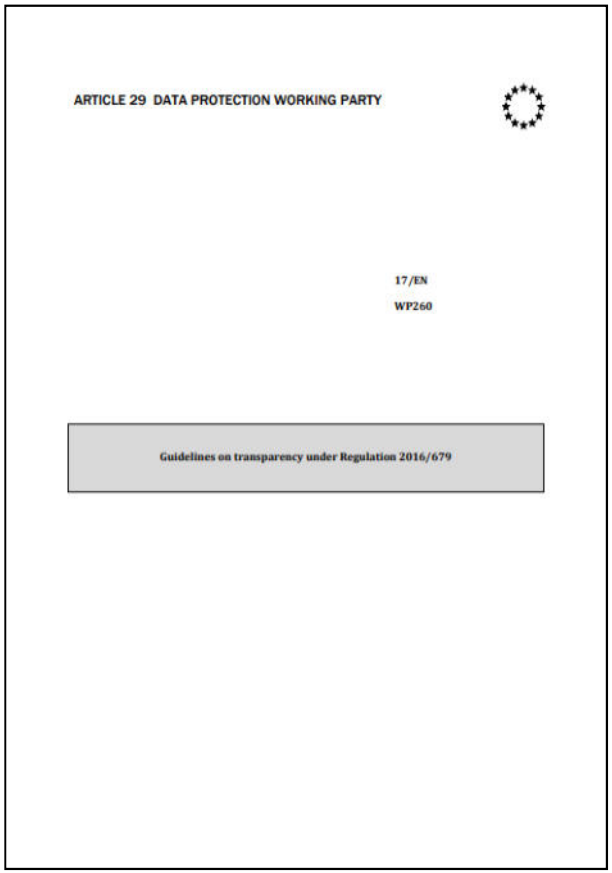
- Transparenz ist gesetzliche Pflicht, nicht UX-Option.
- Pflichtinformationen aus Art. 13/14 und Art. 7 müssen adressatengerecht vermittelt werden.
- Layered Policies, Icons, Labels oder Apps sind nur Mittel; sie ersetzen die Pflichtinformationen nicht.
- Im IoT und bei KI/komplexen Systemen ist Transparenz eine Gestaltungs- und keine reine Textaufgabe. Informationsbeschaffung, Dokumentation und verständliche Vermittlung sind Teil der Herausforderung für Verantwortliche.

Quellen zum Thema Transparenz und DSGVO

1. Verfassungsrang
   - Art. 8 EuGRCh – Fairnessprinzip

2. DSGVO
   - Art. 5 (1) (a)
   - Artt. 12 ff
   - Art. 15-22
   - Art. 34

3. Stellungnahmen:
   Art. 29 Datenschutzgruppe WP260
   (Bisher nur Englisch)


ARTICLE 29 DATA PROTECTION WORKING PARTY

17/EN
WP260

Guidelines on transparency under Regulation 2016/679

http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850

Herzlichen Dank für die gemeinsame Diskussion zum Thema

Kontakt:
Harald Zwingelberg
uld6@datenschutzzentrum.de
www.datenschutzzentrum.de
0431/988-1222

Vorlesungsfolien enthalten auf Ergebnissen der Datenschutz-Forschungsprojekten

AnoMed

PRIMA

TRUMAN

Gefördert durch:

Bundesministerium für Forschung, Technologie und Raumfahrt

Funded by the European Union

sowie für AnoMed (2022-2024):

Finanziert von der Europäischen Union
NextGenerationEU