

Warmlaufen für Artikel 25 DSGVO: Datenschutz by Design & by Default

Dr. h.c. Marit Hansen
Landesbeauftragte für Datenschutz Schleswig-Holstein
09.01.2024



Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Überblick

1. Wichtigkeit von „by Design“
2. Art. 25 im Gefüge der DSGVO
3. Abs. 1: „by Design“
4. Abs. 2: „by Default“
5. Entscheidungen
6. Ausblick
7. Links

Wichtigkeit von „by Design“

Erwägungsgrund 4 der DSGVO:

„The processing of personal data **should be designed** to serve mankind. [...]“

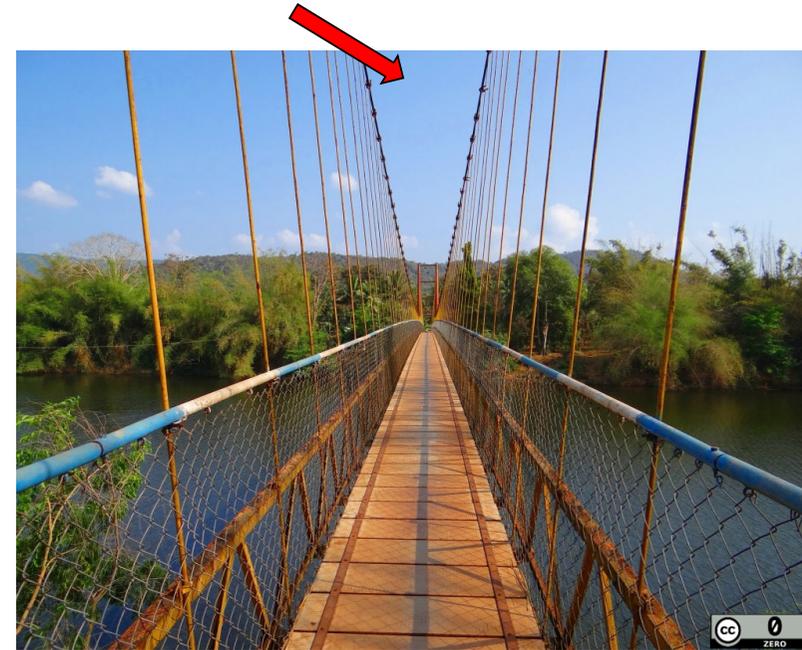
Überblick

1. Wichtigkeit von „by Design“
2. Art. 25 im Gefüge der DSGVO
3. Abs. 1: „by Design“
4. Abs. 2: „by Default“
5. Entscheidungen
6. Ausblick
7. Links

Wichtigkeit von „by Design“



Unsicherer Zustand, eigene Maßnahmen nötig



Vertrauenswürdigkeit durch sichtbare Maßnahmen und Überprüfbarkeit

Überblick

1. Wichtigkeit von „by Design“
2. Art. 25 im Gefüge der DSGVO
3. Abs. 1: „by Design“
4. Abs. 2: „by Default“
5. Entscheidungen
6. Ausblick
7. Links

Art. 25 DSGVO – „by design and by default“

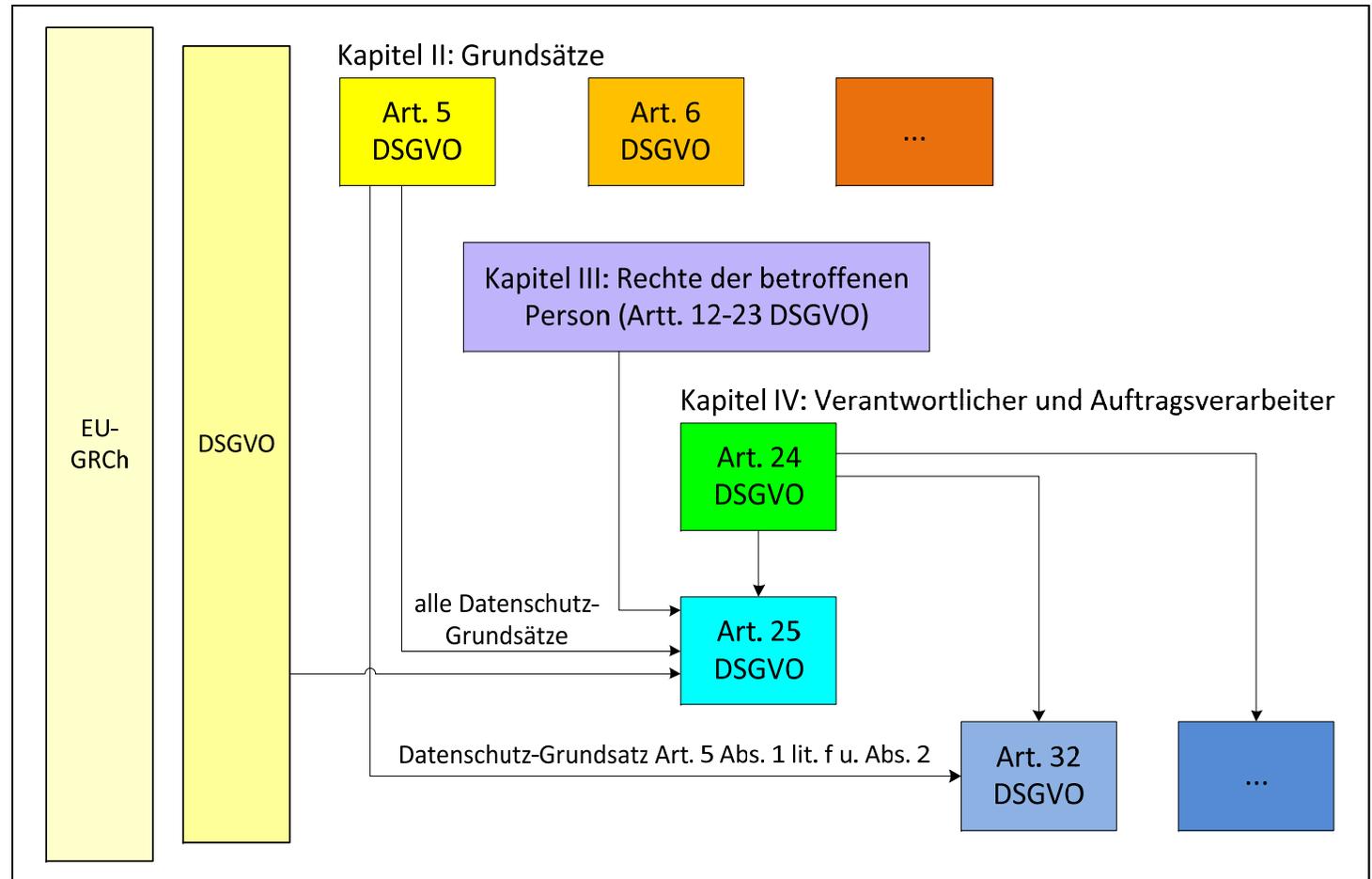
- [DE] Artikel 25: Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen
- [FR] Article 25: Protection des données dès la conception et protection des données par défaut
- [ES] Artículo 25: Protección de datos desde el diseño y por defecto
- [SV] Artikel 25: Inbyggd dataskydd och dataskydd som standard
- [NL] Artikel 25: Gegevensbescherming door ontwerp en door standaardinstellingen

„Technik“ nur in der deutschen Fassung;
d.h. breiter zu verstehen

Art. 25 im Gefüge der DSGVO

Überblick

1. Wichtigkeit von „by Design“
2. Art. 25 im Gefüge der DSGVO
3. Abs. 1: „by Design“
4. Abs. 2: „by Default“
5. Entscheidungen
6. Ausblick
7. Links



Überblick

1. Wichtigkeit von „by Design“
2. Art. 25 im Gefüge der DSGVO
3. Abs. 1: „by Design“
4. Abs. 2: „by Default“
5. Entscheidungen
6. Ausblick
7. Links

Art. 25 im Gefüge der DSGVO

Art. 5 DSGVO

– immer zu erfüllen bei **personenbezogenen Daten**

Oberthema: Fairness

Abs. 1:

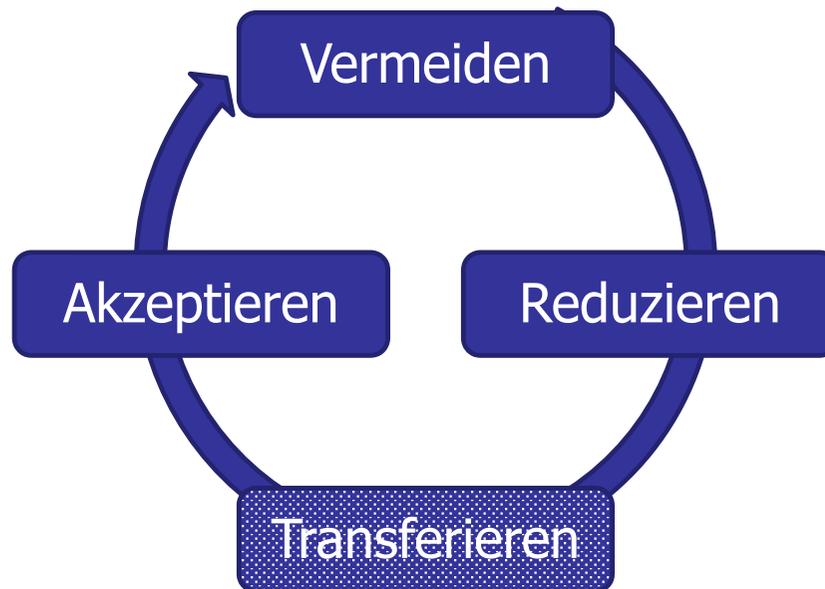
- a) Rechtmäßigkeit, Verarbeitung nach **Treu und Glauben**, Transparenz
- b) **Zweckbindung**
- c) **Datenminimierung**
- d) **Richtigkeit**
- e) **Speicherbegrenzung**
- f) **Integrität und Vertraulichkeit (Datensicherheit)**

Abs. 2: **Rechenschaftspflicht**

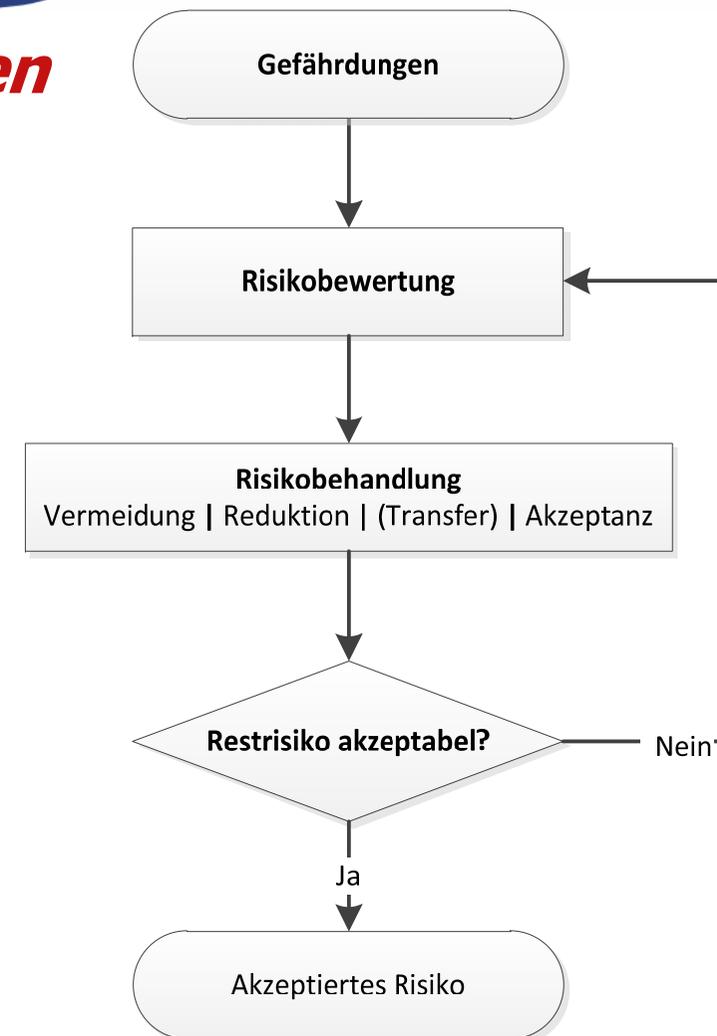
Überblick

1. Wichtigkeit von „by Design“
2. Art. 25 im Gefüge der DSGVO
3. Abs. 1: „by Design“
4. Abs. 2: „by Default“
5. Entscheidungen
6. Ausblick
7. Links

Nicht nur Art. 25: Strategien der Risikobehandlung



- Wichtigkeit von technischen und organisatorischen Maßnahmen (TOM)
- Der Verantwortliche ist und **bleibt verantwortlich**. Insoweit kein Transfer!

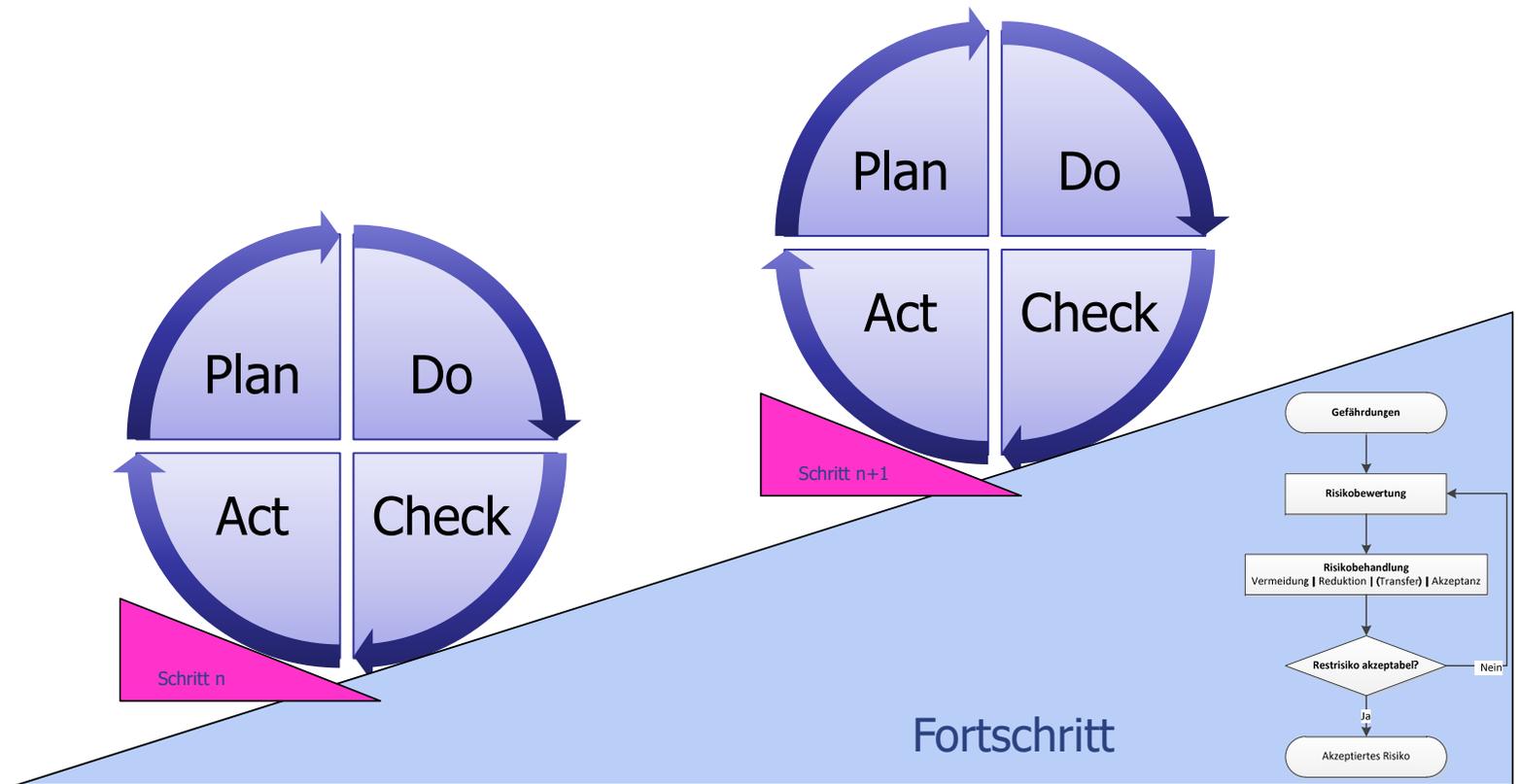


ISO/IEC 27005, <https://www.bsi.bund.de/dok/10990674>

PDCA-Zyklen über die Zeit, auch für Risikobehandlung

Überblick

1. Wichtigkeit von „by Design“
2. Art. 25 im Gefüge der DSGVO
3. Abs. 1: „by Design“
4. Abs. 2: „by Default“
5. Entscheidungen
6. Ausblick
7. Links



Überblick

1. Wichtigkeit von „by Design“
2. Art. 25 im Gefüge der DSGVO
3. Abs. 1: „by Design“
4. Abs. 2: „by Default“
5. Entscheidungen
6. Ausblick
7. Links

Absatz 1: „by Design“

Artikel 25 Datenschutz durch Technikgestaltung [...]

(1) 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 –,

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.

Unter welchen Bedingungen?

Wer?

Wann?

Was ist zu tun?

Was konkret?
Mit welchem Ziel?

Überblick

1. Wichtigkeit von „by Design“
2. Art. 25 im Gefüge der DSGVO
3. Abs. 1: „by Design“
4. Abs. 2: „by Default“
5. Entscheidungen
6. Ausblick
7. Links

Absatz 1: „by Design“ – Erwägungsgrund 78

- Nachweis durch **interne Strategien & t+o Maßnahmen**, u.a.
 - Datenminimierung
 - Frühestmögliche Pseudonymisierung
 - Transparenz in Bezug auf Funktionen+Verarbeitung
 - Ermöglichung der Überwachung der Verarbeitung durch die betroffenen Personen
 - Ermöglichung für Sicherheitsfunktionen „on top“ durch Verantwortlichen
- **Ermutigung für Hersteller**
- Berücksichtigung in **öffentlichen Ausschreibungen**

Überblick

1. Wichtigkeit von „by Design“
2. Art. 25 im Gefüge der DSGVO
3. Abs. 1: „by Design“
4. Abs. 2: „by Default“
5. Entscheidungen
6. Ausblick
7. Links

Wie genau? – Bsp. Videoüberwachung

Beispiel **Datenminimierung** bei Bildaufnahmen/Videoüberwachung:
Wann, welche Daten, wie auswertbar ... wirklich erforderlich?



Foto: Markus Hansen

**Achtung: Unterschied
Datenschutz / Privatheitsschutz**

Überblick

1. Wichtigkeit von „by Design“
2. Art. 25 im Gefüge der DSGVO
3. Abs. 1: „by Design“
4. Abs. 2: „by Default“
5. Entscheidungen
6. Ausblick
7. Links

Wie genau? – Bsp. Videoüberwachung

Sichere und datenschutzfreundliche Gestaltung

1. Rechtsgrundlage
2. Auswahl, Installation und Betrieb von Videoüberwachungs-systemen: sichere (Art. 32 DSGVO) und datenschutzfreundliche (Art. 25 DSGVO) Gestaltung
 - Inwieweit kann eine Videoüberwachung **zeitlich eingeschränkt** werden und welche **Bereiche der Überwachung können ausgeblendet** oder **verpixelt** werden?
 - „Verlängertes Auge“ oder **Aufzeichnung** (wie? wie lange?)?
 - „Eingebauter Datenschutz“ schon bei der **Beschaffung**: **Nicht benötigte Funktionalität** (z. B. **freie Schwenkbarkeit, umfassende Überwachung per Dome-Kamera, Zoomfähigkeit, Funkübertragung, Internetveröffentlichung, Audioaufnahme**) sollte von der beschafften Technik **nicht unterstützt** oder zumindest bei der Inbetriebnahme **deaktiviert** werden.

Überblick

1. Wichtigkeit von „by Design“
2. Art. 25 im Gefüge der DSGVO
3. Abs. 1: „by Design“
4. Abs. 2: „by Default“
5. Entscheidungen
6. Ausblick
7. Links

Bsp. Transparenz-Unterstützung

Datenschutz-Steckbrief

E-Mail-Newsletter

Wir verarbeiten personenbezogene Daten zu dem **Zweck**,

- um Newsletter per E-Mail zu verschiedenen Themenbereichen zu versenden.

Wir verarbeiten personenbezogene Daten von folgenden betroffenen Personen (**Betroffenkategorien**):

- Personen, die den Newsletter abonniert haben
- Personen, die den Newsletter versenden

Wir verarbeiten folgende personenbezogene Daten (**Datenkategorien**):

- E-Mail-Adresse
- Inhalte des Newsletters (öffentlich; ggf. personenbezogene Informationen von Absenderseite)

Personenbezogene Daten der Personen, die den Newsletter abonniert haben, werden von uns **nicht weitergegeben**.

Personenbezogene Daten werden nicht gesammelt und ausgewertet, um Persönlichkeits-, Verhaltens-, Bewegungsprofile o. Ä. zu erstellen, d. h. es findet **kein Profiling** statt.

Personenbezogene Daten werden bei uns in einem elektronischen Newslettersystem **gespeichert**, in dem sich die Interessierten **selbstständig eintragen** und auch wieder **austragen** können. Auf diese Möglichkeit wird im Abspann jedes Newsletters hingewiesen.

Im Newslettersystem werden keine versendeten Newsletter **gespeichert**, d. h. es findet keine Archivierung der Nachrichteninhalte statt.

Die rechtliche Grundlage:

- Einwilligung (§ 2 Abs. 1 Nr. 1 Datenschutzordnung)
- Die Einwilligung wird in Form eines **Double-Opt-In**-Verfahrens abgegeben.

Beispiel:
elektronisches Newslettersystem

Beispiel:
Double-Opt-In



Achtung
Klingelkamera

Informationen zu **Ihren Rechten** erhalten Sie auf unserer Webseite:
www.datenschutzzentrum.de/datenschutzerklaerung

Name und Kontaktdaten des Verantwortlichen:

Unabhängiges Landeszentrum für Datenschutz
Holstenstraße 98
24103 Kiel
mail@datenschutzzentrum.de
0431/ 988 1200

Kontaktdaten des Datenschutzbeauftragten:

bdsb@datenschutzzentrum.de
0431/ 988 1280

Zweck und Rechtsgrundlage der Datenverarbeitung:

Einlasskontrolle im Rahmen der Wahrnehmung des Hausrechts gemäß § 14 Abs. 1 Nr. 2 Landesdatenschutzgesetz (LDStG)

Funktionsweise der Kamera und Gegengsprechfunktion:

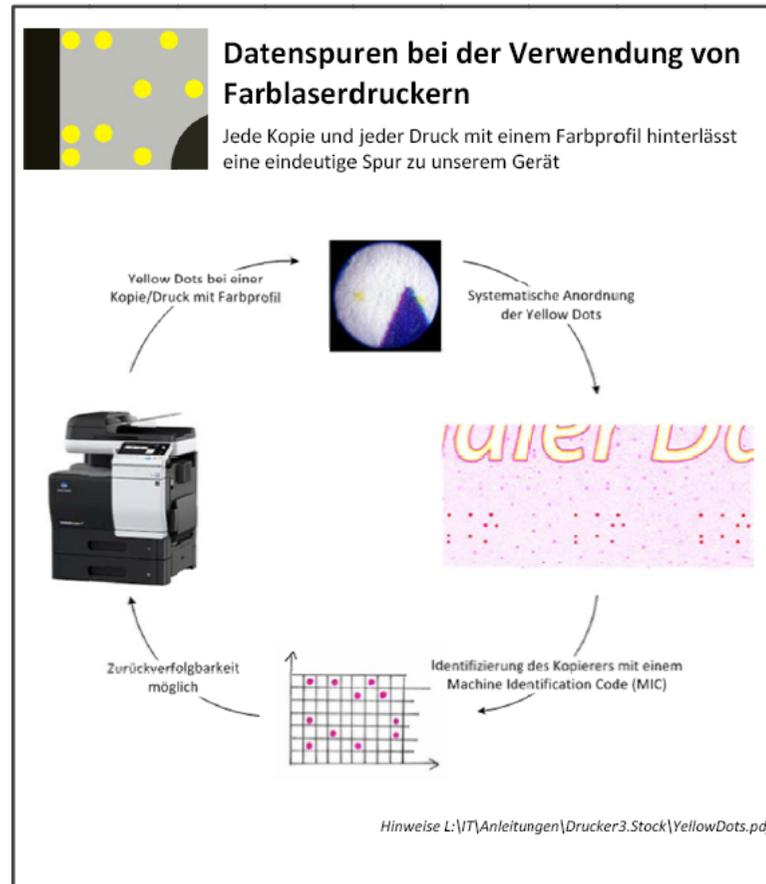
Erst beim Klingeln werden die Kamera und die Gegengsprechfunktion kurzzeitig angeschaltet. Der Erfassungsbereich der Kamera ist dann auf den unmittelbaren Eingangsbereich beschränkt. Eine Speicherung der Daten erfolgt nicht. Ansonsten sind die Kamera und die Gegengsprechfunktion ausgeschaltet.

Tätigkeitsbericht
2019 des ULD S-H,
Tz. 6.1.4:
<https://uldsh.de/tb37>

Überblick

1. Wichtigkeit von „by Design“
2. Art. 25 im Gefüge der DSGVO
3. Abs. 1: „by Design“
4. Abs. 2: „by Default“
5. Entscheidungen
6. Ausblick
7. Links

Bsp. Transparenz für Risiken



Hinweis auf „Yellow dots“ am Farbkopierer

Tätigkeitsbericht
2019 des ULD S-H,
Tz. 10.4:
<https://uldsh.de/tb37>

ULD (2019): Report „Vorsicht: Yellow Dots! Versteckte Informationen in Farbkopien“,
<https://www.datenschutzzentrum.de/artikel/1274-Yellow-Dots.html>

Überblick

1. Wichtigkeit von „by Design“
2. Art. 25 im Gefüge der DSGVO
3. Abs. 1: „by Design“
4. Abs. 2: „by Default“
5. Entscheidungen
6. Ausblick
7. Links

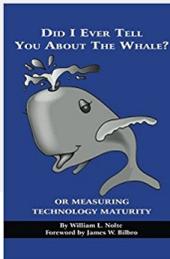
„by Design“ & Privacy-Enhancing Technologies

“The use of PETs can help to design information and communication systems and services in a way that **minimises the collection and use of personal data and facilitate compliance with data protection rules.** The use of PETs should result in making breaches of certain data protection rules more difficult and/or helping to detect them.”

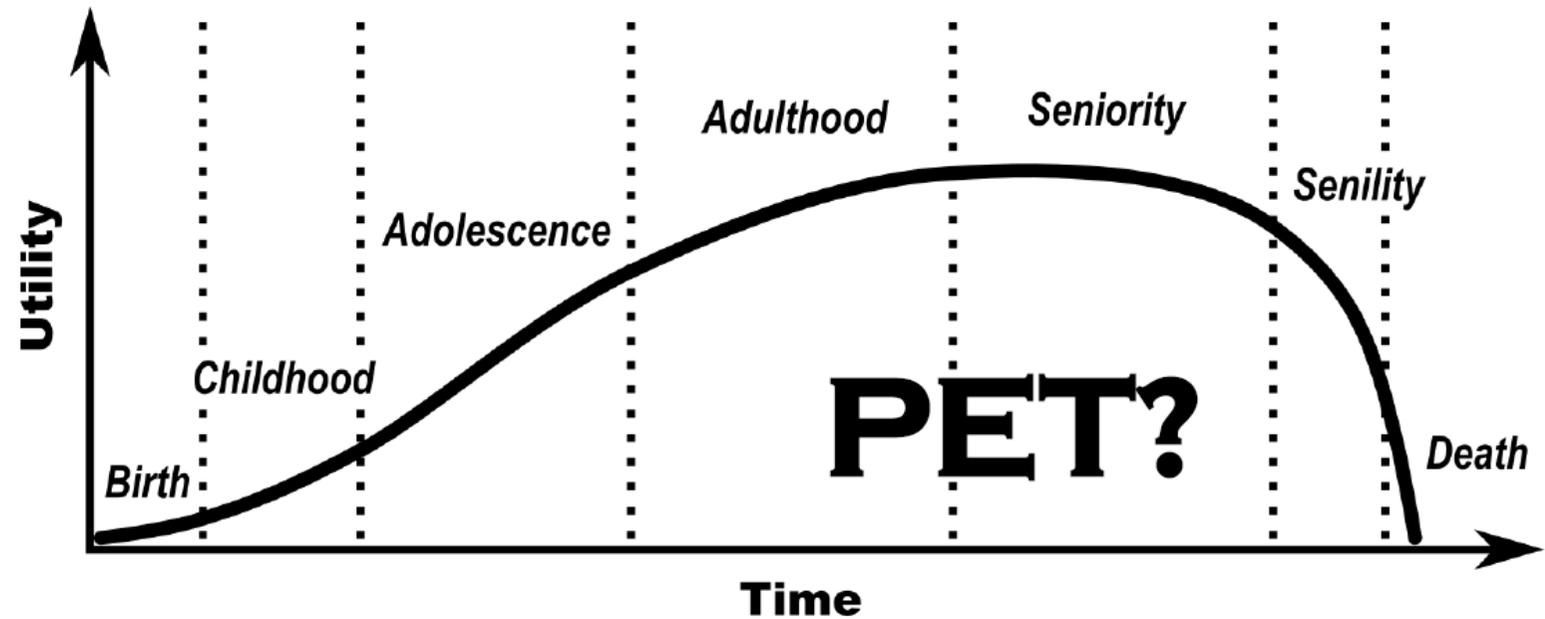
European Commission, MEMO/07/159

Überblick

1. Wichtigkeit von „by Design“
2. Art. 25 im Gefüge der DSGVO
3. Abs. 1: „by Design“
4. Abs. 2: „by Default“
5. Entscheidungen
6. Ausblick
7. Links



„by Design“ & Privacy-Enhancing Technologies



Beispiele: MD5, Windows XP, ...

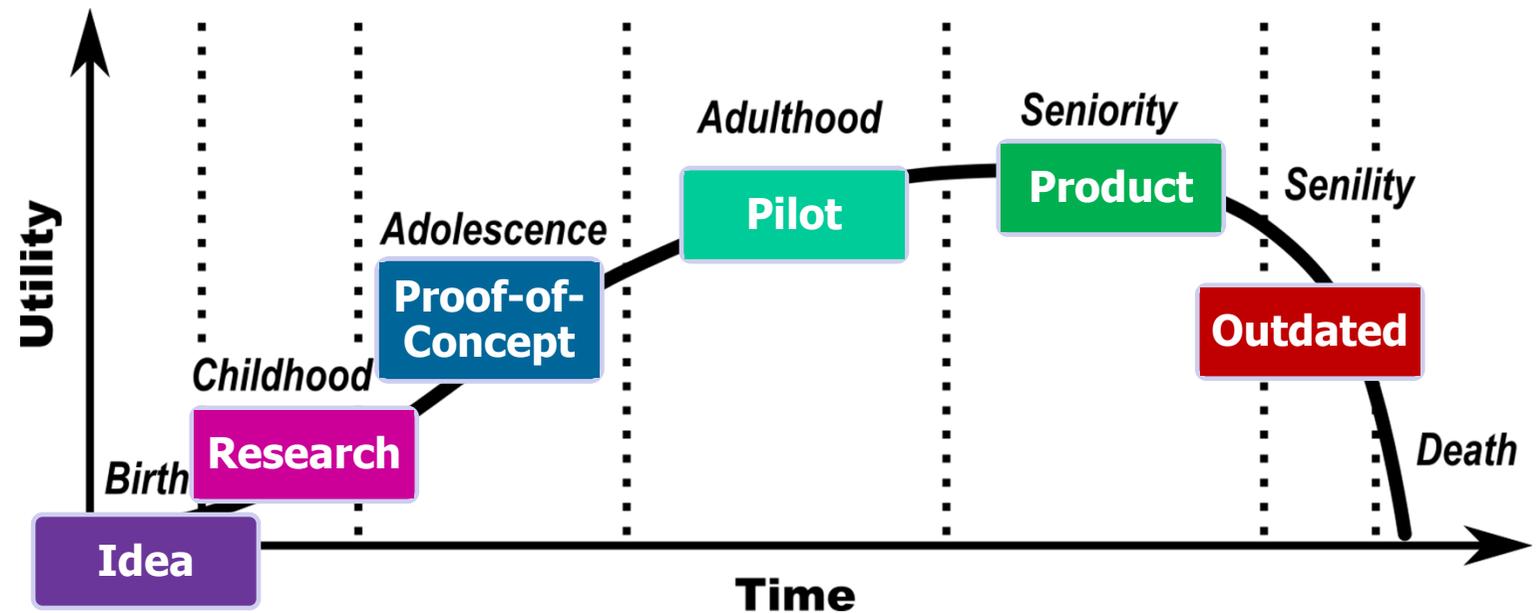
Überblick

1. Wichtigkeit von „by Design“
2. Art. 25 im Gefüge der DSGVO
3. Abs. 1: „by Design“
4. Abs. 2: „by Default“
5. Entscheidungen
6. Ausblick
7. Links



„by Design“ & Privacy-Enhancing Technologies

Reifegrad, „Stand der Technik“?



Überblick

1. Wichtigkeit von „by Design“
2. Art. 25 im Gefüge der DSGVO
3. Abs. 1: „by Design“
4. Abs. 2: „by Default“
5. Entscheidungen
6. Ausblick
7. Links

„by Design“ & Privacy-Enhancing Technologies

- **PETs** können zur Umsetzung des Art. 25 DSGVO beitragen
- Reifegrad wesentlich:
dabei **Wirksamkeit und Nebenwirkungen** im Blick haben
- Bezug zu **PETs i.S.v. Tools für Selbstdatenschutz** der Nutzenden:
 - Der Verantwortliche ist verantwortlich für das Treffen der technischen und organisatorischen Maßnahmen – Eigeneinsatz der Nutzenden darf **nicht vorausgesetzt** werden
 - Achtung bei Gestaltung **„no service for users with PETs“**: Ausschluss von Gruppen von Nutzenden; Beispiel (2012):
<https://www.golem.de/news/tor-eu-gibt-blockade-von-anonymisierungsservern-auf-1203-90766.html>

Überblick

1. Wichtigkeit von „by Design“
2. Art. 25 im Gefüge der DSGVO
3. Abs. 1: „by Design“
4. Abs. 2: „by Default“
5. Entscheidungen
6. Ausblick
7. Links



Überblick

1. Wichtigkeit von „by Design“
2. Art. 25 im Gefüge der DSGVO
3. Abs. 1: „by Design“
4. Abs. 2: „by Default“
5. Entscheidungen
6. Ausblick
7. Links



Überblick

1. Wichtigkeit von „by Design“
2. Art. 25 im Gefüge der DSGVO
3. Abs. 1: „by Design“
4. Abs. 2: „by Default“
5. Entscheidungen
6. Ausblick
7. Links

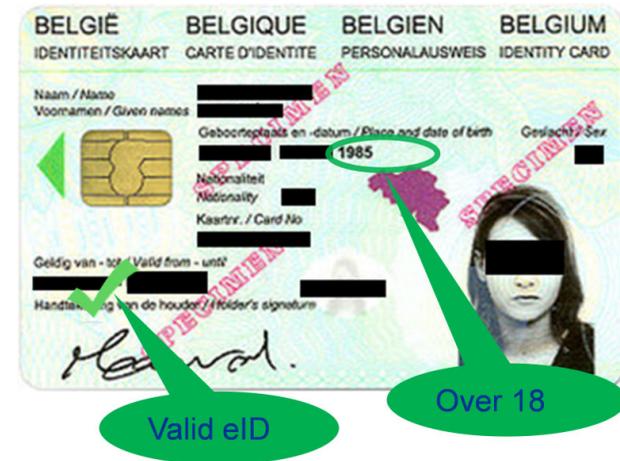
Zu bedenken: Infrastruktur-Charakter

Beispiel **Datenminimierung** bei Berechtigungsnachweisen:
Welche Daten sind wirklich erforderlich?

Aber: abhängig von Gestaltung verfügbarer **Infrastrukturen**



Symbolbild (kein echter belgischer Ausweis)



Überblick

1. Wichtigkeit von „by Design“
2. Art. 25 im Gefüge der DSGVO
3. Abs. 1: „by Design“
4. Abs. 2: „by Default“
5. Entscheidungen
6. Ausblick
7. Links

Absatz 2 – noch einmal der Blick in Absatz 1

Artikel 25 Datenschutz durch Technikgestaltung [...]

(1) 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 –,

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.

Unter welchen Bedingungen?

Wer?

Wann?

Was ist zu tun?

Was konkret?
Mit welchem Ziel?

Überblick

1. Wichtigkeit von „by Design“
2. Art. 25 im Gefüge der DSGVO
3. Abs. 1: „by Design“
4. Abs. 2: „by Default“
5. Entscheidungen
6. Ausblick
7. Links

Absatz 2: „by Default“

Artikel 25 [...] durch datenschutzfreundliche Voreinstellungen

(2) Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.

Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit.

Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

Wer?
Was ist zu tun?

Was konkret?
Mit welchem Ziel?

Welche Kriterien?

Sonderfall
Social Media

Immer!

Unter welchen Bedingungen?

Überblick

1. Wichtigkeit von „by Design“
2. Art. 25 im Gefüge der DSGVO
3. Abs. 1: „by Design“
4. Abs. 2: „by Default“
5. Entscheidungen
6. Ausblick
7. Links

Was ist gemeint mit „by Default“?

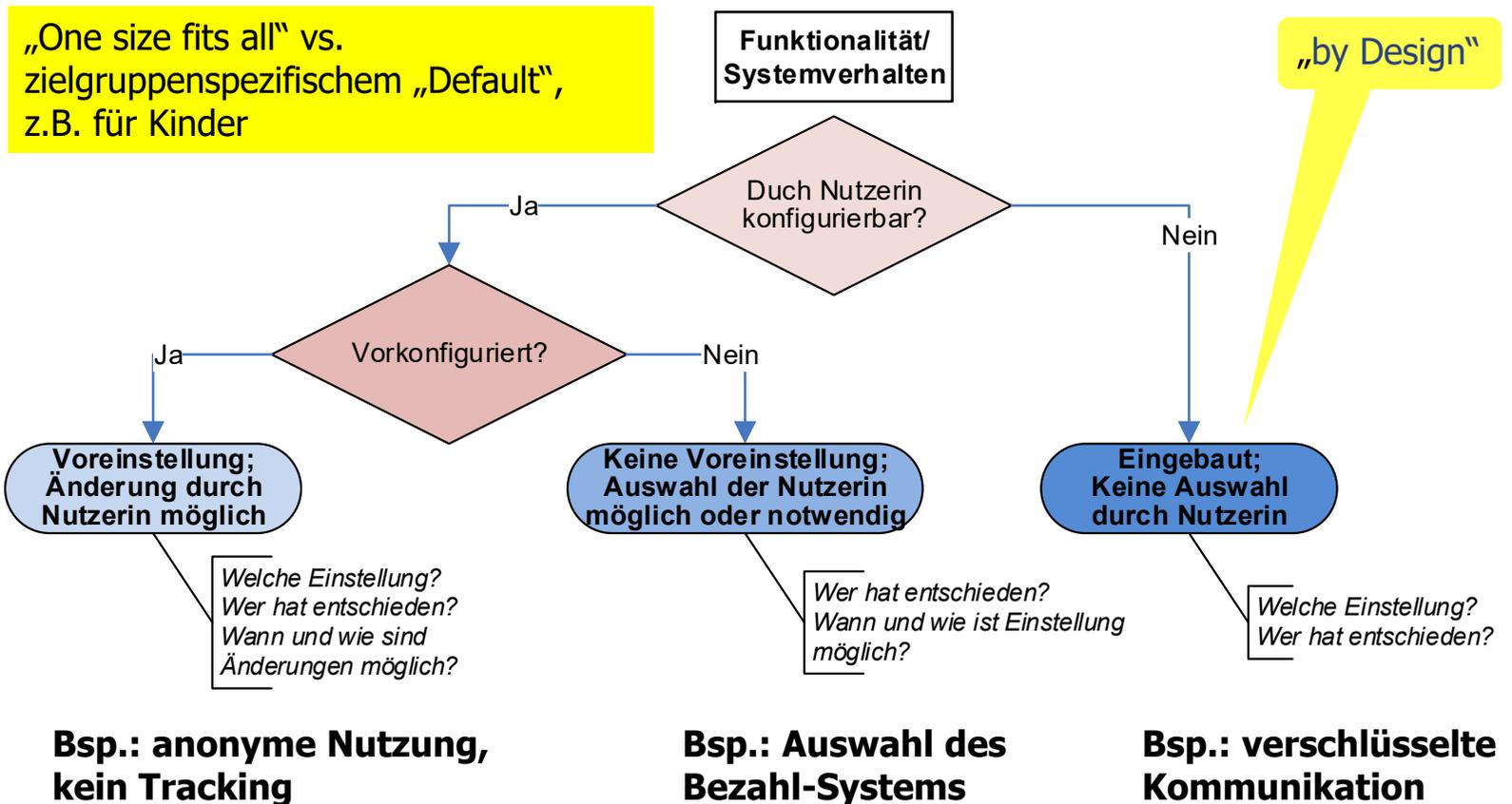
- **Startpunkt** „Datenschutz“
- **„durch Voreinstellung“:**

*„Entscheidungen über Konfigurationswerte oder Verarbeitungsoptionen, die in einem Verarbeitungssystem eingestellt oder vorgeschrieben sind“
(EDSA, Leitlinien 4/2019, Rn. 41)*

Überblick

1. Wichtigkeit von „by Design“
2. Art. 25 im Gefüge der DSGVO
3. Abs. 1: „by Design“
4. Abs. 2: „by Default“
5. Entscheidungen
6. Ausblick
7. Links

Absatz 2: „by Default“ – 3 Fälle



Art. 25 Abs. 2 DSGVO auch relevant bzgl. Deceptive Design

Überblick

1. Wichtigkeit von „by Design“
2. Art. 25 im Gefüge der DSGVO
3. Abs. 1: „by Design“
4. Abs. 2: „by Default“
5. Entscheidungen
6. Ausblick
7. Links

- Deceptive Design
- Addictive Design



 Bild: Gerd Altmann via Pixabay



 Bild: rawpixel via Pixabay

Überblick

1. Wichtigkeit von „by Design“
2. Art. 25 im Gefüge der DSGVO
3. Abs. 1: „by Design“
4. Abs. 2: „by Default“
5. Entscheidungen
6. Ausblick
7. Links

Jeweils ca. 1/3

- Fehlende Rechtsgrundlage
- Verletzung der Betroffenenrechte
- Sicherheit der Verarbeitung

Oft **mehrere verletzte Vorschriften** der DSGVO genannt

Entscheidungen generell

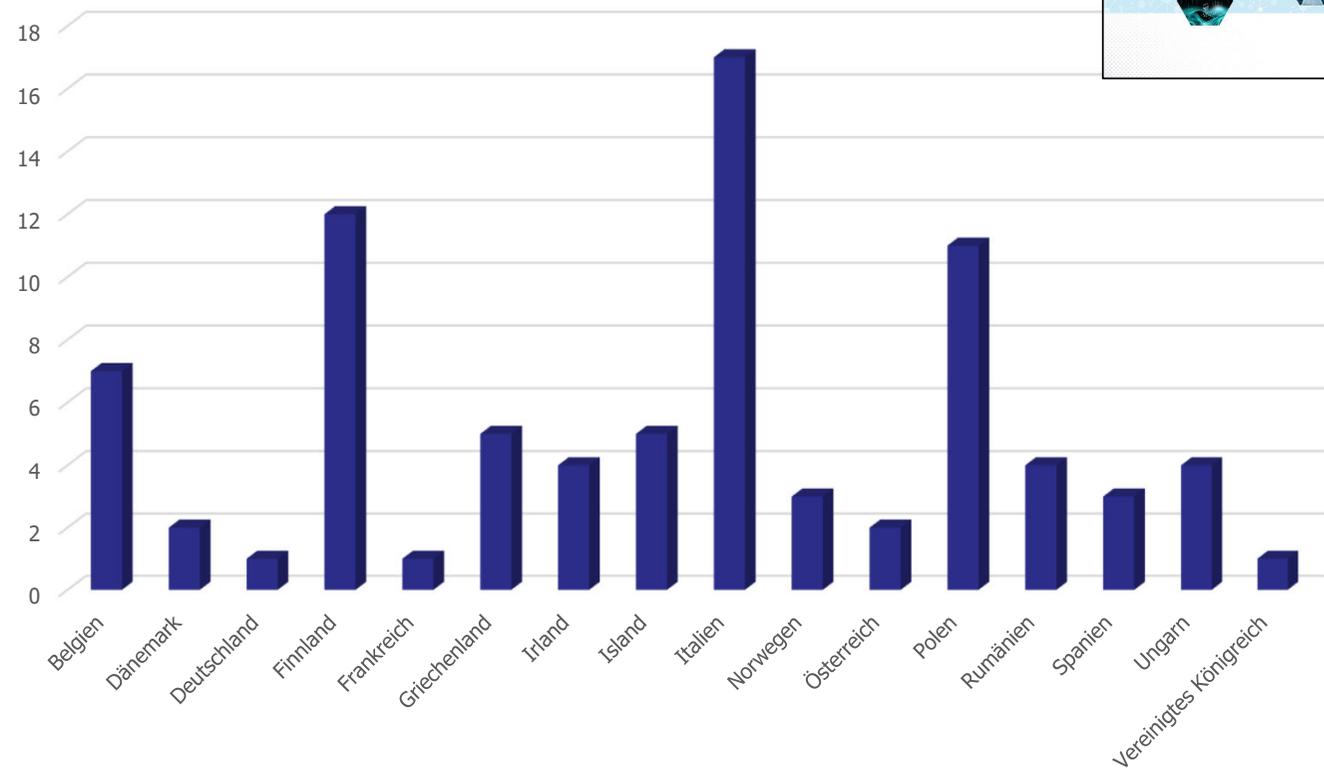


Überblick

1. Wichtigkeit von „by Design“
2. Art. 25 im Gefüge der DSGVO
3. Abs. 1: „by Design“
4. Abs. 2: „by Default“
5. Entscheidungen
6. Ausblick
7. Links

Entscheidungen

Art. 25-Entscheidungen 2018-2023 (FPF)

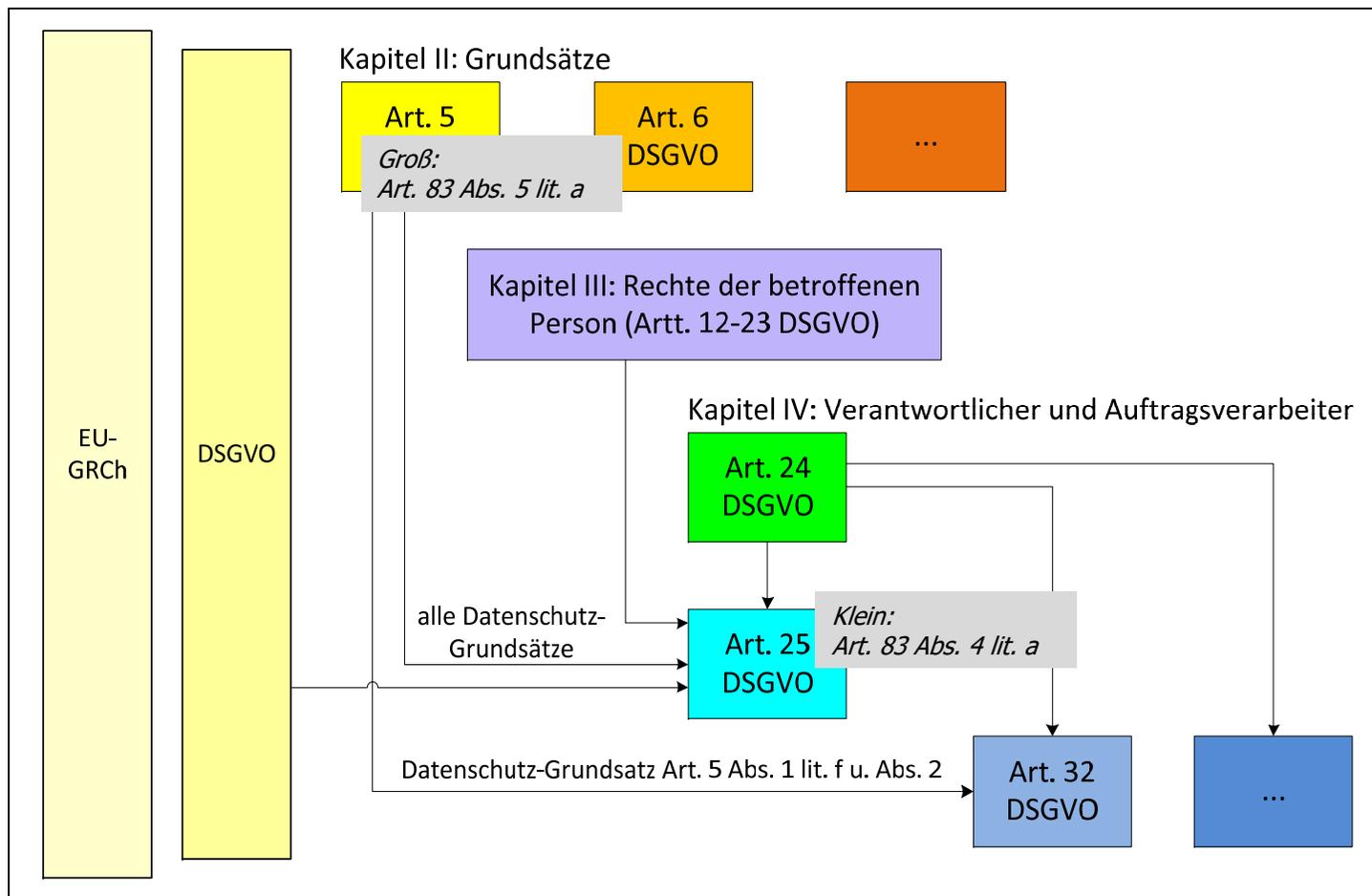


<https://fpf.org/wp-content/uploads/2023/05/FPF-Article-25-GDPR-A4-FINAL-Digital.pdf>

„Großer“ oder „kleiner“ Bußgeldrahmen?

Überblick

1. Wichtigkeit von „by Design“
2. Art. 25 im Gefüge der DSGVO
3. Abs. 1: „by Design“
4. Abs. 2: „by Default“
5. Entscheidungen
6. Ausblick
7. Links



Überblick

1. Wichtigkeit von „by Design“
2. Art. 25 im Gefüge der DSGVO
3. Abs. 1: „by Design“
4. Abs. 2: „by Default“
5. Entscheidungen
6. Ausblick
7. Links

Entscheidungen

- „Deutsche Wohnen“: **14,5 Mio € Bußgeld** (nicht rechtskräftig) – LG Berlin, 18.02.2021 – 526 OWi LG
// KG, 06.12.2021 – 3 Ws 250/21 – 161 AR 84/21
- DPC Ireland: Facebook „Data Scraping“, 25.11.2022 – **265 Mio € Bußgeld**
// Schadenersatz zB LG Bonn, Urt. v. 7.6.2023, Az. 13 O 126/22
- DPC Inquiry Reference: IN-21-9-1, In the matter of TikTok Technology Limited [...], 01.09.2023 – **345 Mio € Bußgeld**

Quellen:

<https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-in-facebook-data-scraping-inquiry>

https://edpb.europa.eu/system/files/2023-09/final_decision_tiktok_in-21-9-1_-_redacted_8_september_2023.pdf

Überblick

1. Wichtigkeit von „by Design“
2. Art. 25 im Gefüge der DSGVO
3. Abs. 1: „by Design“
4. Abs. 2: „by Default“
5. Entscheidungen
6. Ausblick
7. Links

Ausblick

- Art. 25 Abs. 3 DSGVO: **Zertifizierung** „ein Faktor“ (anders als für Art. 32 DSGVO: keine CoC)
- Zunahme an Art. 25-Entscheidungen, weitere Konkretisierungen, klarere Sicht auf „**Was kann, was muss?**“
- **Standardisierung**: EN 17529:2022: „**Datenschutz und Schutz der Privatsphäre durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen**“ sowie CEN/CLC/TR 17919:2023 „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen - ... Videoüberwachungsindustrie ...“
- Empfehlung: **Warmlaufen** = eigene Systeme prüfen, ggf. nachbessern

Materialien

Überblick

1. Wichtigkeit von „by Design“
2. Art. 25 im Gefüge der DSGVO
3. Abs. 1: „by Design“
4. Abs. 2: „by Default“
5. Entscheidungen
6. Ausblick
7. Links

- Datatilsynet: Software Development with Data Protection by Design and by Default, 2017, <https://www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/data-protection-by-design-and-by-default/>
- DSK: SDM V3.0, 2022, <https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/>
- EDSA: Leitlinien 4/2019 zu Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, V2.0, 2020, https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_de.pdf
- EDSA: Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them, V2.0, 2023, https://edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf
- ENISA: Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies, 2016, <https://www.enisa.europa.eu/publications/pets>
- Future of Privacy Forum: Unlocking Data Protection By Design & By Default: Lessons from the Enforcement of Article 25 GDPR, 2023, <https://fpf.org/resource/new-fpf-report-unlocking-data-protection-by-design-and-by-default-lessons-from-the-enforcement-of-article-25-gdpr/>
- Hansen/Jensen/Rost: Protection Goals for Privacy Engineering, IWPE, 2015, <https://ieeexplore.ieee.org/ielx7/7160794/7163193/07163220.pdf>
- Hoepman: Privacy Design Strategies, 2018, <https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf>
- Veale/Binns/Ausloos: When Data Protection by Design and Data Subject Rights Clash, in: IDPL 8 (2) 2018, 105, <https://doi.org/10.1093/idpl/ipy002>