Datenschutz-Werkzeuge „by Design" und „by Default"

Dr. Thomas Probst / Benjamin Raschke

Sommerakademie 2017

Herausforderung
„Informationelle Nichtbestimmung"

18.09.2017, Kiel

Übersicht

1. Rechtliche Grundlagen
2. Data Protection by Design
   a) Zuständigkeit
   b) Software-Entwicklung
      - Strategien
      - Entwurfsmuster
      - Technologien
3. Data Protection by Default
   a) Grundsatzfragen
   b) Grenzen und Beispiele
4. Austausch und Fazit

Privacy oder Data Protection?

- „historischer" Begriff: „Privacy by design" (A. Cavoukian)
- stammt aus dem kanadischen Rechtsraum, der sich am angloamerikanischen Begriff „privacy" (Privatheit) orientiert
- Im europäischen Rechtsraum wird der Begriff „data protection" verwendet.
- Entscheidend ist „by design" bzw. „by default", nicht privacy bzw. data protection.
- Die Begriffe werden daher meist synonym verwendet.

Rechtliche Grundlagen
Data protection by Design

Datenschutz-Grundverordnung – Artikel 25

(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.

Rechtliche Grundlagen
Data protection by Default

Datenschutz-Grundverordnung – Artikel 25

Übersetzungsfehler!

(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.

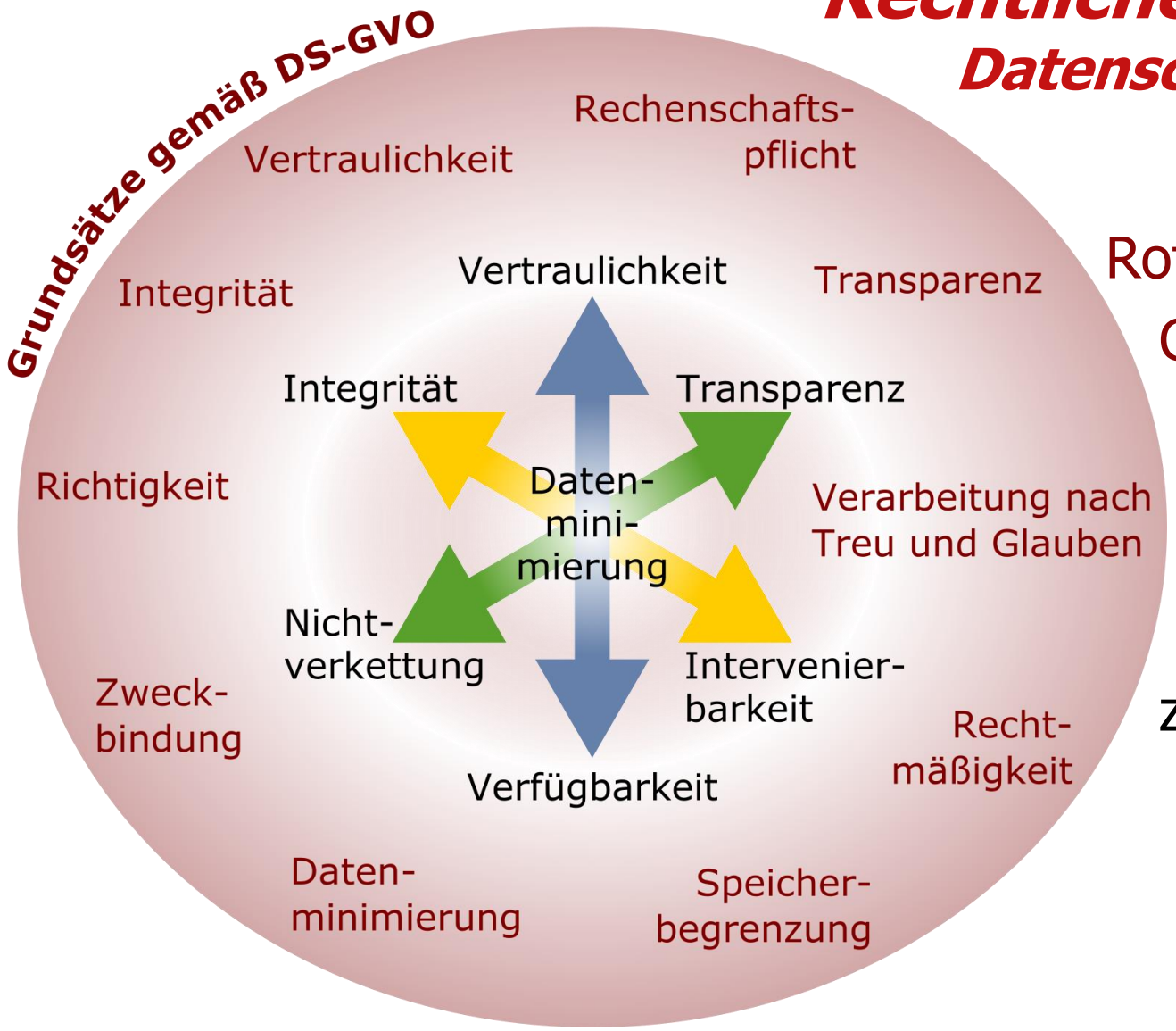
Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen **zugänglich** gemacht werden.

Rechtliche Grundlagen
Zertifizierung

Datenschutz-Grundverordnung – Artikel 25

(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.

Rechtliche Grundlagen
Datenschutzgrundsätze



Rot:

Grundsätze des Artikel 5 DS-GVO

Schwarz: Gewährleistungs-ziele

Data Protection by Design und by Default
Organisation

Wer soll es machen?

- Normadressat ist der **Verantwortliche**.
- Formal sind damit **Hersteller** von Hard-und Software nicht von der Norm betroffen.
- Über Nachfrage der Verantwortlichen nach „Datenschutz by design" und „by default" im Rahmen von Beschaffungen und Beauftragungen schlägt die Anforderung auf Hersteller, Berater, Dienstleister und Auftragsverarbeiter zurück.

Data Protection by Design und by Default
Erwägungsgrund 78 der DS-GVO

In Bezug auf

Entwicklung, **Gestaltung**, **Auswahl** und **Nutzung** von

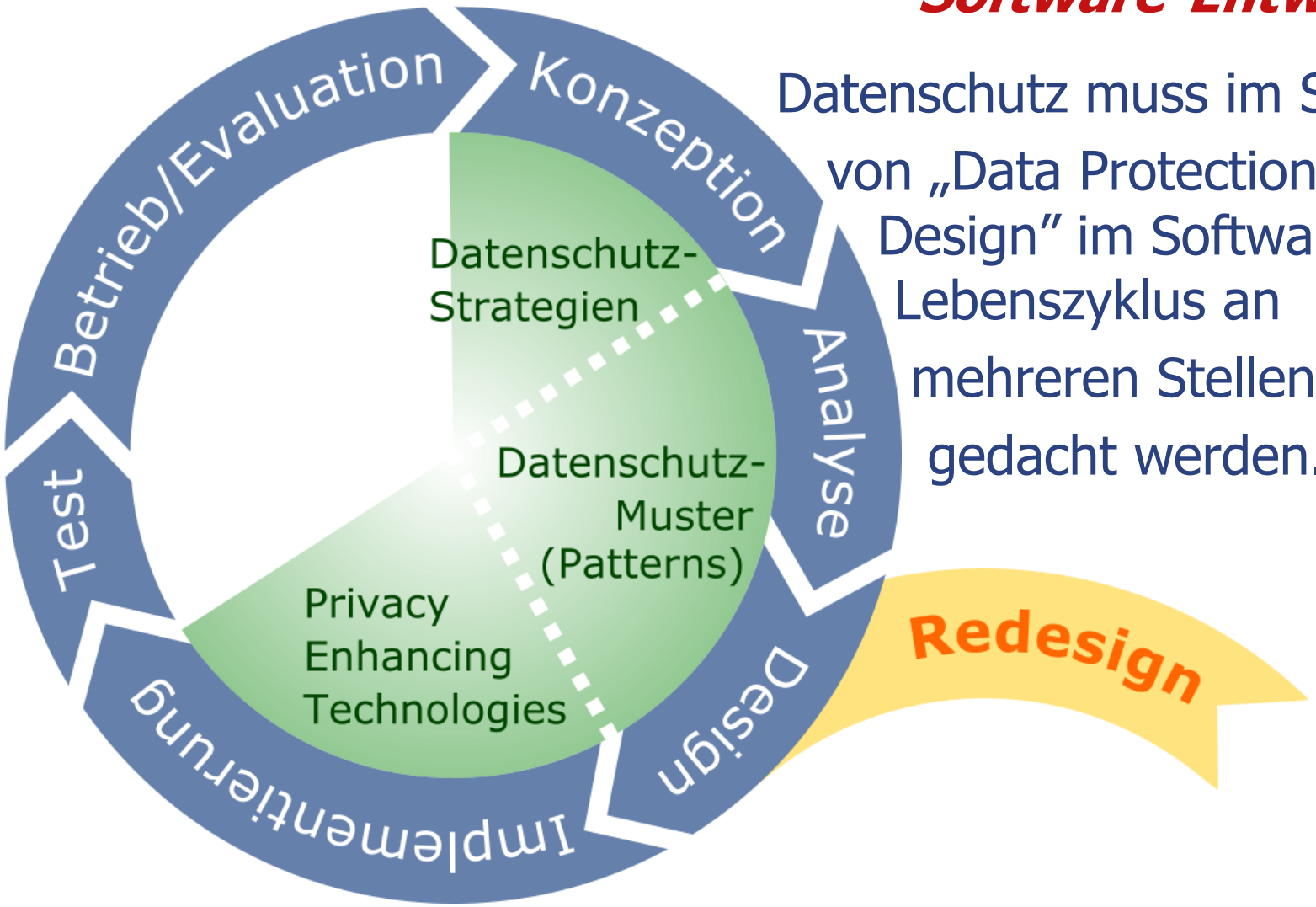
Anwendungen, Diensten und **Produkten**,

die [...] 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.

Data Protection by Design
Software-Entwicklung

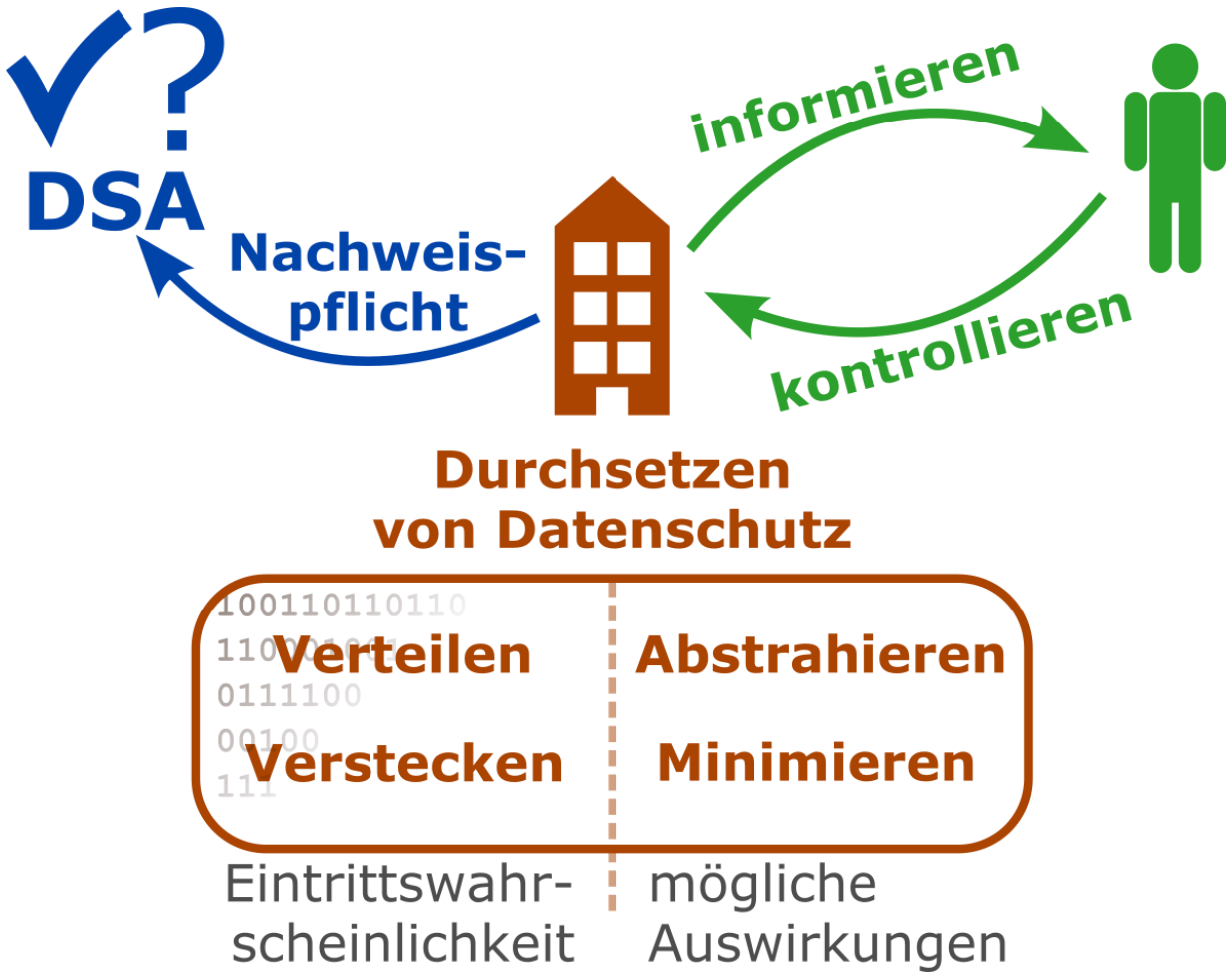


Datenschutz muss im Sinne von „Data Protection by Design" im Software-Lebenszyklus an mehreren Stellen mitgedacht werden.

Data Protection by Design
Software-Entwicklung

Datenschutz-Strategien
(nach Hoepman)

- Minimize
- Hide
- Separate
- Abstract
- Inform
- Control
- Enforce
- Demonstrate



Data Protection by Design
Software-Entwicklung

Datenschutz-Muster (Patterns)

- Entwurfsmuster bieten für wiederholt auftretende Probleme erprobte Konzepte und lassen sich in das Design einfügen.
- Mit Datenschutz-Mustern werden Strukturen angeboten, die den Datenschutz-Strategien folgen und bei „Data Protection by Design" unterstützen.
- Eine Sammlung mit einer Auswahl gibt es auf https://privacypatterns.org/

Data Protection by Design
Software-Entwicklung

Pattern
„Verschlüsselung auf Seite des Nutzers"

😐 Daten werden bei Online-Dienst gespeichert und von diesem verschlüsselt.

→ Verschlüsselung der Daten beim Nutzer.

Beispiele:
Online Backup-Systeme
Online Passwort-Speicher

Pattern
„Meta-Daten löschen"

😐 Nutzern sind (sensible) Meta-Daten oft nicht bewusst, z.B. automatisch generierte Daten.

→ Meta-Daten sofort löschen oder standardmäßig verbergen.

Beispiele:
Twitter und Flickr löschen/ verbergen EXIF-Daten.

Data Protection by Design
Software-Entwicklung

Pattern
„Datenschutz-Verletzungen melden"

😐 Meldungen von Verletzungen des Datenschutzes müssen gemeldet werden, z.B. der Aufsichtsbehörde.

→ Monitoring-System einrichten, das Verstöße erkennt und meldet.

Siehe auch:

ISO/IEC 29100

Pattern
„Erhebung von Nutzdaten einschränken"

😐 Datenübertragung vom Nutzer zur Zentrale kann risikoreich sein.

→ Verarbeitung personenbezogener Daten in vertrauenswürdige Umgebung (eigene Geräte) verlagern.

Beispiel:

Intelligente Wasserzähler

Data Protection by Design
Software-Entwicklung

Beispiele für Privacy Enhancing Technologies

- Verschlüsselung
  Ende-zu-Ende-Verschlüsselung, Forward Secrecy, Let's encrypt
- Anonymisierung in Datenbanken
  k-Anonymität, l-Diversität, Differential Privacy
- Datenschutzerhaltende Berechnungen
  homomorphe Verschlüsselung, Multi-Party Computation
- PET-Werkzeuge auf Nutzer-Seite
  („by design" Kompatibilität sicherstellen, z.B. NoScript)

Data Protection by Default
Datenschutzfreundliche Voreinstellungen

Idee:

Beim „Einschalten“ bzw. nach der Standard-installation soll Verfahren/Programme/Systeme „datenschutzsicher“ sein.

Erforderlichkeit für den Verarbeitungszwecke im Hinblick auf

- Menge
- Verarbeitungsumfang
- Speicherfrist
- Zugänglichkeit

Data Protection by Default
Datenschutzfreundliche Voreinstellungen

Artikel 25 Abs. 2 Satz 3:
„Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden."

- Einzelne Person als Entscheider? Nicht der Verantwortliche?
- Dies ist gemeint:
  englischer Text „without the individual's intervention"
- „Soziale-Netze-Regelung"
- weite Interpretation: auch für Administratoren/Bediener

Data Protection by Default
Wired-in or by default?

Fragestellung bei der Implementierung:

konfigurierbar (+ Defaultwert) oder

fest eingebaut („verdrahtet")?

Beispiel 1:

Webserver:

- nur http (unverschlüsselt)
- http + https (unverschlüsselt + verschlüsselt)
- nur https (verschlüsselt, http wird automatisch zu https)

- Einfluss von Dritten: Ranking bei Suchmaschinen

Data Protection by Default
Wired-in or by default?

Beispiel 2:

Browserkonfiguration

- http-Aufrufe automatisiert durch https-Aufrufe ersetzten
  (z.B. "https everywhere"-Plugin)
- standardmäßige Installation von Browsern mit solchem Plugin ?

Data Protection by Default
Grenzen?

Problemfelder

- Ist eine Anwendung möglicherweise völlig unbenutzbar, wenn sie "per default" keinerlei Daten verarbeitet?
- Ist eine Konfiguration mit unbegrenzter Datenverarbeitung dann nur einen Mausklick entfernt?

Technische Lösung:

- Konfigurationsprofile mit Konfigurationen für typische Anwendungsfälle

Beispiele:

- Standard-Regelsätze für Firewalls
- Gruppenrichtlinien-Sätze für Serverhärtung und Konfiguration

Beispiele für den Einsatz
Das Zertifikatsprotokoll OCSP

Gültigkeitsprüfung von (SSL/TLS)-Zertifikaten

- früher: Sperrlisten (Certificate Revocation Lists, CRL) mit zeitlichem Verzug zur Offline-Nutzung
- derzeit: Online-Überprüfung der Zertifikate mit OCSP

  (Online Certificate Status Protocol)

  Problem: Zertifizierungsstelle erfährt von jeder Zertifikatsprüfung (und damit von allen Webseitenaufrufen bzw. Signaturprüfungen)
- ein Lösungsweg: OCSP-Stapeling
  Webserver erhalten von der Zertifizierungsstelle signierte und zeitlich begrenzt gültige Echtheitsnachweise, die sie mit abgerufenen Webseiten ausliefern

Austausch und Fazit

- Welche Erfahrungen gibt es mit dem Anspruch „Data Protection by Design and by Default”?
- Wo ist besonderer Bedarf an Werkzeugen, Anleitungen, …?
- Gibt es schon Ideen oder Pläne zur Umsetzung von Datenschutz „by design” oder „by redesign”?

Vielen Dank