Datenschutz „by Design“ & „by Default“

Marit Hansen

Berlin, 5. Juni 2019

BvD-Verbandstage 2019

forum <privatheit> selbstbestimmtes_leben_in_der_digitalen_welt

ULD Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Überblick

1. Artikel 25 der DSGVO im Gesamtgefüge der Datenschutzreform
2. „by Design“: Datenschutz richtig einbauen
3. „by Default“: Mehr als das Erforderlichkeitsprinzip
4. Wie geht´s? Vom abstrakten Recht in die konkrete Praxis
5. Fazit

Art. 25 DSGVO *(vor der Korrektur)*

L 119/48 DE Amtsblatt der Europäischen Union 4.5.2016

Artikel 25

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

(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 — trifft, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

(2) Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich 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.

(3) Ein genehmigtes Zertifizierungsverfahren gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in den Absätzen 1 und 2 des vorliegenden Artikels genannten Anforderungen nachzuweisen.

Datenschutz „by Design“ & „by Default“

- Art. 25 DSGVO – mehr als „eingebaute Sicherheit“ (Art. 32 DSGVO)
- Richtet sich an:
  - Datenverarbeiter (primär: Verantwortlicher)
  - Indirekt: Dienstleister und Hersteller von IT-Systemen
- Ziel: Gestaltung von Systemen + Diensten
  von Anfang an über den gesamten Lebenszyklus
  a) datenminimierend
  b) mit möglichst datenschutzfreundlichen Voreinstellungen
- Wichtig für jede Beschaffung + Nachweispflicht

Wichtigkeit von „by Design“

Erwägungsgrund 4 der Datenschutz-Grundverordnung

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

Adressaten:
- Verantwortliche
- Auftragsverarbeiter
- Hersteller!
- Gesetzgeber!

Frühere Ansätze liefen großenteils leer

§ 3a BDSG Datenvermeidung und Datensparsamkeit

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen.

Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.

Und wenn nicht?
Keine Sanktion.

§ 9 BDSG + Anlage (zu § 9 Satz 1 BDSG):
„xy-Kontrolle“ – na ja.

Technischer Datenschutz der DSGVO als „Game Changer“

Bild: Astryd_MAD via Pixabay

Mächtige Toolbox, wenn entsprechend verwendet

- Marktortprinzip (Art. 3 DSGVO)
- Verantwortung (Art. 24 DSGVO)
- Datenschutz „by design“ (Art. 25(1) DSGVO)
- Datenschutz „by default“ (Art. 25(2) DSGVO)
- Sicherheit (Art. 32 DSGVO)
- Datenschutz-Folgenabschätzung (Art. 35 DSGVO – „Rechte und Freiheiten natürlicher Personen“)
- Zertifizierung (Artt. 42+43 DSGVO)
- Bußgelder & Sanktionen (Art. 83+84 DSGVO)
- Gerichte

Vorab: Zulässigkeits-prüfung

Anmerkung: „by Design“ = „durch Technikgestaltung“?

- [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
- [DE] Artikel 25: Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen
- [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

Bild: athree23 via Pixabay

1. Artikel 25 der DSGVO im Gesamtgefüge der Datenschutzreform
2. „by Design“: Datenschutz richtig einbauen
3. „by Default“: Mehr als das Erforderlichkeitsprinzip
4. Wie geht´s? Vom abstrakten Recht in die konkrete Praxis
5. Fazit

Datenschutz durch Technikgestaltung

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

Viele möglicherweise begrenzende Bedingungen ↑↓

trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen – wie z. B. Pseudonymisierung – trifft, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

Begrenzung durch „Stand der Technik“ und „Implementierungskosten“?

Identische Formulierung in Art. 32 „Sicherheit der Verarbeitung“

Artikel 25

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

(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 Maßn ausgelegt sind, die Datenschutzgrundsätze wie etwa Daten Garantien in die Verarbeitung aufzunehmen, um den Anforde betroffenen Personen zu schützen.

(2) Der Verantwortliche trifft geeignete technische und o Voreinstellung grundsätzlich nur personenbezogene Daten, d tungszweck erforderlich ist, verarbeitet werden. Diese Ver bezogenen Daten, den Umfang ihrer Verarbeitung, ihre Sp müssen insbesondere sicherstellen, dass personenbezogene Person einer unbestimmten Zahl von natürlichen Personen zu

(3) Ein genehmigtes Zertifizierungsverfahren gemäß Art Erfüllung der in den Absätzen 1 und 2 des vorliegenden Artik

Artikel 32

Sicherheit der Verarbeitung

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des U Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und S Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftrag geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schut gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem phys technischen Zwischenfall rasch wiederherzustellen;

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der techr organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, Verarbeitung verbunden sind, insbesondere durch — ob unbeabsichtigt oder unrechtmäßig — Vernichtu Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

ULD www.datenschutzzentrum.de

Begrenzung durch „Stand der Technik“ und „Implementierungskosten“?

Article 17

Security of processing

1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

Auf EU-Ebene nichts Neues, siehe EU-Datenschutz-Richtlinie 95/46/EG

Begrenzung durch „Stand der Technik“ und „Implementierungskosten“?

Nicht enthalten in Art. 24 DSGVO („Verantwortung“)

Artikel 24

Verantwortung des für die Verarbeitung Verantwortlichen

(1) Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.

(2) Sofern dies in einem angemessenen Verhältnis zu den Verarbeitungstätigkeiten steht, müssen die Maßnahmen gemäß Absatz 1 die Anwendung geeigneter Datenschutzvorkehrungen durch

(3) Die Einhaltung der genehmigten Verhaltensregeln gemäß Artikel 40 verfahrens gemäß Artikel 42 kann als Gesichtspunkt herangezogen wer Verantwortlichen nachzuweisen.

„Stand der Technik“ und „Implementierungskosten“ können bei hohen Risiken nicht als „Ausrede“ dienen

(z.B. Art. 36 Vorherige Konsultation)

Datenschutz durch Technikgestaltung

Artikel 25 Datenschutz durch Technikgestaltung […]

Was ist zu tun? „Eingebauter Datenschutz“, u.a. Art. 5 DSGVO betont, aber insgesamt DSGVO

(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 – trifft, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

Was sagt die Datenschutz-Grundverordnung?

Art. 5 DSGVO
– immer zu erfüllen bei personenbezogenen Daten

Abs. 1:

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

Bild: skylarvision via Pixabay

Abs. 2: Rechenschaftspflicht

Überblick


Bild: athree23 via Pixabay

1. Artikel 25 der DSGVO im Gesamtgefüge der Datenschutzreform
2. „by Design“: Datenschutz richtig einbauen
3. „by Default“: Mehr als das Erforderlichkeitsprinzip
4. Wie geht´s? Vom abstrakten Recht in die konkrete Praxis
5. Fazit

Datenschutz durch datenschutzfreundliche Voreinstellungen

Artikel 25 […] durch datenschutzfreundliche Voreinstellungen

bedingungslos

(2) Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung ~~grundsätzlich~~ 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.

Korrigierter Übersetzungsfehler!

ULD www.datenschutzzentrum.de

Datenschutz durch datenschutzfreundliche Voreinstellungen

Artikel 25 […] durch datenschutzfreundliche Voreinstellungen

Betont das Erforderlichkeitsprinzip (Artikel 5)

(2) Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung ~~grundsätzlich~~ 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.

Nicht nur minimaler Datenkatalog; auch generelle Risikominimierung

Datenschutz durch datenschutzfreundliche Voreinstellungen

Artikel 25 […] durch datenschutzfreundliche Voreinstellungen

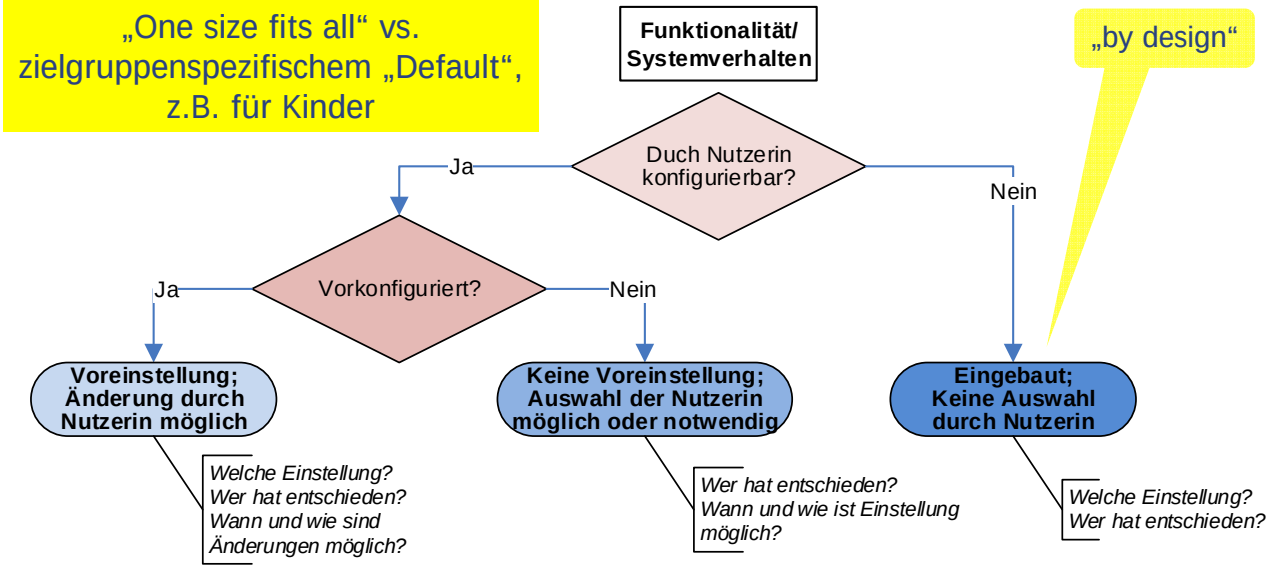
(2) Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung ~~grundsätzlich~~ nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung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

Bsp.: Social Networks

„… by Default“: Drei Fälle der (Vor-)Konfiguration

„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.: Marit Hansen: Data Protection by Default in Identity-Related Applications. Proc. IDMAN 2013, IFIP AICT 396, S. 4-17.

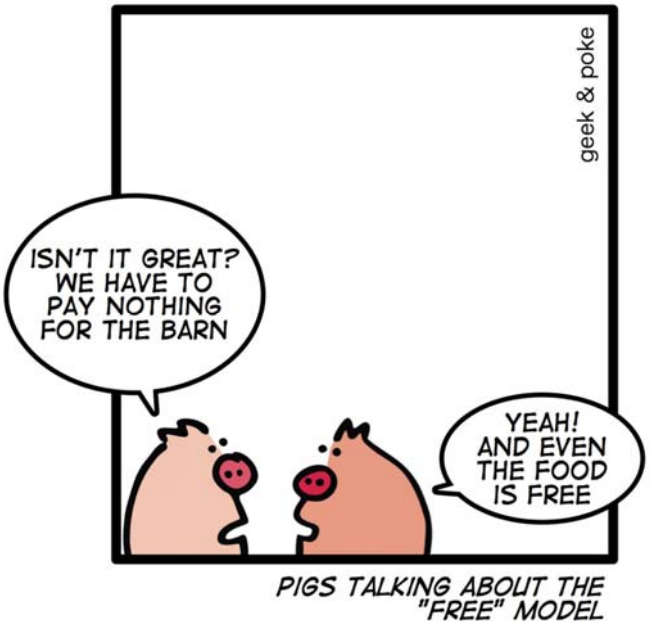
Heutiges Internet-Modell

Wie wird sich dies in der Zukunft mit Datenschutz „by Default“ entwickeln?

Und ohne „Dark Patterns?“

Forbrukerrådet (Norwegen): Report „Deceived by Design“, https://www.forbrukerradet.no/dark-patterns/

Chancen für Alternativen!



http://geek-and-poke.com/geekandpoke/2010/12/21/the-free-model.html

Überblick

Bild: athree23 via Pixabay

1. Artikel 25 der DSGVO im Gesamtgefüge der Datenschutzreform
2. „by Design“: Datenschutz richtig einbauen
3. „by Default“: Mehr als das Erforderlichkeitsprinzip
4. Wie geht´s? Vom abstrakten Recht in die konkrete Praxis
5. Fazit

Datenschutz „by Design“ & „by Default“ gemäß Erwägungsgrund 78 DSGVO

- Nachweis durch interne Strategien & t+o Maßnahmen, u.a.
  - Datenminimierung
  - Schnellstmögliche 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

Aggregation
Anonymisierung
Attributbasierte Berechtigungszertifikate
Dashboard
Auskunftsportal
Elektronischer Datenbrief
Machine-readable Policies
Icons
Dezentralisierung
Zweck-Kennzeichnung
Kein Freitext
Automatisches Löschen
Sticky Policies
Schnittstellen zu Selbstdatenschutz-Tools

Exkurs: Pseudonymisierung

Art. 4 Nr. 5 DSGVO:

„Pseudonymisierung“ die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten **ohne Hinzuziehung zusätzlicher Informationen nicht mehr** einer spezifischen betroffenen Person zugeordnet werden können,

↓ gezielte Nichtverfügbarkeit

sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden;

Exkurs: Pseudonymisierung

Art. 4 Nr. 5 DSGVO (visualisiert)

s.a. Tätigkeitsbericht 2019 des ULD S-H, Tz. 2.3.3: https://uldsh.de/tb37

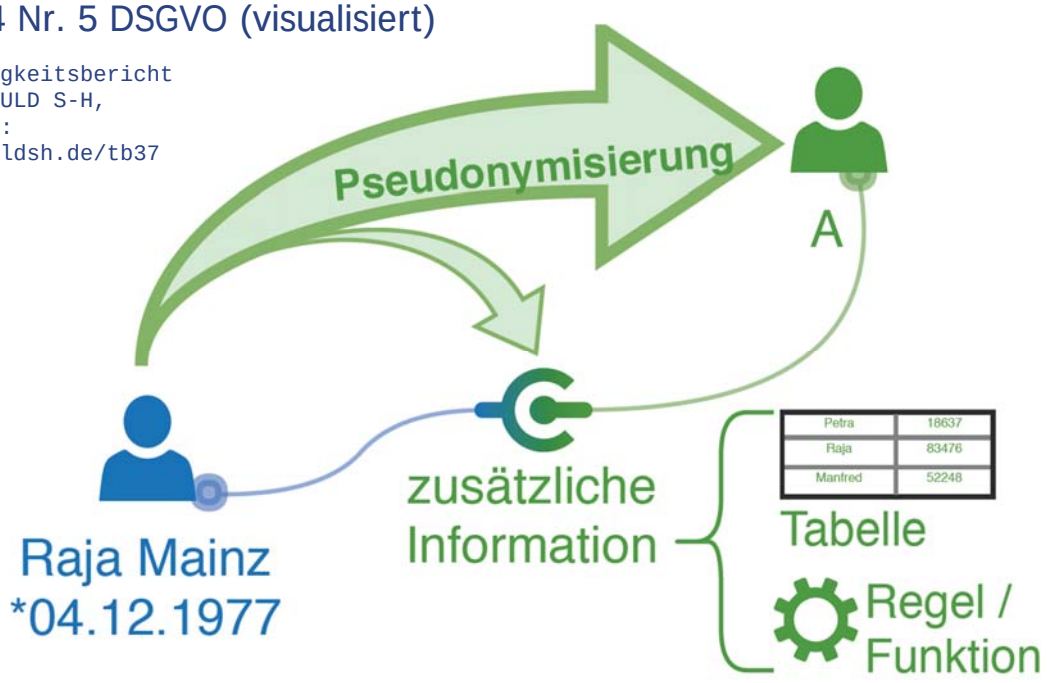


Bild: Benjamin Walczak (ULD)

Unterschiede Pseudo-/Anonymisierung

Pseudonymisierung

Verarbeitung dergestalt, dass

aus personenbezogenen Daten [Input]

veränderte Daten (pseudonymisierte Daten) [Output]

werden,
die dann nur mit Hilfe „zusätzlicher Informationen“ einer spezifischen Person zugeordnet werden können.

(Pseudonymisierung ist selbst Verarbeitung i.S.d. DSGVO.)

weiterhin personenbezogen!

Anonymisierung

Verarbeitung dergestalt, dass

aus personenbezogenen Daten [Input]

veränderte Daten ohne Personenbezug (anonymisierte Daten) [Output]

werden.

(Anonymisierung ist selbst Verarbeitung i.S.d. DSGVO.)

Exkurs: anonymisiert/anonym

Erwägungsgrund 26 DSGVO:

> [...] Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d. h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen,
> oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann.
> Diese Verordnung betrifft somit nicht die Verarbeitung solcher anonymer Daten, auch für statistische oder für Forschungszwecke.

Weiterhin wertvoll: WP 216 der Art. 29-Datenschutzgruppe

- Art. 29 Data Protection Working Party:
  Opinion 05/2014 on "Anonymisation Techniques” (WP 216)
  https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

- Drei Risiken, die zur Identifizierung von Personen führen können:
  - Singling out
  - Linkability
  - Inference

- Anonymisierung möglich durch „randomization and generalization“
- Vielfache Möglichkeiten der Pseudonymisierung

Beispiel: Videoüberwachung nach der DSGVO

Sichere und datenschutzfreundliche Gestaltung

Bei der Auswahl, der Installation und dem Betrieb von Videoüberwachungssysteme ist auf die sichere (Art. 32 DSGVO) und datenschutzfreundliche (Art. 25 DSGVO) Gestaltung zu achten. Insbesondere muss der Verantwortliche prüfen, inwieweit eine

Videoüberwachung zeitlich eingeschränkt werden kann und welche Bereiche der Überwachung ausgeblendet oder verpixelt werden können.

Schon bei der Beschaffung der Videotechnik sollte auf „eingebauten Datenschutz“ geachtet werden. 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.

Beispiel: 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 Newsletter-System

Personenbezogene Daten werden bei uns in einem elektronischen Newsletter-System **gespeichert**, in dem sich die Interessierten **selbstständig eintragen** und auch wieder **austragen** können. Auf diese Möglichkeit wird im Abspann jedes Newsletters hingewiesen.
Im Newsletter-System werden keine versendeten Newsletter **gespeichert**, d. h. es findet keine Archivierung der Nachrichteninhalte statt.

Beispiel: Double-Opt-In

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

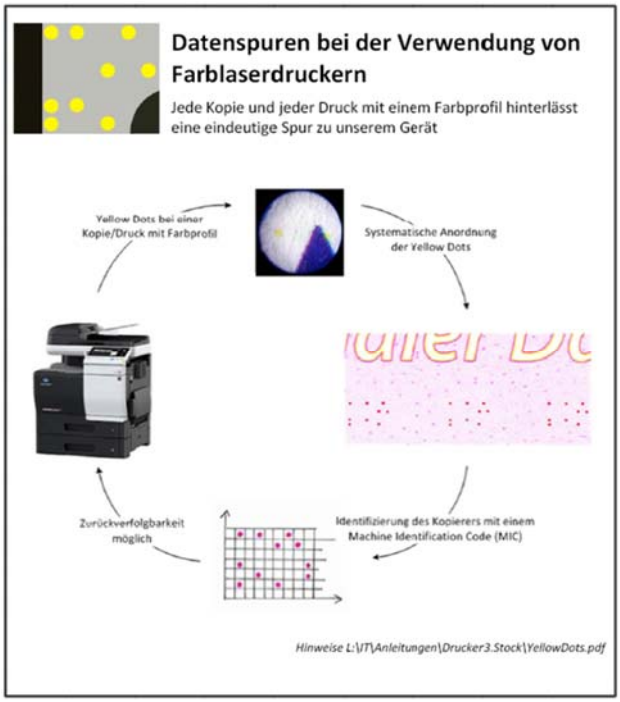
BEISPIEL

„Datenschutz-Steckbrief“

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

Beispiel: Transparenz für „Klingelkamera“

Beispiel: Wenn der Markt nichts hergibt, zumindest Transparenz



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

Zu tun: interne Strategien

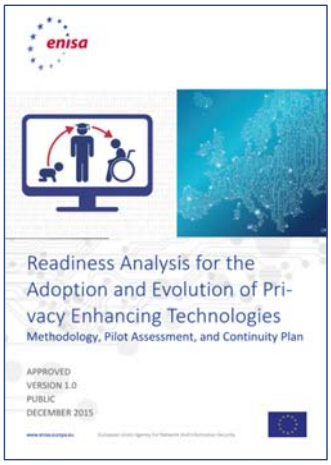
- Abhängigkeit von Herstellern – aber diese sind nicht direkt adressiert
- Indirekte Effekte nutzen:
  - „... sollten die Hersteller der Produkte, Dienste und Anwendungen ermutigt werden ...“ (EG 78)
  - Öffentliche Ausschreibung (EG 78)
  - Verpflichtung der Verantwortlichen zum Nachweis der DSGVO-Compliance, z.B. Datenschutz-Folgenabschätzung bei hohem Risiko (Art. 35 DSGVO) und bei Zertifizierung (Art. 42 DSGVO): DSGVO-Compliance und Informationen der Hersteller und Dienstleister müssen eingefordert werden
- Für interne Strategien: Aufnahme in Datenschutz-Management

Interne Strategien

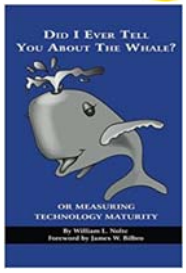
- Datenschutz-Management
  - Regelmäßige Treffen + anlassbezogenes Handeln
  - Mit Sicherheits-Management
  - Ausschreibungen / Beschaffungen in Bezug auf Verarbeitung personenbezogener Daten
    - Kriterien wie Nachweis der Einhaltung der DSGVO, spezifische Anforderungen (z.B. Datenminimierung)
    - Einbindung des bDSB
  - Überprüfung bestehender Verfahren: geht‘s besser?
  - Überprüfung früherer Art. 33-Meldungen
  - Von der Einzelfall-Behandlung zum regulären Prozess
- Wertschätzung des Berichts der/des bDSB: Wahrnehmen & Umsetzen

„Stand der Technik“ entmystifizieren

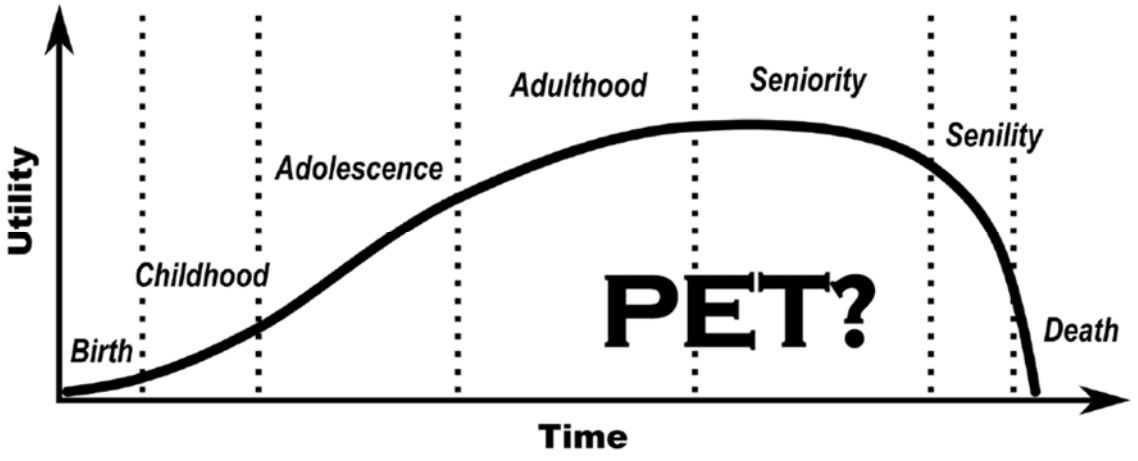
- „Stand der Technik“ kann obere und untere Grenze sein
- „Stand der Technik“ definieren und fortschreiben
- „Technology Readiness Level“ ohne „Quality“ sinnlos: Arbeiten zu „PET Maturity“
- Lücke zwischen Forschung und Praxis, Markt wird auf Nachfrage reagieren
- In (naher?) Zukunft: Übersichten mit Konzepten + Repositories mit Implementierungen



https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/pets (2015)



Technology Maturity



Graphik: ULD

Bsp.: MD5, Windows XP, ...

Anleihe vom BSI (Fokus auf Informationssicherheit)

Standards und Kriterien

Mindeststandard des BSI nach § 8 Abs. 1 Satz 1 BSIG

Das BSI als die nationale Cyber-Sicherheitsbehörde erarbeitet Mindeststandards für die Sicherheit der Informationstechnik des Bundes auf der

Mindeststandards

- SSL/TLS-Protokoll
- Schnittstellenkontrolle
- Sichere Web-Browser
- Nutzung externer Cloud-Dienste

Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG)
§ 8 Vorgaben des Bundesamtes

(1) Das Bundesamt erarbeitet Mindeststandards für die Sicherheit der Informationstechnik des Bundes. Das Bundesministerium des Innern kann im Benehmen mit dem IT-Rat diese Mindeststandards ganz oder teilweise als allgemeine Verwaltungsvorschriften für alle Stellen des Bundes erlassen. Das Bundesamt berät die Stellen des Bundes auf Ersuchen bei der Umsetzung und Einhaltung der Mindeststandards. Für die in § 2 Absatz 3 Satz 2 genannten Gerichte und Verfassungsorgane haben die Vorschriften nach diesem Absatz empfehlenden Charakter.

Anleihe beim BSI: TLS 1.2 (2015)

1. **Bürger-Behörden-Kommunikation:** Wenn Daten zwischen Bundesbehörden und Bürgern übertragen werden (z. B. durch Web-Server und Browser, E-Mail, FTP), müssen die Bestandssysteme bis zum 01.07.2015 migriert sein, sodass die Transportverschlüsselung mit TLS gemäß dieses Mindeststandards unter Beiziehung der TR-03116-4 angeboten wird.
2. **Wirtschaft-Behörden-Kommunikation:** Wenn Daten zwischen Bundesbehörden und der Wirtschaft über ein Fachverfahren übertragen werden, muss das Fachverfahren bis zum 31.12.2016 migriert sein, sodass die Transportverschlüsselung mit TLS gemäß dieses Mindeststandards verwendet wird.
3. **Inter-Behördenkommunikation:** Wenn Daten zwischen zwei oder mehreren Bundesbehörden über ein Fachverfahren übertragen werden, muss das Fachverfahren bis zum 31.12.2016 migriert sein, sodass die Transportverschlüsselung mit TLS gemäß dieses Mindeststandards verwendet wird.
4. **Interne Behördenkommunikation:** Wenn Daten innerhalb einer Bundesbehörde übertragen werden, müssen die Bestandssysteme bis zum 01.07.2017 migriert sein, sodass die Transportverschlüsselung mit TLS gemäß dieses Mindeststandards verwendet wird.

Sollten die Bestandssysteme innerhalb der angegebenen Fristen vollständig oder unter Hinzunahme von Alternativlösungen nicht migriert werden können, sind Abweichungen von diesem Mindeststandard spätestens 8 Wochen vor Ablauf der Migrationsfrist durch die jeweilige Bundesbehörde an das BSI [...] zu notifizieren.

Heute Empfehlung, morgen ein „Muss“!

Bußgeld für Kontaktformulare ohne Verschlüsselung

30. NOVEMBER 2015 | 30 KOMMENTARE | VON DR. DATENSCHUTZ

Aus gegebenen Anlass soll an dieser Stelle noch einmal darauf hingewiesen sein, dass das Bayerische Landesamt für Datenschutzaufsicht derzeit Unternehmen in ihrem Zuständigkeitsbereich dahingehend überprüft, ob deren Webseiten, auf denen Kontaktformulare verwendet werden, anerkannte Verschlüsselungsverfahren implementiert haben. Die Anforderung betrifft aber nicht nur Webseiten mit Kontaktformularen.

Was passiert derzeit?

Das Bayerische Landesamt für Datenschutzaufsicht beanstandet zurzeit Webseiten, die trotz Verwendung von Kontaktformularen, mittels derer personenbezogene Daten elektronisch übertragen werden, keine angemessenen Schutzmaßnahmen wie beispielsweise eine verschlüsselte Datenübertragung implementiert haben.

https://www.datenschutzbeauftragter-info.de/bussgeld-fuer-kontaktformulare-ohne-verschluesselung/ (2015)

3.2 SSL/TLS-Versionen

Das SSL-Protokoll existiert in den Versionen 1.0, 2.0 und 3.0, wobei die Version 1.0 nicht veröffentlicht wurde. TLS 1.0 ist eine direkte Weiterentwicklung von SSL 3.0 und wird in [RFC2246] spezifiziert. Des Weiteren gibt es die Versionen 1.1 und 1.2 des TLS-Protokolls, welche in [RFC4346] und [RFC5246] spezifiziert werden.

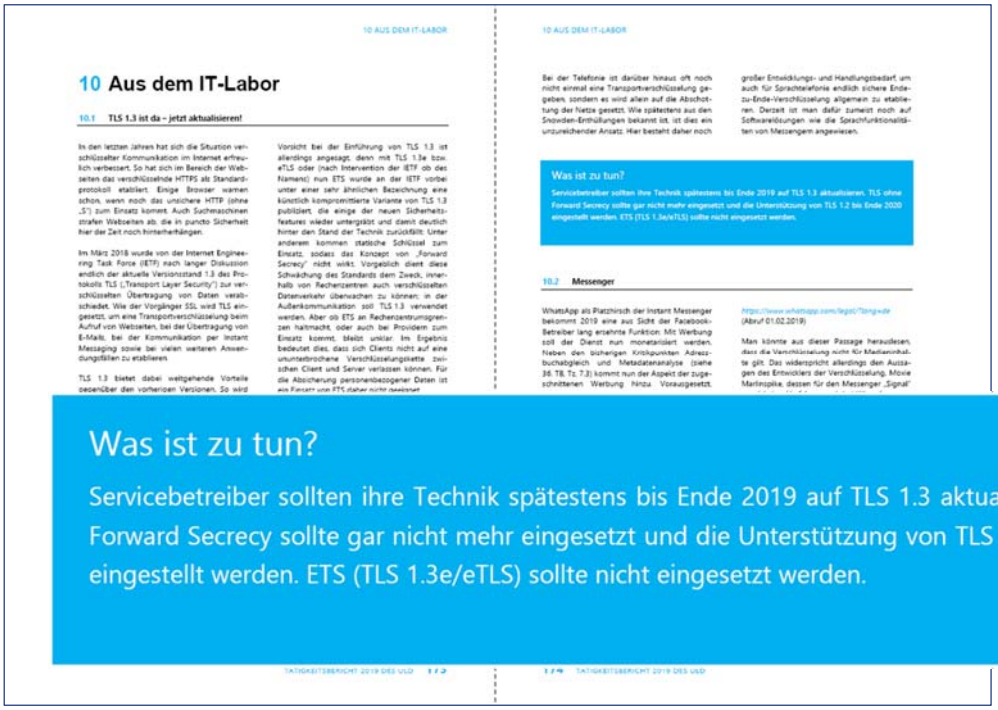
Empfehlungen für die Wahl der TLS-Version sind:

- Grundsätzlich wird TLS 1.2 empfohlen.
- TLS 1.1 wird **nicht mehr empfohlen** (siehe dazu Abschnitt 3.3.2).
- TLS 1.0 wird **nicht empfohlen.**
- SSL v2 ([SSLv2]) und SSL v3 ([SSLv3]) werden **nicht empfohlen** (siehe auch [RFC6176]).

Bundesamt für Sicherheit in der Informationstechnik (BSI) 5

https://www.datenschutzzentrum.de/sdm/

Ansage: zu TLS 1.3 wechseln (Stand 2019)



10 Aus dem IT-Labor

10.1 TLS 1.3 ist da – jetzt aktualisieren!

10.2 Messenger

Was ist zu tun?

Servicebetreiber sollten ihre Technik spätestens bis Ende 2019 auf TLS 1.3 aktualisieren. TLS ohne Forward Secrecy sollte gar nicht mehr eingesetzt und die Unterstützung von TLS 1.2 bis Ende 2020 eingestellt werden. ETS (TLS 1.3e/eTLS) sollte nicht eingesetzt werden.

Tätigkeitsbericht 2019 des ULD S-H, Tz. 10.1: https://uldsh.de/tb37

DSGVO-Compliance mit Art. 25

Bild: Martin Cox

Bild: Paul B

- Überblick über Datenverarbeitung (Art. 30 DSGVO)
- Überblick über Risiken (Artt. 24+25+32, Artt. 33+34, Artt. 35+36 DSGVO)
- Schriftliche Dokumentation der internen Strategien und TOMs
  - Punkte aus Art. 25 + EG 78 durchgehen – inkl. Artt. 32 + 35 DSGVO
  - Prozesse bei Beschaffung – bDSB integrieren
  - Prozesse bei Auftragsverarbeitung – Compliance einfordern
  - Prozesse bei Änderungen – Change Management à la DSGVO
  - Umgang mit Beschwerden – aus Fehlern lernen, vertrauensbildende Maßnahmen
- Interne Überprüfung: geht´s besser? – Datenminimierung (Pseudonymisierung), Transparenz, ...
- Weiterbildung vorsehen – Status Quo + Markt werden sich ändern
- Hilfestellung bei den Datenschutzbehörden erfragen

Vom Minimum zum Optimum

Bild: Martin Cox

Minimum:

- Dokumentation von internen Strategien und Maßnahmen als Nachweis (Art. 5 (2) + Art. 24 DSGVO)
- Gesamtansatz für eingebauten Datenschutz + Sicherheit (Art. 25 + Art. 32 DSGVO)
- Auf Anforderungen der Aufsichtsbehörden reagieren
- Klare Verantwortlichkeit (Vorstand; möglichst unterstützt von betriebl. DSB)

Für „Optimum“ zusätzlich:

Bild: Paul B

- Datenschutz-Management-system für gesamten Lebenszyklus einsetzen
- Proaktiv agieren
- Lösungsraum kennen und erweitern
- Zertifizierung anstreben
- Zu Best Practices + Standardisierung beitragen

Überblick

Bild: athree23 via Pixabay

1. Artikel 25 der DSGVO im Gesamtgefüge der Datenschutzreform
2. „by Design“: Datenschutz richtig einbauen
3. „by Default“: Mehr als das Erforderlichkeitsprinzip
4. Wie geht´s? Vom abstrakten Recht in die konkrete Praxis
5. Fazit

Fazit

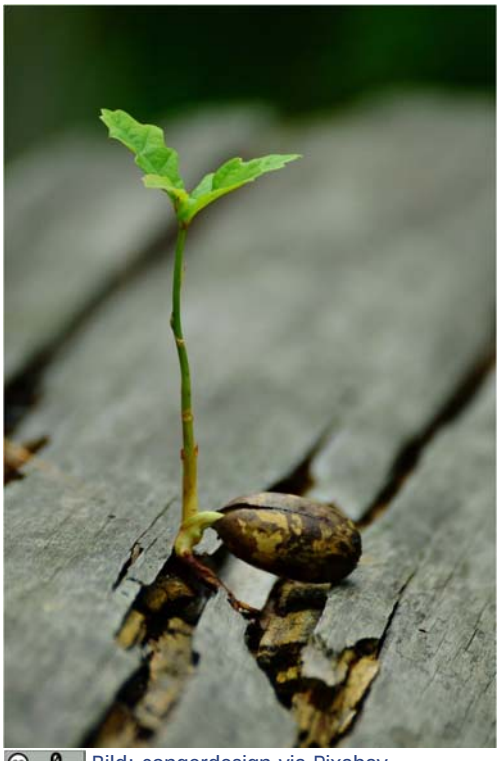


Bild: congerdesign via Pixabay

- „Eingebauter Datenschutz“ zurzeit noch unbefriedigend:
  - Status Quo
  - europarechtlich
  - nationalgesetzlich
- Gestaltung ist mehr als Technik
- Ins Datenschutz-Management integrieren
- Wichtig: kein eingefrorener Stand, sondern dynamischer Prozess


Ich freue mich
auf die Diskussion.