Fokus: „Data Protection by Design and by Default“
(Art. 25 Datenschutz-Grundverordnung)

Privacy by Design

Marit Hansen
Landesbeauftragte für Datenschutz
Schleswig-Holstein

5. DFN-Konferenz Datenschutz
Hamburg, 29.11.2016

forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Überblick

- Datenschutz durch Technikgestaltung: mehr als Datensicherheit
- Anforderungen der EU-Datenschutz-Grundverordnung
- Das Standard-Datenschutzmodell als Kompass für die Praxis
- Systemgestaltung mit Datenschutz: vom Minimum zum Optimum
- Best-Practice-Beispiele
- Fazit

Beim Datenschutz geht es primär um ~~Daten~~

Bild: Ashtyn Renee

Menschen mit ihren Rechten

Prüffragen bei der Gestaltung:

- Auswirkungen auf Menschen?
- Auswirkungen auf die Gesellschaft?

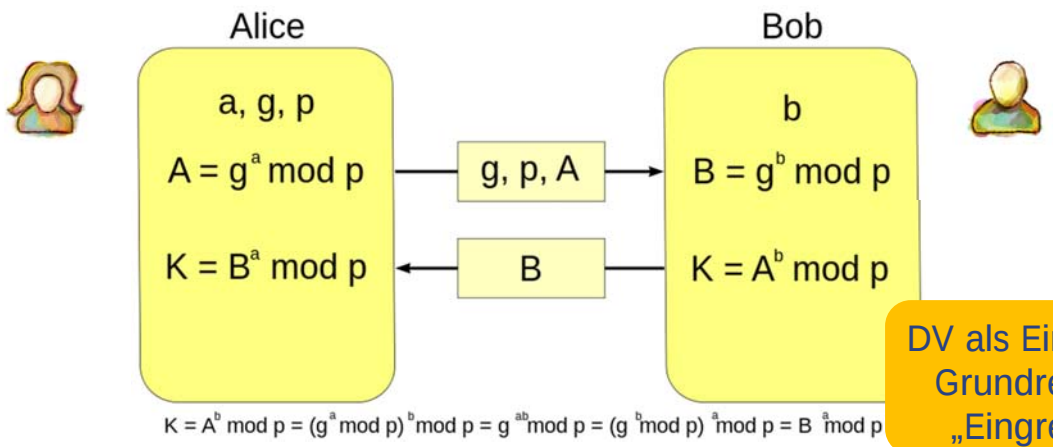
Datenschutz nötig: Machtgefälle

Wichtig: Perspektive der betroffenen Personen

Ansatzpunkt: personen-bezogene Daten

Bild: Azureon2

Perspektive: Alice & Bob



DV als Eingriff in Grundrechte: „Eingreifer“

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

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

Überblick

- Datenschutz durch Technikgestaltung: mehr als Datensicherheit
- Anforderungen der EU-Datenschutz-Grundverordnung
- Das Standard-Datenschutzmodell als Kompass für die Praxis
- Systemgestaltung mit Datenschutz: vom Minimum zum Optimum
- Best-Practice-Beispiele
- Fazit

Datenschutz-Grundverordnung

- Nachfolger der EU-Datenschutz-Richtlinie von 1995
- Konstrukt „Verordnung“: unmittelbar anwendbar
- Anwendungsvorrang gegenüber nationalem Recht
- 70 Öffnungsklauseln (Regelungsaufträge und Regelungsoptionen) für nationalen Gesetzgeber
- Geltung ab 25.05.2018


VERORDNUNGEN

- Marktortprinzip
- One-Stop-Shop:
  einfacher für Verbraucher(innen)
- Kohärenzmechanismus:
  Einigung der Aufsichtsbehörden

Vergleich: „Alle nach unten zum letzten Basislager!“

- EU-Werkzeug Verordnung: eine für alle (eigentlich)
- Gemeinsamer rechtlicher Startpunkt
- Von dort aus Territorium erschließen

Wichtigkeit von „by Design“

Erwägungsgrund 4

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

Datenschutz „by Design“ & „by Default“

- Kommt mit der EU-Datenschutz-Grundverordnung (Art. 25)
- Richtet sich primär an Datenverarbeiter (d.h. „Verantwortliche“ und „Auftragsverarbeiter“)
- Richtet sich nur indirekt an Hersteller von IT-Systemen
- Ziel: Gestaltung von Systemen + Diensten von Anfang an über den gesamten Lebenszyklus
  a) datensparsam
  b) mit möglichst datenschutzfreundlichen Voreinstellungen

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

ULD www.datenschutzzentrum.de

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

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 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 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.

ULD www.datenschutzzentrum.de

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.

Privacy by Design

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 DS-GVO: „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 datenschutzfreundliche Voreinstellungen

Artikel 25 Datenschutz […] 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.

Bsp.: Social Networks

Datenschutz „by Design“ & „by Default“ gemäß Erwägungsgrund 78 DS-GVO

- 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

(78) Zum Schutz der in Bezug auf die Verarbeitung personenbezogener Daten bestehenden Rechte und Freiheiten natürlicher Personen ist es erforderlich, dass geeignete technische und organisatorische Maßnahmen getroffen werden, damit die Anforderungen dieser Verordnung erfüllt werden. Um die Einhaltung dieser Verordnung nachweisen zu können, sollte der Verantwortliche interne Strategien festlegen und Maßnahmen ergreifen, die insbesondere den Grundsätzen des Datenschutzes durch Technik (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) Genüge tun. Solche Maßnahmen könnten unter anderem darin bestehen, dass die Verarbeitung personenbezogener Daten minimiert wird, personenbezogene Daten so schnell wie möglich pseudonymisiert werden, Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten hergestellt wird, der betroffenen Person ermöglicht wird, die Verarbeitung personenbezogener Daten zu überwachen, und der Verantwortliche in die Lage versetzt wird, Sicherheitsfunktionen zu schaffen und zu verbessern. In Bezug auf Entwicklung, Gestaltung, Auswahl und Nutzung von Anwendungen, Diensten und Produkten, die entweder auf der Verarbeitung von personenbezogenen Daten beruhen oder zur Erfüllung ihrer Aufgaben personenbezogene Daten verarbeiten, sollten die Hersteller der Produkte, Dienste und Anwendungen ermutigt werden, das Recht auf Datenschutz bei der Entwicklung und Gestaltung der Produkte, Dienste und Anwendungen zu berücksichtigen und unter gebührender Berücksichtigung des Stands der Technik sicherzustellen, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen. Den Grundsätzen des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen sollte auch bei öffentlichen Ausschreibungen Rechnung getragen werden.

- Ermutigung für Hersteller

- Berücksichtigung in öffentlichen Ausschreibungen

Sicherheit: Art. 32

Maßstab:
- Stand der Technik,
- Implementierungs-kosten,
- Verarbeitung,
- Risiken

Artikel 32

Sicherheit der Verarbeitung

(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 des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

Wieder Pseudonymisierung

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

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

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

Lebenszyklus: regelmäßige Überprüfung

Geldbußen: Art. 83

Bei Art. 25 (Datenschutz durch Technikgestaltung) und Art. 32 (Sicherheit) „kleines“ Bußgeld möglich

Artikel 83

Allgemeine Bedingungen für die Verhängung von Geldbußen

(1) Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 5 und 6 in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

(4) Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:

a) die Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln 8, 11, 25 bis 39, 42 und 43;

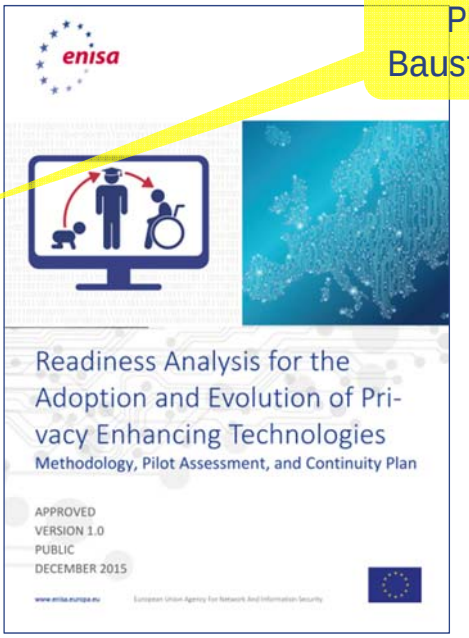
Lösungsansatz: Einsatz von Privacy-Enhancing Technologies (PETs)

“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

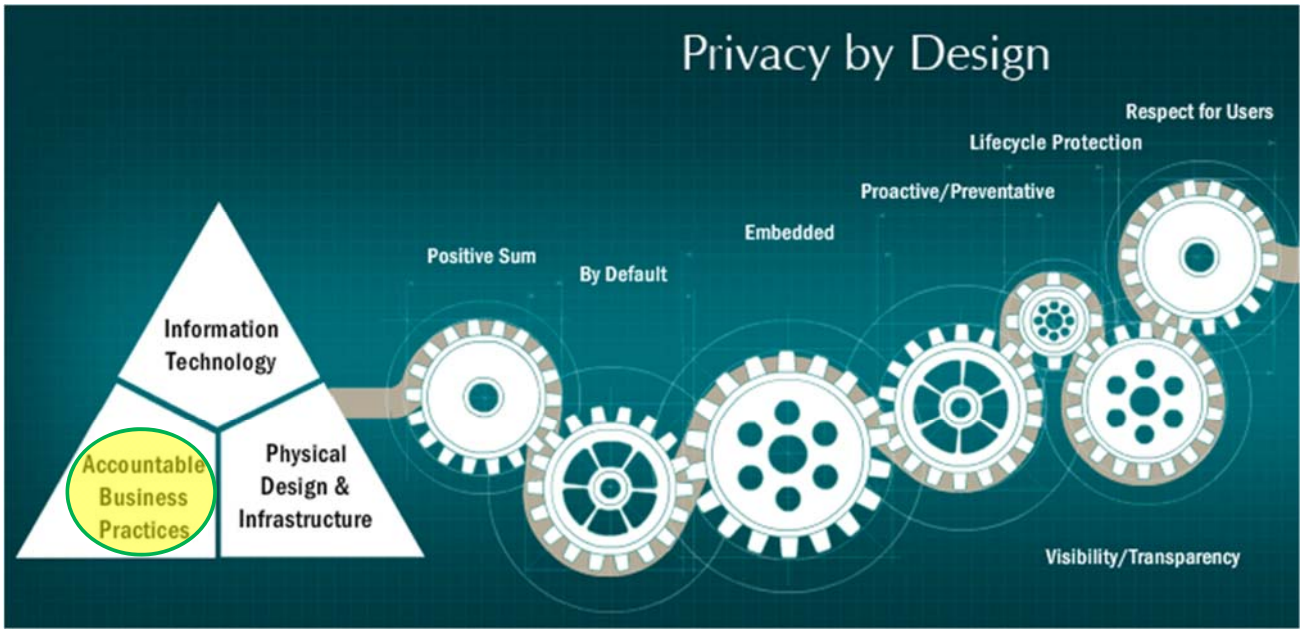
PETs und ihr Reifegrad: State of the Art?

PETs sind ein Baustein der Lösung



https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design (2014)
https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/pets (2015)

Privacy by Design à la Ann Cavoukian



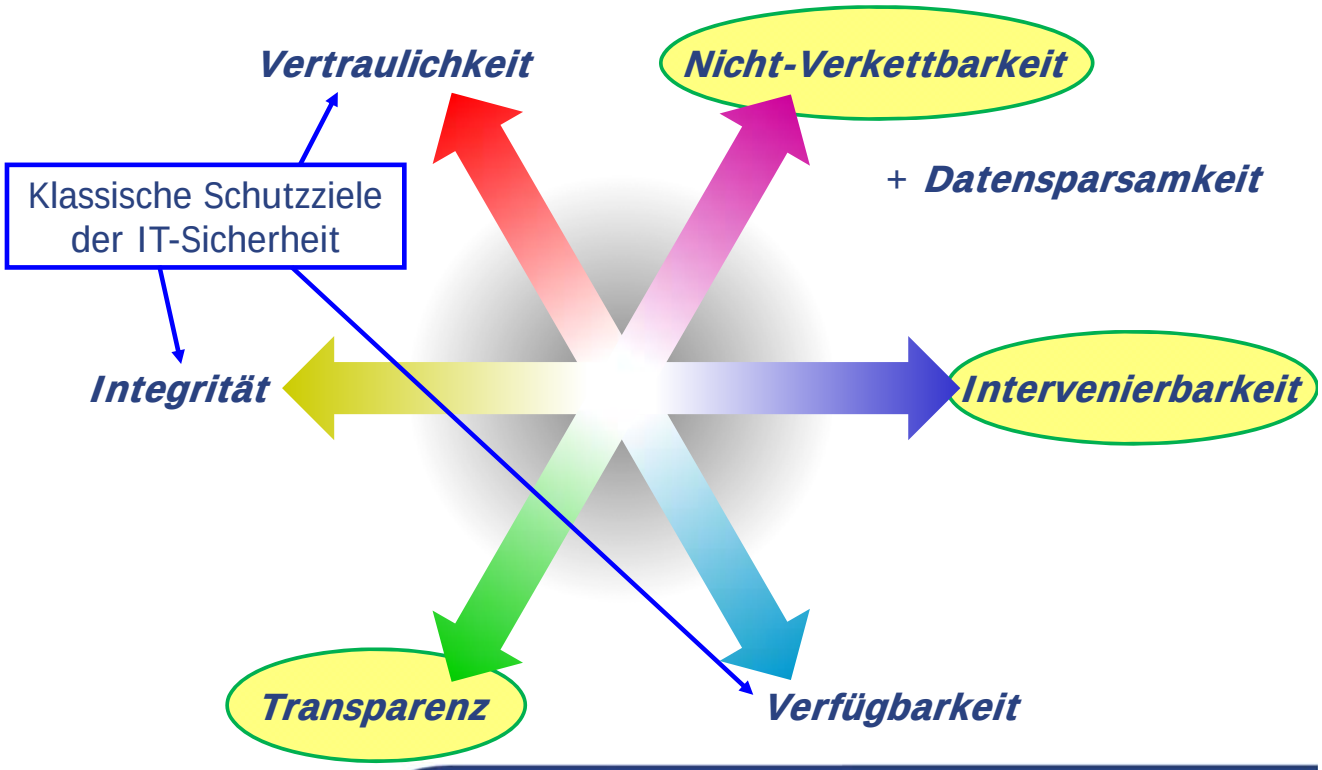
http://privacybydesign.ca/

Überblick

Bild: Margaret W. Carruthers

- Datenschutz durch Technikgestaltung: mehr als Datensicherheit
- Anforderungen der EU-Datenschutz-Grundverordnung
- Das Standard-Datenschutzmodell als Kompass für die Praxis
- Systemgestaltung mit Datenschutz: vom Minimum zum Optimum
- Best-Practice-Beispiele
- Fazit

Gewährleistungsziele



Schutzziele adressieren nicht nur Technik – insbesondere Intervenierbarkeit

- Intervenierbarkeit kaum in Privacy-Engineering-Literatur
- Gründe:
  - Schwer zu formalisieren und zu messen
  - Verglichen mit Forschung zu Datenminimierung sehr viel weniger Techniken und Lösungen
  - Kann oft nicht allein im IT-System gelöst werden
  - Erfordert ein laufendes System mit klaren Verantwortlichkeiten (Betreiber, Nutzer) – nicht auf Prototyp-Ebene
  - Nicht eine fixe Lösung, sondern prozessorientiert für den gesamten Lebenszyklus der Systemevolution

Das Standard-Datenschutzmodell ...

- überführt datenschutzrechtliche Anforderungen in einen Katalog von Gewährleistungszielen,
- gliedert die betrachteten Verfahren in die Komponenten Daten, IT-Systeme und Prozesse,
- berücksichtigt die Einordnung von Daten in drei Schutzbedarfsabstufungen,

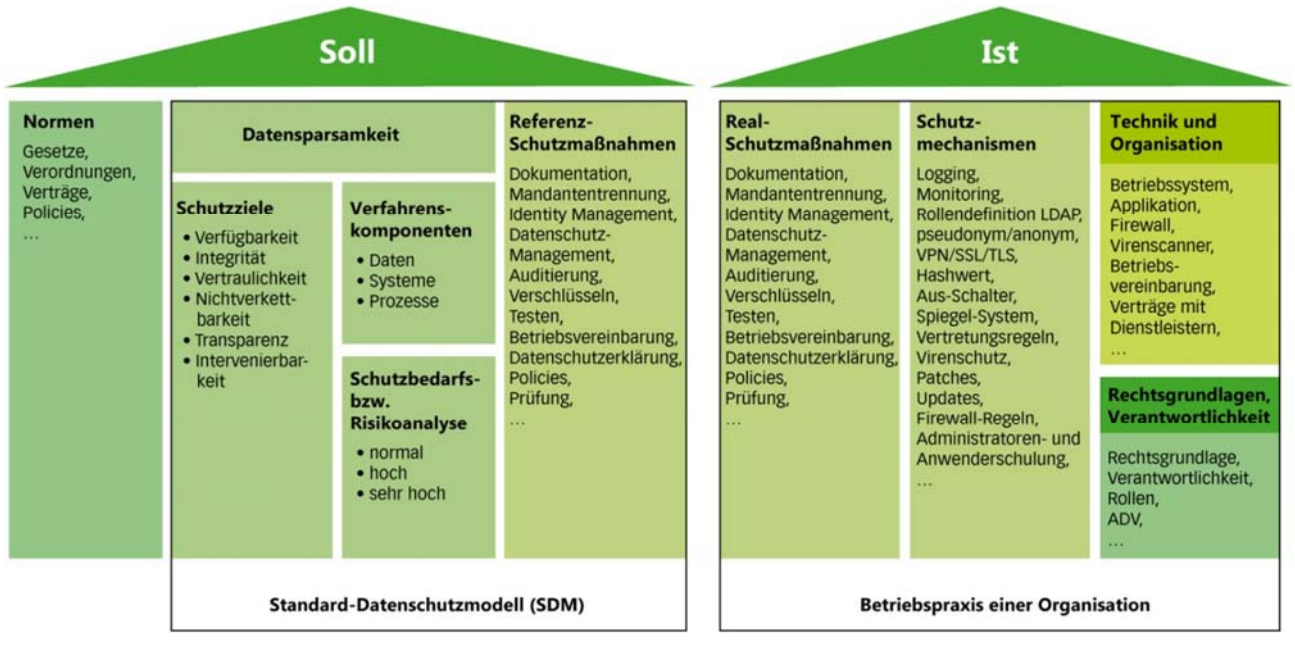
- ergänzt diese um entsprechende Betrachtungen auf der Ebene von Prozessen und IT-Systemen und
- bietet einen hieraus systematisch abgeleiteten Katalog mit standardisierten Schutzmaßnahmen.

https://www.datenschutz-mv.de/datenschutz/sdm/sdm.html

Drei Schutzbedarfsabstufungen im Standard-Datenschutzmodell

- „Normal“: personenbezogene Daten
- „Hoch“:
  - besondere personenbezogene Daten und/oder
  - erhebliche Konsequenzen für betroffene Personen möglich und/oder
  - keine effektiven Interventionsmöglichkeiten
- „Sehr hoch“:
  - „hoch“ plus existenzielle Abhängigkeit der betroffenen Personen und keine Transparenz für sie
- Außerdem Kumulierungseffekte

Soll-Ist-Abgleich gemäß Standard-Datenschutzmodell



Risikobewertung

- Soll-Ist-Abgleich anhand von Referenz-Maßnahmen des Standard-Datenschutzmodells

Schwierig!

- Risk = Impact x Probability

  Übliche Risiko-Formel liefert nur scheinbar objektive Messbarkeit.

$$R = \sum_{k=1}^{n} I_k \times p(I_k)$$

„Risiko für Rechte und Freiheiten natürlicher Personen“

- Perspektive der betroffenen Person
  - Motivation + Mittel der Organisation, den Zweck zu ändern
  - Verarbeitung der Daten in Drittstaaten mit abweichendem Schutzniveau und geringerem Rechtsschutz
  - Konfliktresolution zwischen IT-Sicherheit und Datenschutz

Überblick

Bild: Martin Cox

Bild: Paul B

- Datenschutz durch Technikgestaltung: mehr als Datensicherheit
- Anforderungen der EU-Datenschutz-Grundverordnung
- Das Standard-Datenschutzmodell als Kompass für die Praxis
- Systemgestaltung mit Datenschutz: vom Minimum zum Optimum
- Best-Practice-Beispiele
- Fazit

Systemgestaltung mit Datenschutz

Bild: Martin Cox

Minimum:

- Defensive Interpretation der gesetzlichen Regelungen
- Dokumentation von internen Strategien und Maßnahmen
- Kommende Anforderungen der Aufsichtsbehörden abwarten und darauf reagieren
- Klare Verantwortlichkeit (Vorstand; möglichst unterstützt von betriebl. DSB)

Für „Optimum“ zusätzlich:

Bild: Paul B

- Proaktiv agieren
- Lösungsraum kennen und erweitern
- Zertifizierung anstreben
- Datenschutz-Management-system für gesamten Lebenszyklus einsetzen
- Mit anderen Akteuren und Disziplinen interagieren: Technik und Prozesse

Für umfassendes Privacy-by-Design vielfältige Disziplinen nötig

Bild: Kevin Dooley

- Recht: Zulässigkeit
- Technik: Engineering
- Wirtschaftswiss.:
  - Organisatorische Prozesse
  - Geschäftsmodelle
- Psychologie++: Nutzerinteraktion, Organisationskultur
- Ethik & Sozial- / Politikwissenschaften ...

Überblick

Bild: Josh Hallett

- Datenschutz durch Technikgestaltung: mehr als Datensicherheit
- Anforderungen der EU-Datenschutz-Grundverordnung
- Das Standard-Datenschutzmodell als Kompass für die Praxis
- Systemgestaltung mit Datenschutz: vom Minimum zum Optimum
- Best-Practice-Beispiele
- Fazit

Referenzmaßnahmen des SDM

Schutzziel	Komponente	Maßnahmen
Verfügbarkeit	Daten, Systeme, Prozesse	Redundanz, Schutz, Reparaturstrategien
Integrität	Daten	Hashwert-Vergleich
	Systeme	Einschränkung von Schreibrechten, Integritätsprüfungen
	Prozesse	Festlegung von Referenzwerten (min/max), Steuerung der Regulation
Vertraulichkeit	Daten, Systeme	Verschlüsselung
	Prozesse	Rechte- und Rollenkonzepte

Schutzziel	Kompo-nente	Maßnahmen
Nichtverkettbarkeit ⇨ Zweck-bestimmung	Daten	Anonymität, Pseudonymität, attributbasierte Credentials
	Systeme	Trennung (Isolierung) von Datenbeständen, Systemen und Prozessen
	Prozesse	Identity Management, Anonymitätsinfrastrukturen, Audits
Transparenz ⇨ Prüffähigkeit	Daten	Dokumentation, Protokollierung
	Systeme	Systemdokumentation, Protokollierung von Konfigurationsänderungen
	Prozesse	Dokumentation von Verfahren, Protokollierung
Intervenierbarkeit ⇨ Ankerpunkte	Daten	Zugriff auf Daten für betroffene Personen (Auskunft, Berichtigung, Sperrung, Löschung)
	Systeme	Aus-Schalter
	Prozesse	Helpdesk/einheitlicher Ansprechpartner für Änderungen/Löschungen, Change Management

Best Practice „Datenminimierung“: Authentifikation ohne Identifikation

Vorab Prüfen der Anforderungen:
Welche Daten sind wirklich erforderlich?

Vollständige Daten:

Oft sind nicht alle Daten erforderlich

Minimale Daten:

Symbolbild (nicht belgischer Ausweis)

Best Practice „Datenschutz by Default“

Grundentscheidung:

- Was ist überhaupt vom Nutzer konfigurierbar?

In Social Networks:

- Keine personenbezogenen Daten für alle sichtbar, wenn nicht vom Nutzer aktiv bestimmt
- Bewusste Nutzer-Entscheidung, welche „Friends“ Zugriff haben

Personenbezogenes Tracking:

- Grundsätzlich als Default zu deaktivieren
- Anonyme Analysen möglich

Personalisierte Dienste:

- Nutzer-Entscheidung für Dienst-Nutzung
- Dann Default im Rahmen der Erforderlichkeit

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

ULD www.datenschutzzentrum.de

Überblick

Bild: Rob Pongsajapan

- Datenschutz durch Technikgestaltung: mehr als Datensicherheit
- Anforderungen der EU-Datenschutz-Grundverordnung
- Das Standard-Datenschutzmodell als Kompass für die Praxis
- Systemgestaltung mit Datenschutz: vom Minimum zum Optimum
- Best-Practice-Beispiele
- Fazit

Zusammenfassung: Datenschutz „by …“

Daten-schutz	Was?	Wirklich neu?	Wird es klappen?	Bemerkungen
… by Design	Techn.+org. Maßnahmen für alle Anforderungen aus DS-GVO: optimal „eingebauter Datenschutz“	Nein (§ 3a BDSG), aber bislang kaum durchgesetzt	+ mächtiges Werkzeug – erfordert viel Know-how beim Verantwortlichen und der Aufsichtsbehörde – „Feigenblatt“-Methode möglich: Mini-Schritte und Dokumentation	Hersteller sind nicht Adressat. Wer kümmert sich um Infrastrukturen? Ausschreibungen!
… by Default				

ULD www.datenschutzzentrum.de

Zusammenfassung: Datenschutz „by …“

Daten-schutz	Was?	Wirklich neu?	Wird es klappen?	Bemerkungen
… by Design	Techn.+org. Maßnahmen für alle Anforderungen aus DS-GVO: optimal „eingebauter Datenschutz“	Nein (§ 3a BDSG), aber bislang kaum durchgesetzt	+ mächtiges Werkzeug – erfordert viel Know-how beim Verantwortlichen und der Aufsichtsbehörde – „Feigenblatt“-Methode möglich: Mini-Schritte und Dokumentation	Hersteller sind nicht Adressat. Wer kümmert sich um Infrastrukturen? Ausschreibungen!
… by Default	Primär umgesetztes Erforderlichkeits-prinzip	Teilweise; Durchsetzung war bislang schwierig	+ mächtiges Werkzeug – Effekt kann geschwächt werden durch datenreiche Angebote auf Einwilligungsbasis	Begriff in Art. 25(2) DS-GVO eng definiert, aber mehr Anforderungen ableitbar

Fazit

Bild: Rob Pongsajapan

- Systemgestaltung ist wesentlich für Datenschutz
- Regelungen abstrakt: Aussagen und Hilfsmittel von Aufsichtsbehörden in Sicht
- Prozesse bzgl. „Datenschutz by Design“ jetzt schon evaluieren
- Vorgehen und Entscheidungen dokumentieren
- Aufruf an Entwickler: Lösungen gesucht!!

Vielen Dank für die Aufmerksamkeit!

Marit Hansen
https://www.datenschutzzentrum.de/

forum <privatheit> selbstbestimmtes_leben_in_der_digitalen_welt

ipen

ULD Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein