VORLESUNG DATENSCHUTZ

SOMMERSEMESTER 2024

Durchführung:

Benjamin Bremert und

Beschäftigte des Unabhängigen Landeszentrums

für Datenschutz Schleswig-Holstein (ULD), Kiel

Ansprechpartner: Benjamin Bremert <benjamin@bremert.de>

Rechtsauffassungen sind solche der jeweiligen Referent:innen.

Plattform Privatheit

Datenschutz und Technik III
– Datenschutzfördernde Technik –

CAU-Vorlesung, 06.05.2024

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

Hinweis:
Rechtsauffassungen sind solche der jeweiligen Referent:innen.

Überblick

1. Datenschutz ↔ Informationssicherheit
2. Privacy-Enhancing Technologies
3. Gewährleistungsziele im SDM
4. Art. 25 DSGVO
5. Abs. 1: „by Design“
6. Abs. 2: „by Default“

Machtgefälle zwischen Individuen und Organisationen ⇨ Datenschutz nötig

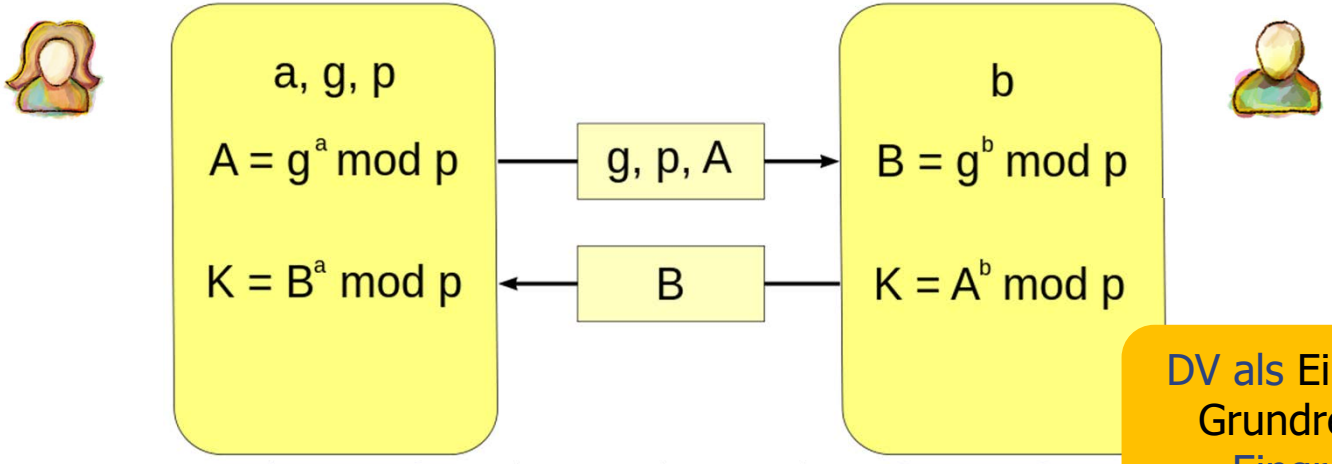
Wichtig: Perspektive des Individuums

 Bild: beludise via Pixabay

Überblick

1. Datenschutz ↔ Informationssicherheit
2. Privacy-Enhancing Technologies
3. Gewährleistungsziele im SDM
4. Art. 25 DSGVO
5. Abs. 1: „by Design“
6. Abs. 2: „by Default“

Perpektive: Alice & Bob



DV als Eingriff in Grundrechte: „Eingreifer“

IT-Sicherheit: Der Angreifer ist Eve (oder Mallory).

Datenschutz: Der Angreifer ist Bob!
(Jedenfalls auch.)

Überblick

1. Datenschutz ↔ Informationssicherheit
2. Privacy-Enhancing Technologies
3. Gewährleistungsziele im SDM
4. Art. 25 DSGVO
5. Abs. 1: „by Design"
6. Abs. 2: „by Default"

Spannungsfeld Technik ↔ Datenschutz

- **Technik-Ziel:** Vermeidung von Redundanzen (und daraus resultierenden Fehlern) in Datenbanken
- **Naive Lösung:**
  eine weltweite Zentral-Datenbank für alle Informationen zu jeder Person
- **Probleme:**
  - Begehrlichkeiten von Marketing-Abteilungen, Arbeitgeber, Versicherungen, Kriminellen ...
  - Zentraler Angriffspunkt
  - Zugriffskontrolle
  - Änderungen in einem Bereich: unsichtbar für andere?
  - Einfluss des Betroffenen, wer was über ihn weiß?

Überblick

1. Datenschutz ↔ Informationssicherheit
2. Privacy-Enhancing Technologies
3. Gewährleistungsziele im SDM
4. Art. 25 DSGVO
5. Abs. 1: „by Design"
6. Abs. 2: „by Default"

Spannungsfeld Technik ↔ Datenschutz

- **Technik-Ziel:** mehrfach verwendbare Applikationen
- **Naive Lösung:**
  umfassende Digitalisierung, kontextübergreifende Identifikatoren, Interoperabilität und Offenheit für vielseitige Nutzungsmöglichkeiten
- **Probleme:**
  - Begehrlichkeiten …
  - Unkontrollierte und unkontrollierbare Verkettbarkeit
  - „Function Creep"; Aufweichung einer Zweckbindung
  - Durchsetzbarkeit von Löschen und Sperren?

Überblick

1. Datenschutz ↔ Informationssicherheit
2. Privacy-Enhancing Technologies
3. Gewährleistungsziele im SDM
4. Art. 25 DSGVO
5. Abs. 1: „by Design"
6. Abs. 2: „by Default"

Wichtigkeit von „by Design"

Erwägungsgrund 4 der DSGVO:

„The processing of personal data should be designed to serve mankind. […]"

Überblick

1. Datenschutz ↔ Informationssicherheit
2. Privacy-Enhancing Technologies
3. Gewährleistungsziele im SDM
4. Art. 25 DSGVO
5. Abs. 1: „by Design"
6. Abs. 2: „by Default"

Wichtigkeit von „by Design"

Unsicherer Zustand, eigene Maßnahmen nötig

Vertrauenswürdigkeit durch sichtbare Maßnahmen und Überprüfbarkeit

Überblick

1. Datenschutz ↔ Informationssicherheit
2. Privacy-Enhancing Technologies
3. Gewährleistungsziele im SDM
4. Art. 25 DSGVO
5. Abs. 1: „by Design"
6. Abs. 2: „by Default"

Seit 1995: „Datenschutz durch Technik"

- Schon früher Informatik-Publikationen, z.B. zum Einsatz von Kryptographie im Bereich von Anonymisierungstechnik
- Datenschutzbehörden Niederlande/Ontario (Canada): Privacy-Enhancing Technologies: The Path to Anonymity (1995),
  https://www.researchgate.net/publication/243777645_Privacy-Enhancing_Technologies_The_Path_to_Anonymity
- In Deutschland: Arbeiten zu
  - Systemdatenschutz
  - Selbstdatenschutz
  - Mehrseitiger Sicherheit

- Ann Cavoukian (Information and Privacy Commissioner Ontario): Privacy by Design – The 7 Foundational Principles (revised 2011),
  https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

Überblick

1. Datenschutz ↔ Informationssicherheit
2. Privacy-Enhancing Technologies
3. Gewährleistungsziele im SDM
4. Art. 25 DSGVO
5. Abs. 1: „by Design"
6. Abs. 2: „by Default"

Was sind Privacy-Enhancing Technologies?

"Privacy-Enhancing Technologies (PET)
are a coherent system of ICT measures
that protects privacy [...]
by eliminating or reducing personal data or
by preventing unnecessary and/or
undesired processing of personal data;
all without losing the functionality
of the data system."

Borking / Raab (2001)

Überblick

1. Datenschutz ↔ Informationssicherheit
2. Privacy-Enhancing Technologies
3. Gewährleistungsziele im SDM
4. Art. 25 DSGVO
5. Abs. 1: „by Design"
6. Abs. 2: „by Default"

Privacy-Enhancing Technologies – erweiterte Sicht

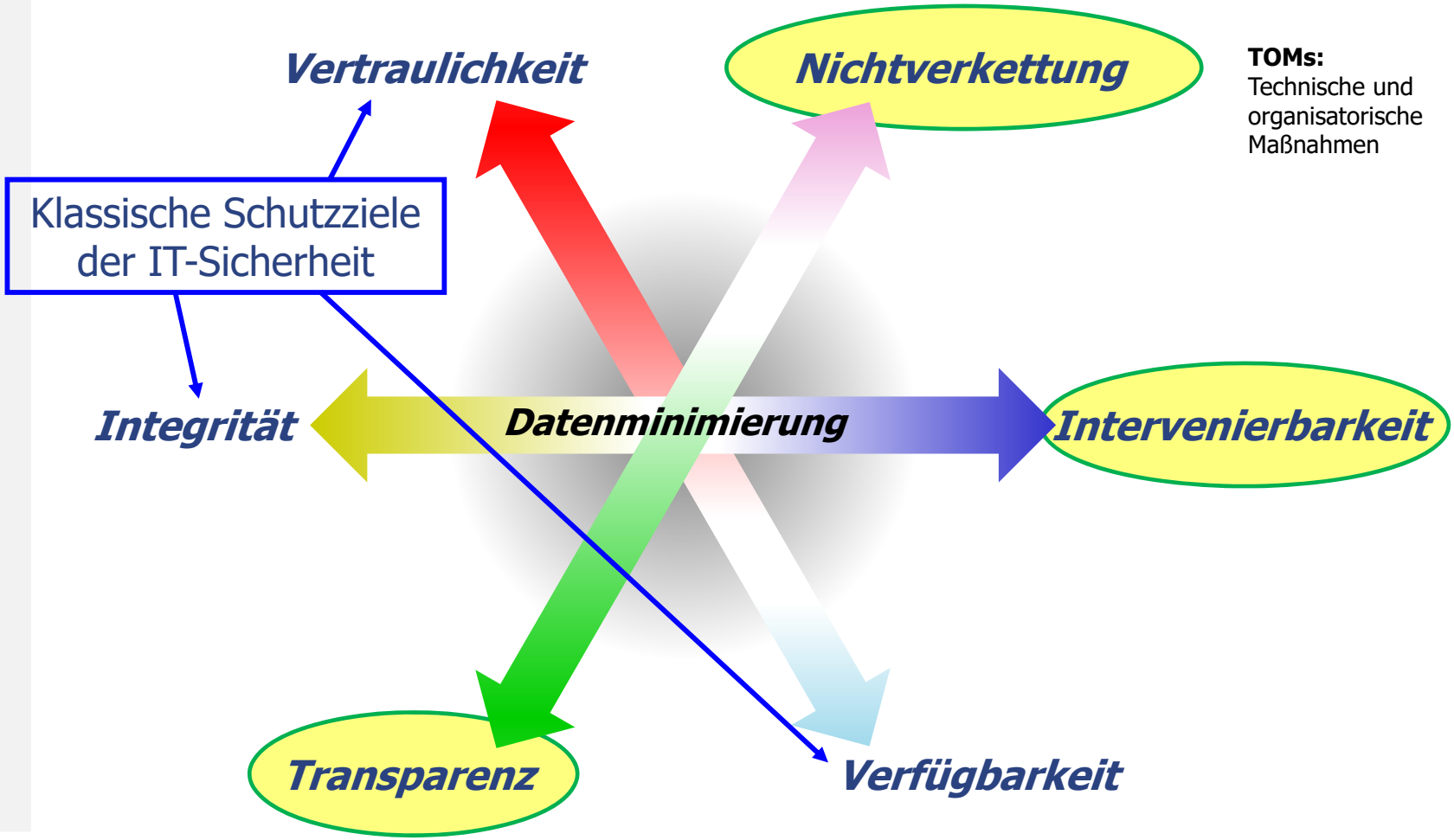
"The use of PETs can help to design information and communication systems and services in a way that minimises the collection and use of personal data and facilitate compliance with data protection rules. The use of PETs should result in making breaches of certain data protection rules more difficult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

European Commission, MEMO/07/159

Gewährleistungsziele im Standard-DS-Modell → TOMs

Überblick

1. Datenschutz ↔ Informationssicherheit
2. Privacy-Enhancing Technologies
3. Gewährleistungsziele im SDM
4. Art. 25 DSGVO
5. Abs. 1: „by Design"
6. Abs. 2: „by Default"



TOMs:
Technische und organisatorische Maßnahmen

Standard-Datenschutzmodell
https://www.datenschutzzentrum.de/sdm/

Überblick

1. Datenschutz ↔ Informationssicherheit
2. Privacy-Enhancing Technologies
3. Gewährleistungsziele im SDM
4. Art. 25 DSGVO
5. Abs. 1: „by Design“
6. Abs. 2: „by Default“

Definitionen im Standard-Datenschutzmodell

Das Gewährleistungsziel Datenminimierung erfasst die grundlegende datenschutzrechtliche Anforderung, die Verarbeitung personenbezogener Daten auf das dem Zweck angemessene, erhebliche und notwendige Maß zu beschränken.

Das Gewährleistungsziel Nichtverkettung bezeichnet die Anforderung, dass personenbezogene Daten nicht zusammengeführt, also verkettet, werden. Sie ist insbesondere dann faktisch umzusetzen, wenn die zusammenzuführenden Daten für unterschiedliche Zwecke erhoben wurden (Zweckbindung).

Überblick

1. Datenschutz ↔ Informationssicherheit
2. Privacy-Enhancing Technologies
3. Gewährleistungsziele im SDM
4. Art. 25 DSGVO
5. Abs. 1: „by Design“
6. Abs. 2: „by Default“

Definitionen im Standard-Datenschutzmodell

Das Gewährleistungsziel Transparenz bezeichnet die Anforderung, dass […] sowohl Betroffene als auch die Betreiber von Systemen sowie zuständige Kontrollinstanzen erkennen können, welche Daten wann und für welchen Zweck […] erhoben und verarbeitet werden, welche Systeme und Prozesse dafür genutzt werden, wohin die Daten zu welchem Zweck fließen und wer die rechtliche Verantwortung […] besitzt.

Das Gewährleistungsziel Intervenierbarkeit bezeichnet die Anforderung, dass den betroffenen Personen die ihnen zustehenden Rechte auf Benachrichtigung, Auskunft, Berichtigung, Löschung […] bei Bestehen der gesetzlichen Voraussetzungen unverzüglich und wirksam gewährt werden und die verarbeitende Stelle verpflichtet ist, die entsprechenden Maßnahmen umzusetzen.

Standard-Datenschutzmodell
https://www.datenschutzzentrum.de/sdm/

Überblick

1. Datenschutz ↔ Informationssicherheit
2. Privacy-Enhancing Technologies
3. Gewährleistungsziele im SDM
4. Art. 25 DSGVO
5. Abs. 1: „by Design“
6. Abs. 2: „by Default“

Auf einen Blick

Das Gewährleistungsziel Datenminimierung erfasst die grundlegende datenschutzrechtliche Anforderung, die Verarbeitung personenbezogener Daten auf das dem Zweck angemessene, erhebliche und notwendige Maß zu beschränken.

Das Gewährleistungsziel Nichtverkettung bezeichnet die Anforderung, dass personenbezogene Daten nicht zusammengeführt, also verkettet, werden. Sie ist insbesondere dann faktisch umzusetzen, wenn die zusammenzuführenden Daten für unterschiedliche Zwecke erhoben wurden (Zweckbindung).

Das Gewährleistungsziel Transparenz bezeichnet die Anforderung, dass […] sowohl Betroffene als auch die Betreiber von Systemen sowie zuständige Kontrollinstanzen erkennen können, welche Daten wann und für welchen Zweck […] erhoben und verarbeitet werden, welche Systeme und Prozesse dafür genutzt werden, wohin die Daten zu welchem Zweck fließen und wer die rechtliche Verantwortung […] besitzt.

Das Gewährleistungsziel Intervenierbarkeit bezeichnet die Anforderung, dass den betroffenen Personen die ihnen zustehenden Rechte auf Benachrichtigung, Auskunft, Berichtigung, Löschung […] bei Bestehen der gesetzlichen Voraussetzungen unverzüglich und wirksam gewährt werden und die verarbeitende Stelle verpflichtet ist, die entsprechenden Maßnahmen umzusetzen.

Wie implementieren?

Überblick

1. Datenschutz ↔ Informationssicherheit
2. Privacy-Enhancing Technologies
3. Gewährleistungsziele im SDM
4. Art. 25 DSGVO
5. Abs. 1: „by Design"
6. Abs. 2: „by Default"

Nichtverkettung

Trennung von Domänen, Gewaltenteilung, Zweckbindung, Anonymisierung

Bild: ivanacoi via Pixabay

Transparenz

Ziel: Nachvollziehbarkeit & Überprüfbarkeit

Bild: geralt via Pixabay

Intervenierbarkeit

z.B. (situationsgerecht): keine automatisierten Entscheidungen, Korrektur, Widerspruch, Rechtsschutz, Rückabwicklung, Haftung …

Bild: geralt via Pixabay

Ziel: Risikobeherrschung –
Risiko für die Rechte und Freiheiten natürlicher Personen
→ (Datenschutz-)Folgenabschätzung

Überblick

1. Datenschutz ↔ Informationssicherheit
2. Privacy-Enhancing Technologies
3. Gewährleistungsziele im SDM
4. Art. 25 DSGVO
5. Abs. 1: „by Design"
6. Abs. 2: „by Default"

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

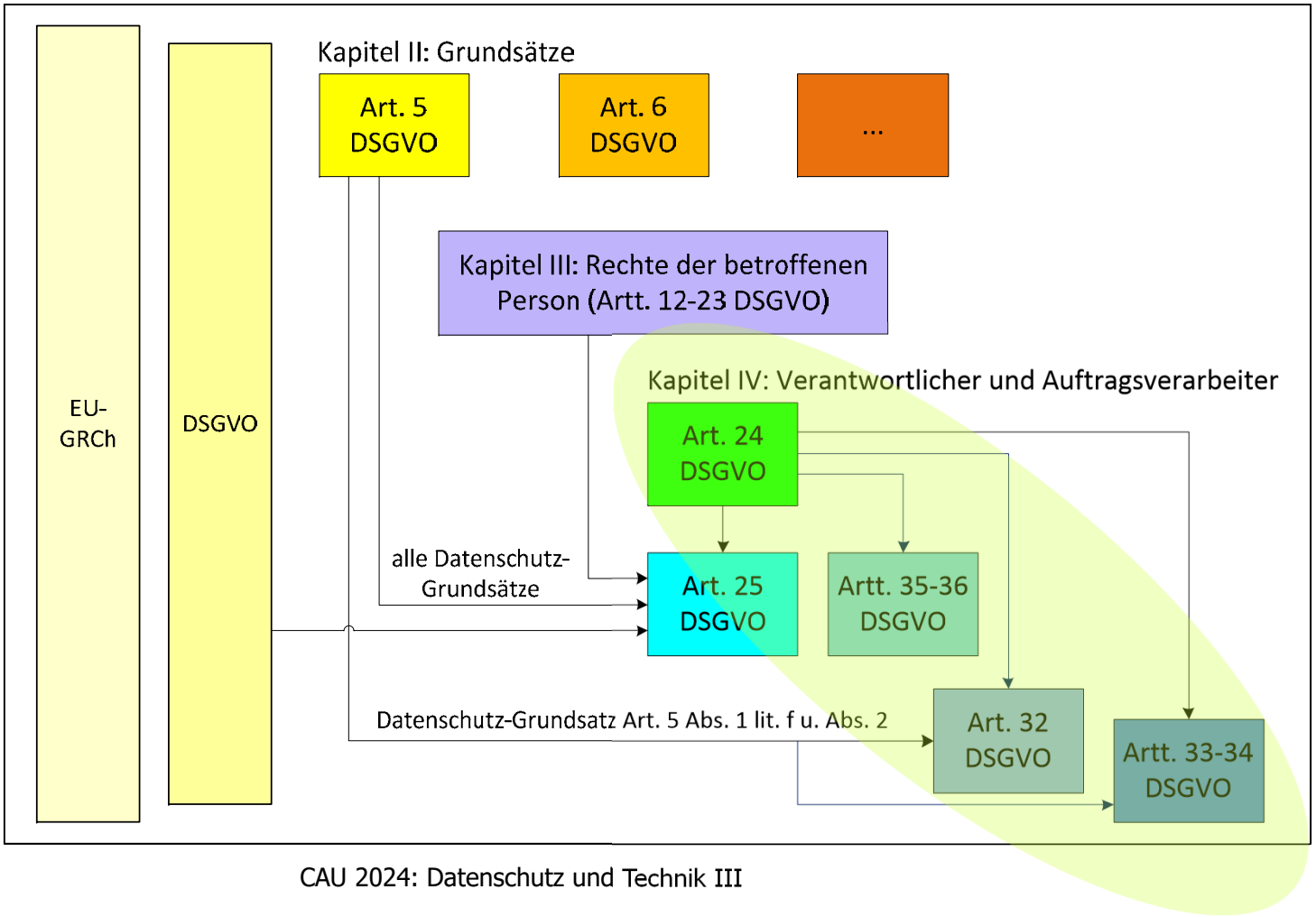
- [DE] Artikel 25: Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen
- [FR] Article 25: Protection des données dès la conception et protection des données par défaut
- [ES] Artículo 25: Protección de datos desde el diseño y por defecto
- [SV] Artikel 25: Inbyggt dataskydd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

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

Überblick

1. Datenschutz ↔ Informationssicherheit
2. Privacy-Enhancing Technologies
3. Gewährleistungsziele im SDM
4. Art. 25 DSGVO
5. Abs. 1: „by Design“
6. Abs. 2: „by Default“

Art. 25 im Gefüge der DSGVO



Überblick

1. Datenschutz ↔ Informationssicherheit
2. Privacy-Enhancing Technologies
3. Gewährleistungsziele im SDM
4. Art. 25 DSGVO
5. Abs. 1: „by Design“
6. Abs. 2: „by Default“

Art. 25 im Gefüge der DSGVO

Art. 5 DSGVO
– immer zu erfüllen bei personenbezogenen Daten

Oberthema: Fairness

Abs. 1:

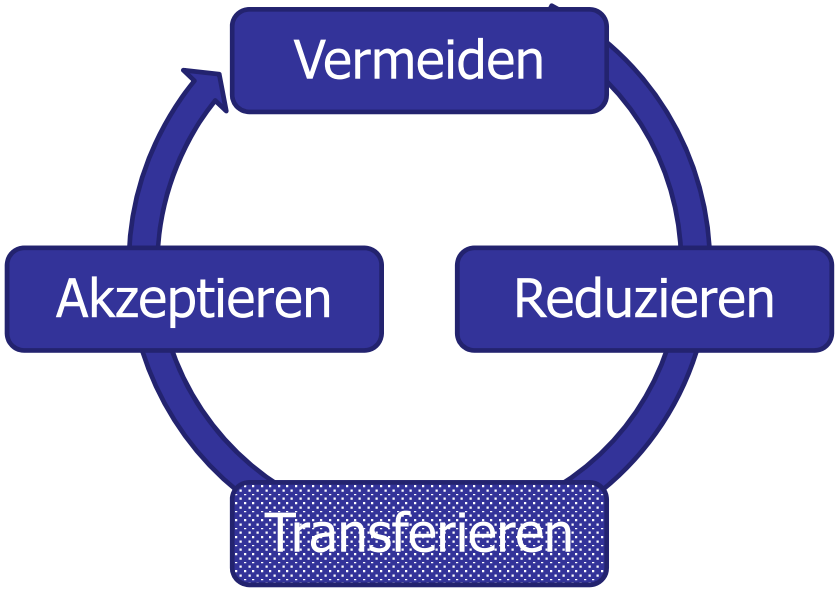
a) Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
b) Zweckbindung
c) Datenminimierung
d) Richtigkeit
e) Speicherbegrenzung
f) Integrität und Vertraulichkeit (Datensicherheit)

Abs. 2: Rechenschaftspflicht

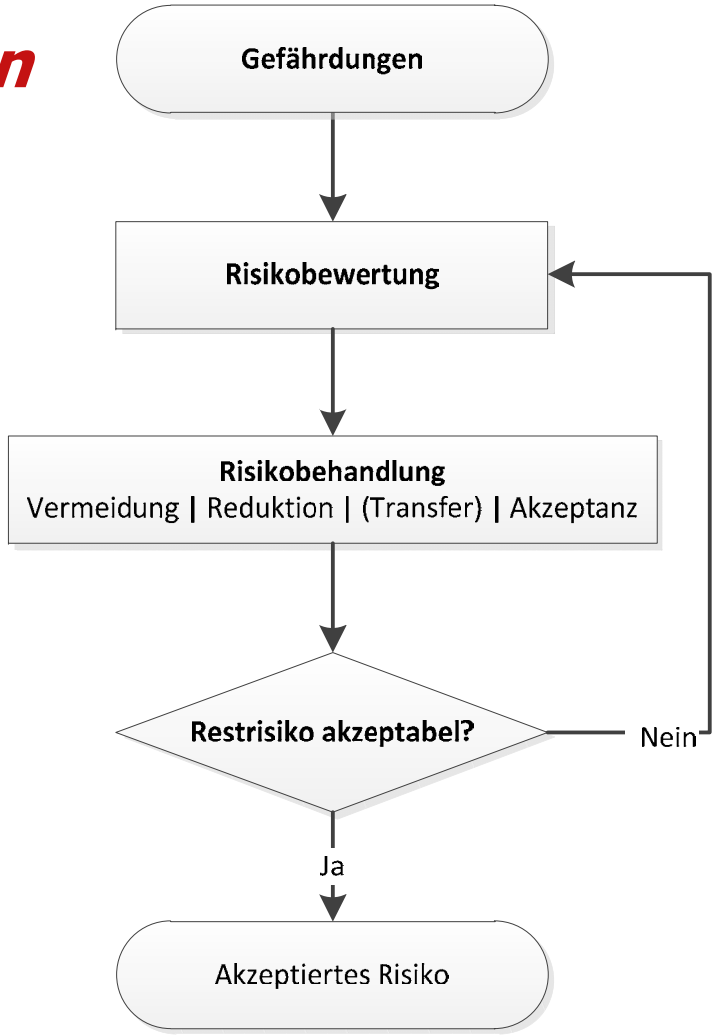
Überblick

1. Datenschutz ↔ Informationssicherheit
2. Privacy-Enhancing Technologies
3. Gewährleistungsziele im SDM
4. Art. 25 DSGVO
5. Abs. 1: „by Design“
6. Abs. 2: „by Default“

Nicht nur Art. 25: Strategien der Risikobehandlung



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

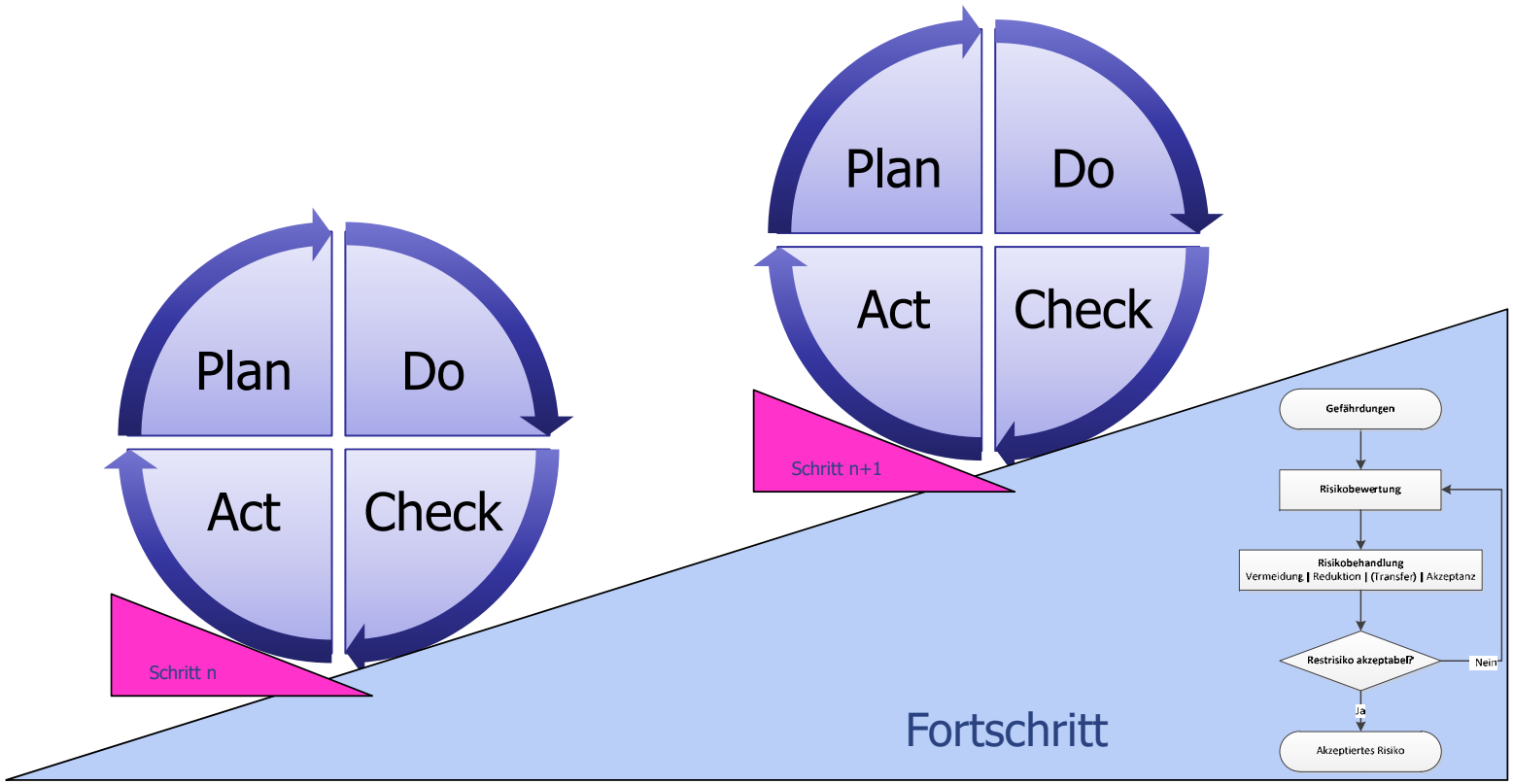


ISO/IEC 27005, https://www.bsi.bund.de/dok/10990674

Überblick

1. Datenschutz ↔ Informationssicherheit
2. Privacy-Enhancing Technologies
3. Gewährleistungsziele im SDM
4. Art. 25 DSGVO
5. Abs. 1: „by Design“
6. Abs. 2: „by Default“

PDCA-Zyklen über die Zeit, auch für Risikobehandlung



Überblick

1. Datenschutz ↔ Informationssicherheit
2. Privacy-Enhancing Technologies
3. Gewährleistungsziele im SDM
4. Art. 25 DSGVO
5. Abs. 1: „by Design“
6. Abs. 2: „by Default“

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

Unter welchen Bedingungen?

trifft der Verantwortliche

Wer?

sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung

Wann?

geeignete technische und organisatorische Maßnahmen – wie z. B. Pseudonymisierung –,

Was ist zu tun?

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.

Was konkret? Mit welchem Ziel?

Überblick

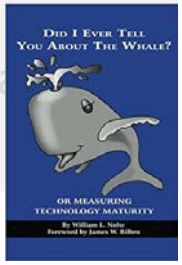
1. Datenschutz ↔ Informationssicherheit
2. Privacy-Enhancing Technologies
3. Gewährleistungsziele im SDM
4. Art. 25 DSGVO
5. Abs. 1: „by Design"
6. Abs. 2: „by Default"

Absatz 1: „by Design" – Erwägungsgrund 78

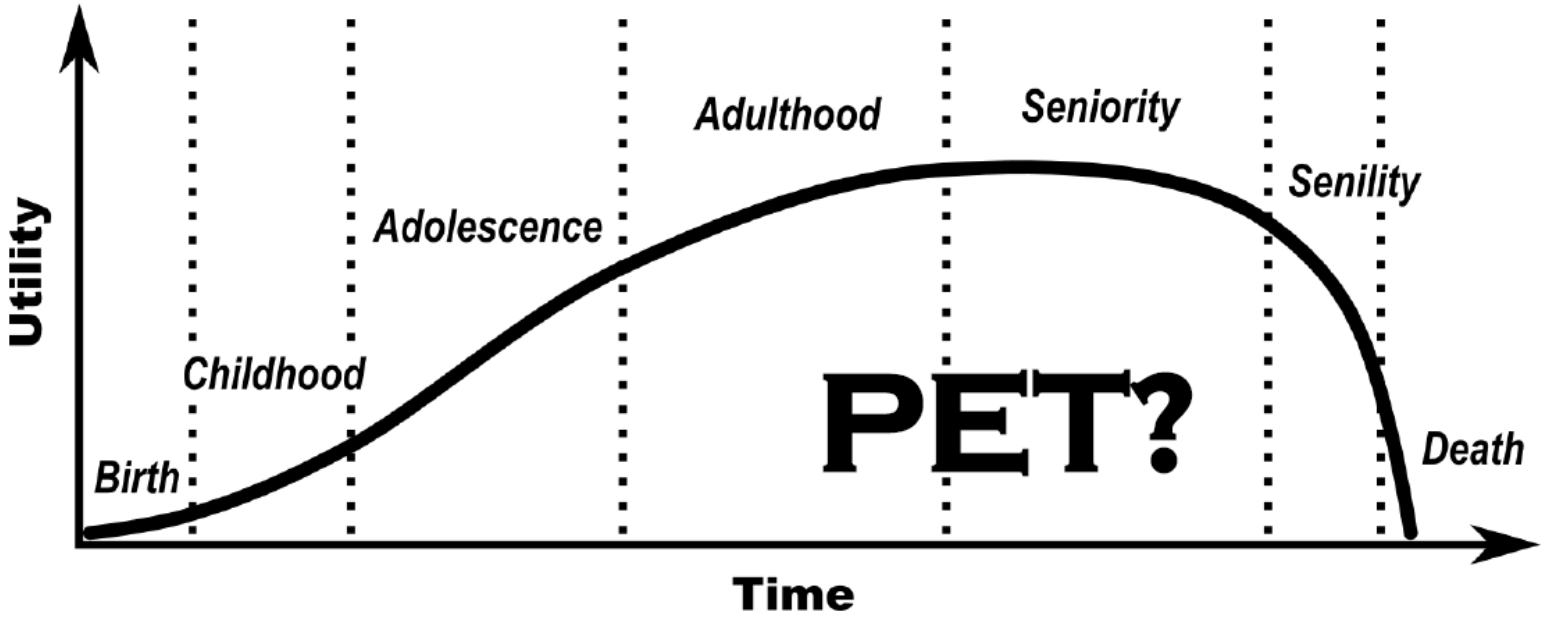
- Nachweis durch interne Strategien & t+o Maßnahmen, u.a.
  - Datenminimierung
  - Frühestmögliche Pseudonymisierung
  - Transparenz in Bezug auf Funktionen+Verarbeitung
  - Ermöglichung der Überwachung der Verarbeitung durch die betroffenen Personen
  - Ermöglichung für Sicherheitsfunktionen „on top"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

Überblick

1. Datenschutz ↔ Informationssicherheit
2. Privacy-Enhancing Technologies
3. Gewährleistungsziele im SDM
4. Art. 25 DSGVO
5. Abs. 1: „by Design“
6. Abs. 2: „by Def



„by Design“ & Privacy-Enhancing Technologies



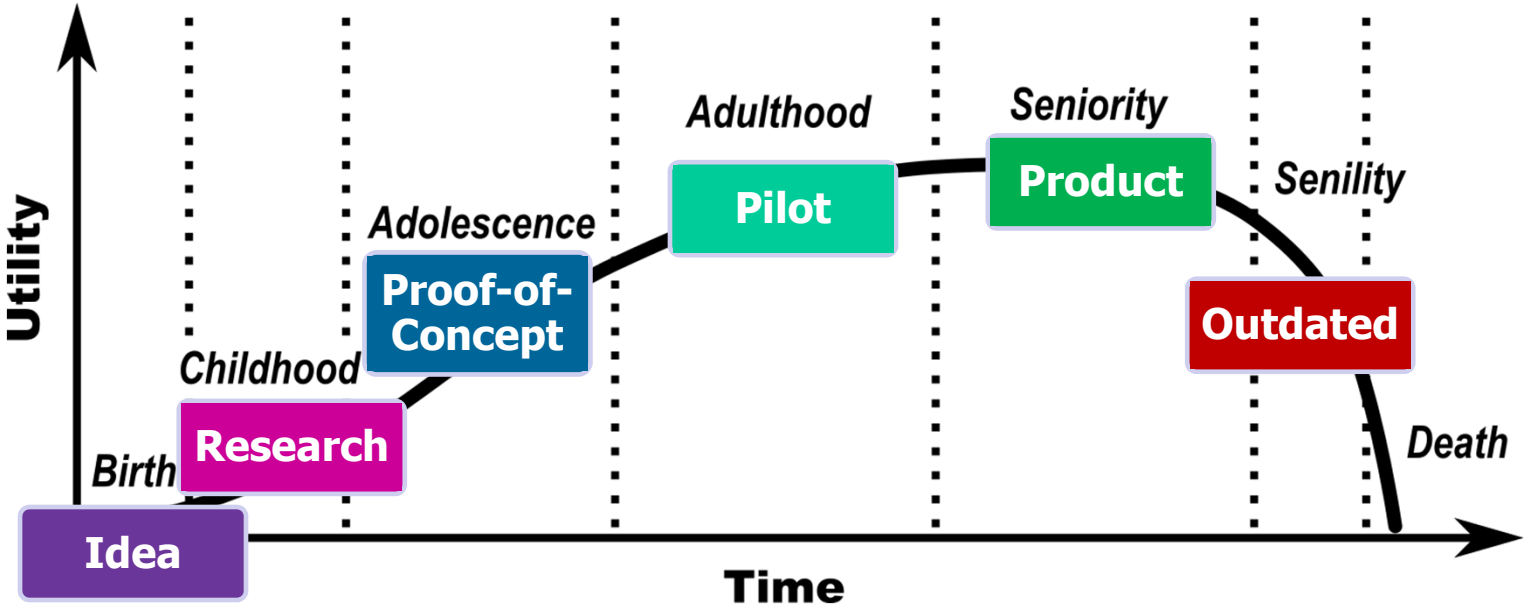
Beispiele: MD5, Windows XP, …

Überblick

1. Datenschutz ↔ Informationssicherheit
2. Privacy-Enhancing Technologies
3. Gewährleistungsziele im SDM
4. Art. 25 DSGVO
5. Abs. 1: „by Design“
6. Abs. 2: „by Defa

„by Design" & Privacy-Enhancing Technologies

Reifegrad, „Stand der Technik“?



Überblick

1. Datenschutz ↔ Informationssicherheit
2. Privacy-Enhancing Technologies
3. Gewährleistungsziele im SDM
4. Art. 25 DSGVO
5. Abs. 1: „by Design"
6. Abs. 2: „by Default"

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. Datenschutz ↔ Informationssicherheit
2. Privacy-Enhancing Technologies
3. Gewährleistungsziele im SDM
4. Art. 25 DSGVO
5. Abs. 1: „by Design"
6. Abs. 2: „by Default"

Wie genau? – Bsp. Videoüberwachung

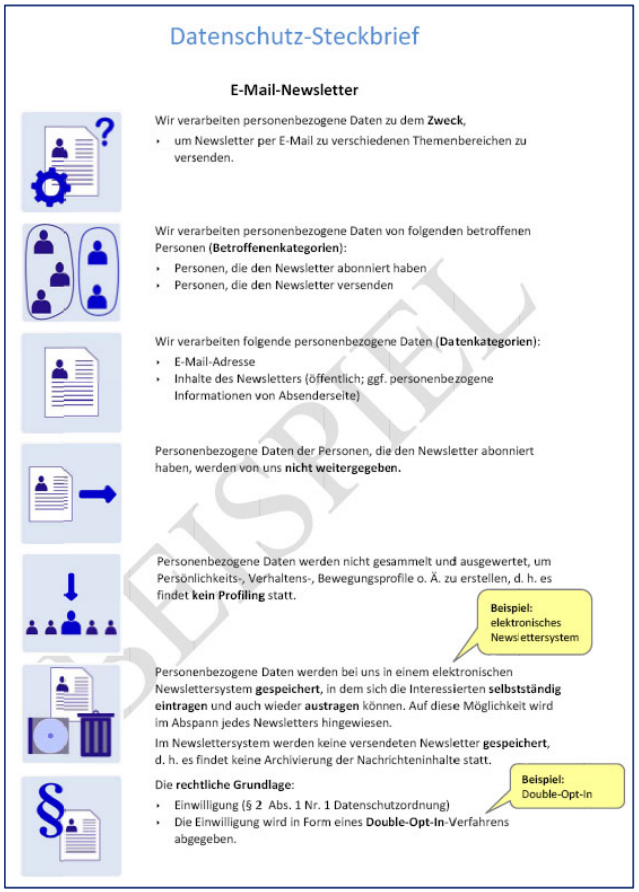
Sichere und datenschutzfreundliche Gestaltung

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. Datenschutz ↔ Informationssicherheit
2. Privacy-Enhancing Technologies
3. Gewährleistungsziele im SDM
4. Art. 25 DSGVO
5. Abs. 1: „by Design“
6. Abs. 2: „by Default“

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 (**Betroffenenkategorien**):
- 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.

Beispiel: elektronisches Newsettersystem

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: Double-Opt-In

BEISPIEL

Achtung
Klingelkamera

Name und Kontaktdaten des Verantwortlichen:

ULD

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 (LDSG)

Funktionsweise der Kamera und Gegensprechfunktion:

Erst beim Klingeln werden die Kamera und die Gegensprechfunktion 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 Gegensprechfunktion ausgeschaltet.

Informationen zu **Ihren Rechten** erhalten Sie auf unserer Webseite:

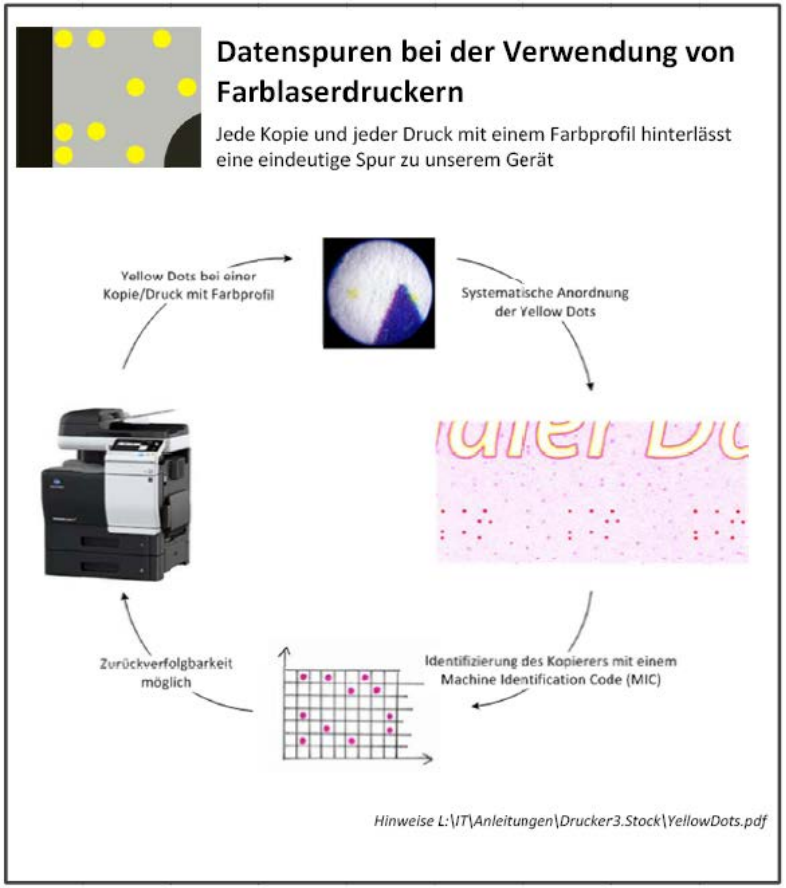
www.datenschutzzentrum.de/datenschutzerklärung

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

Überblick

1. Datenschutz ↔ Informationssicherheit
2. Privacy-Enhancing Technologies
3. Gewährleistungsziele im SDM
4. Art. 25 DSGVO
5. Abs. 1: „by Design“
6. Abs. 2: „by Default“

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. Datenschutz ↔ Informationssicherheit
2. Privacy-Enhancing Technologies
3. Gewährleistungsziele im SDM
4. Art. 25 DSGVO
5. Abs. 1: „by Design“
6. Abs. 2: „by Default“

Überblick

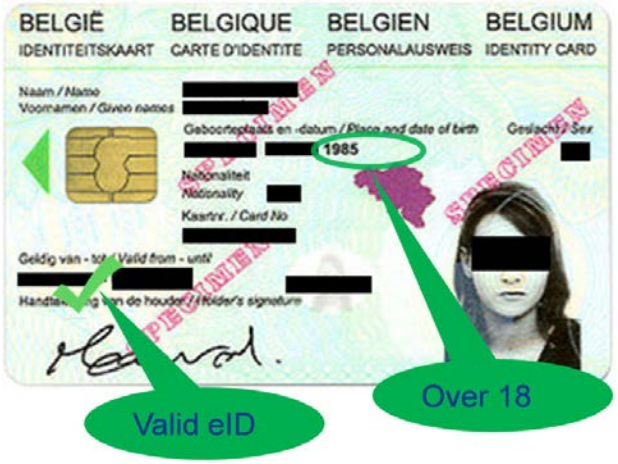
1. Datenschutz ↔ Informationssicherheit
2. Privacy-Enhancing Technologies
3. Gewährleistungsziele im SDM
4. Art. 25 DSGVO
5. Abs. 1: „by Design“
6. Abs. 2: „by Default“

Überblick

1. Datenschutz ↔ Informationssicherheit
2. Privacy-Enhancing Technologies
3. Gewährleistungsziele im SDM
4. Art. 25 DSGVO
5. Abs. 1: „by Design“
6. Abs. 2: „by Default“

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. Datenschutz ↔ Informationssicherheit
2. Privacy-Enhancing Technologies
3. Gewährleistungsziele im SDM
4. Art. 25 DSGVO
5. Abs. 1: „by Design"
6. Abs. 2: „by Default"

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

Unter welchen Bedingungen?

trifft der Verantwortliche

Wer?

sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung

Wann?

geeignete technische und organisatorische Maßnahmen – wie z. B. Pseudonymisierung –,

Was ist zu tun?

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.

Was konkret? Mit welchem Ziel?

Überblick

1. Datenschutz ↔ Informationssicherheit
2. Privacy-Enhancing Technologies
3. Gewährleistungsziele im SDM
4. Art. 25 DSGVO
5. Abs. 1: „by Design"
6. Abs. 2: „by Default"

Absatz 2: „by Default"

Artikel 25 […] durch datenschutzfreundliche Voreinstellungen

(2) Der Verantwortliche — Wer?

trifft geeignete technische und organisatorische Maßnahmen, — Was ist zu tun?

die sicherstellen, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. — Was konkret? Mit welchem Ziel?

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

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

Immer! — Unter welchen Bedingungen?

Überblick

1. Datenschutz ↔ Informationssicherheit
2. Privacy-Enhancing Technologies
3. Gewährleistungsziele im SDM
4. Art. 25 DSGVO
5. Abs. 1: „by Design"
6. Abs. 2: „by Default"

Was ist gemeint mit „by Default"?

- Startpunkt „Datenschutz"
- „durch Voreinstellung":

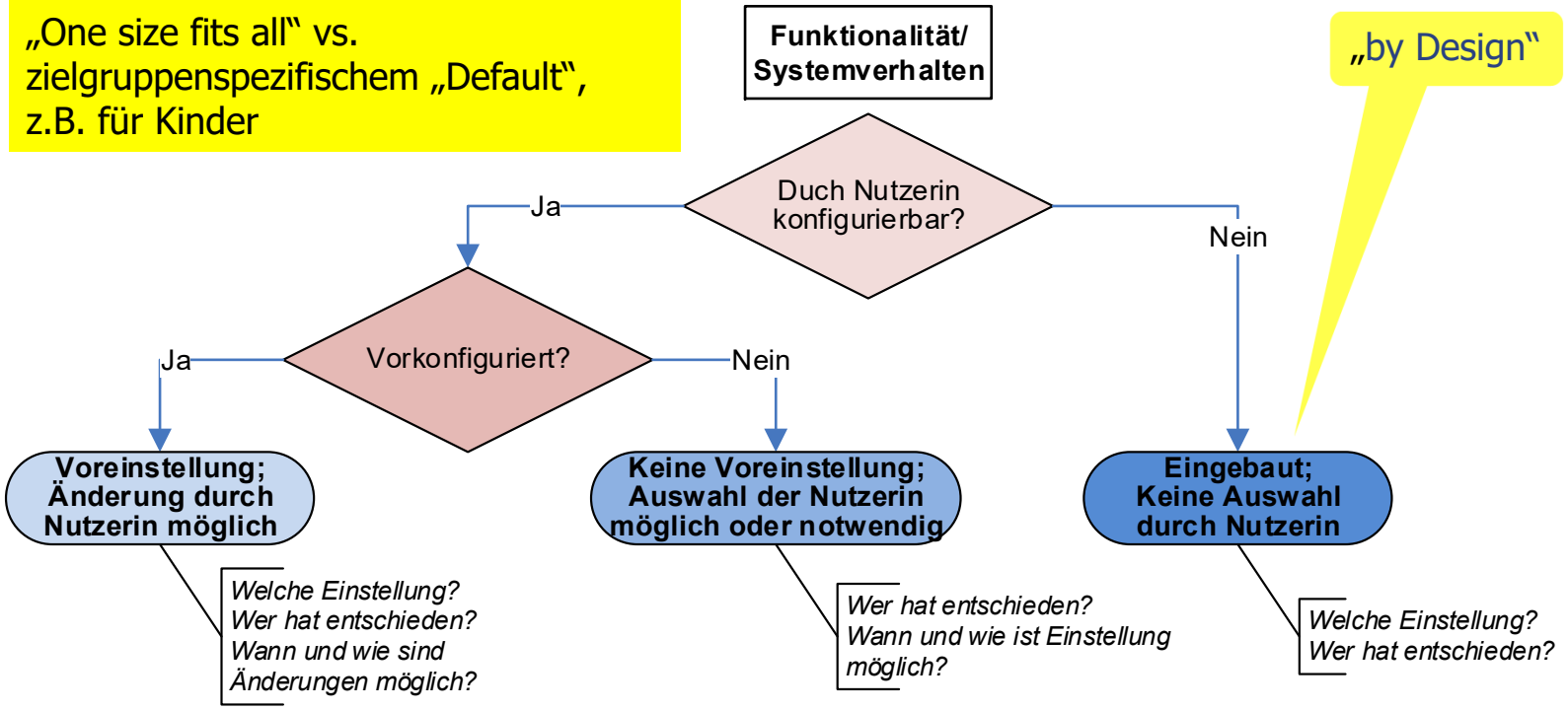
  „Entscheidungen über Konfigurationswerte oder Verarbeitungsoptionen, die in einem Verarbeitungssystem eingestellt oder vorgeschrieben sind"
  (EDSA, Leitlinien 4/2019, Rn. 41)

Überblick

1. Datenschutz ↔ Informationssicherheit
2. Privacy-Enhancing Technologies
3. Gewährleistungsziele im SDM
4. Art. 25 DSGVO
5. Abs. 1: „by Design“
6. Abs. 2: „by Default“

Absatz 2: „by Default“ – 3 Fälle

„One size fits all“ vs. zielgruppenspezifischem „Default“, z.B. für Kinder



Bsp.: anonyme Nutzung, kein Tracking

Bsp.: Auswahl des Bezahl-Systems

Bsp.: verschlüsselte Kommunikation

s.a.: *Hansen:* Data Protection by Default in Identity-Related Applications. Proc. IDMAN, 2013, IFIP AICT 396, 4.

Überblick

1. Datenschutz ↔ Informationssicherheit
2. Privacy-Enhancing Technologies
3. Gewährleistungsziele im SDM
4. Art. 25 DSGVO
5. Abs. 1: „by Design"
6. Abs. 2: „by Default"

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

- Deceptive Design
- Addictive Design

Bild: Gerd Altmann via Pixabay

Bild: rawpixel via Pixabay

Überblick

1. Datenschutz ↔ Informationssicherheit
2. Privacy-Enhancing Technologies
3. Gewährleistungsziele im SDM
4. Art. 25 DSGVO
5. Abs. 1: „by Design"
6. Abs. 2: „by Default"

Materialien

- 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