Anforderungen des Datenschutzes an die (Technik-)Gestaltung

– Impuls –

Marit Hansen
Landesbeauftragte für Datenschutz Schleswig-Holstein

Workshop
„Sichere und datenschutzfreundliche Technik“
Berlin, 07.12.2016

forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Überblick

1. Bisher in Deutschland: § 3a BDSG
2. Neues aus Europa
3. Neues von den deutschen Aufsichtsbehörden: das Standard-Datenschutzmodell
4. Fazit

1. Bisher in Deutschland: § 3a BDSG

§ 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.

2. Neues aus Europa

- Europäische Datenschutz-Reform
  - Art. 25 Datenschutz-Grundverordnung
  - Art. 20 JI-Richtlinie

- eIDAS-Verordnung

VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG

Art. 12 (3) eIDAS-VO

Der Interoperabilitätsrahmen muss folgende Kriterien erfüllen:

[…]

c) er fördert die Umsetzung des Grundsatzes des „eingebauten Datenschutzes“ (privacy by design)

[…]

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

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 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

ULD www.datenschutzzentrum.de

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

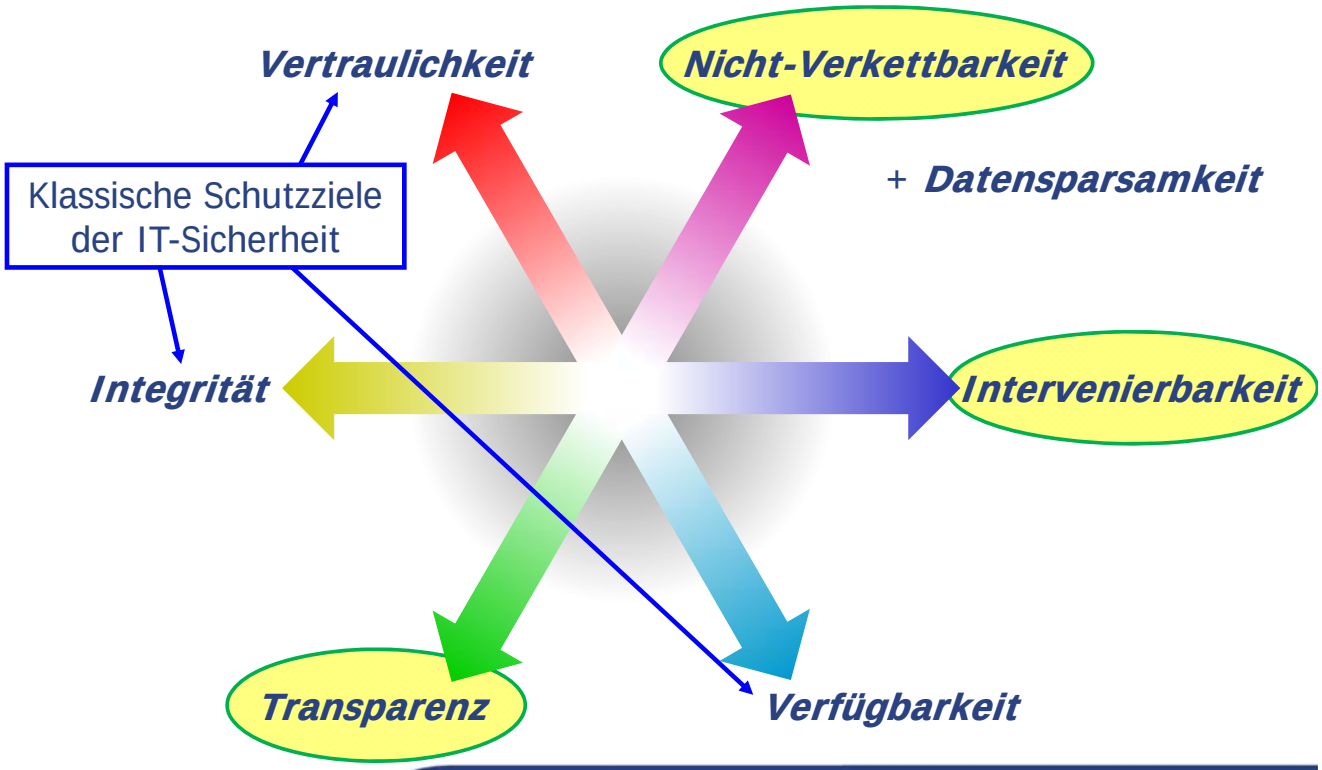
3. Neues von den deutschen Aufsichtsbehörden

Standard-Datenschutzmodell

- Datenschutzrechtliche Anforderungen
  → Gewährleistungsziele
- Personenbezogene Verfahren, bestehend aus Daten, IT-Systemen und Prozessen
- 3 Schutzbedarfsabstufungen für Daten
- Systematisch abgeleiteter Katalog mit standardisierten Schutzmaßnahmen (in Entwicklung)

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

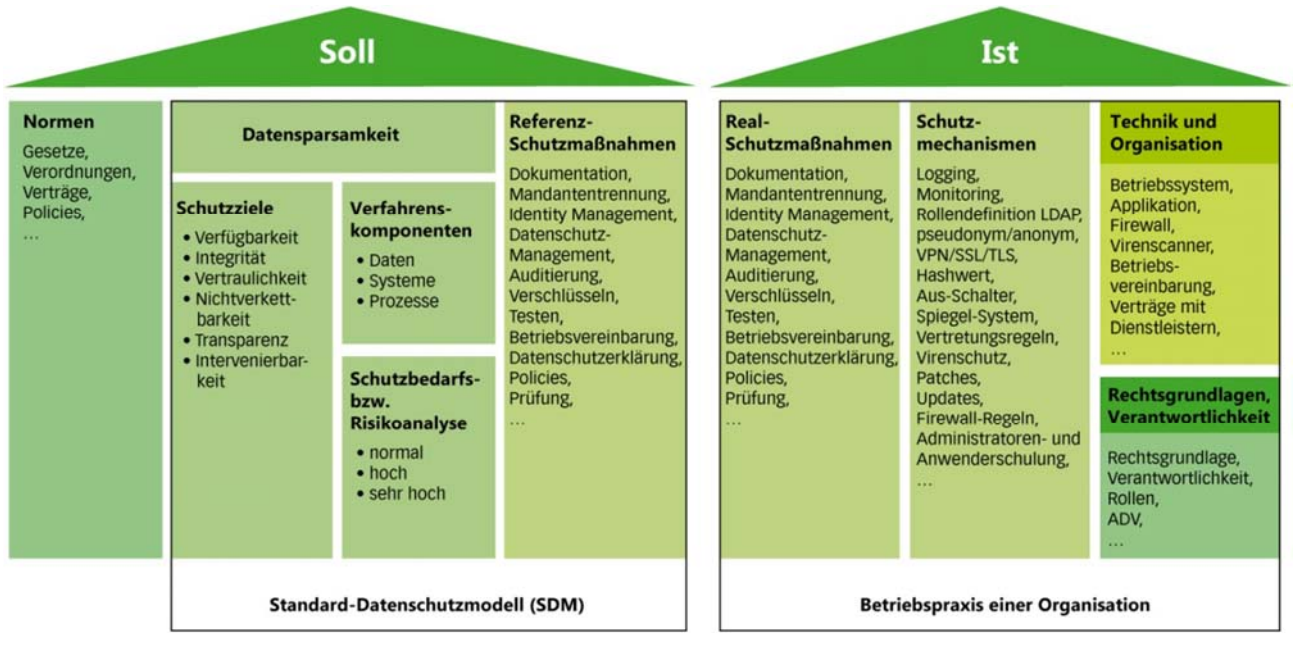
Gewährleistungsziele



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

4. Fazit

- Nicht nur Technikgestaltung
- Vieles nicht neu, aber mittlerweile bessere Chancen auf Realisierung
  - Privacy by Disaster (leider!)
  - Datenschutz-Grundverordnung
- Wichtig: Lösungsraum kennen und erweitern

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