

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

Benjamin Raschke

CAU, Wintersemester 2017/18

Modul „Datenschutz“

29.11.2017, Kiel



Begrüßung und Vorstellung

Vortragender:

Benjamin Raschke, Informatiker, ULD

Zuständigkeit: Analyse und Bewertung von Konzepten und Techniken zur Umsetzung datenschutzrechtlicher Anforderungen in den Bereichen „Data protection by design“ und Data protection by default“

Kontakt:

ULD35@datenschutzzentrum.de

+49 431 988-1395

Übersicht

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

Übersicht des Vortrags

Wir beginnen mit einem kurzen Überblick über die rechtlichen Grundlagen und was wir unter „Data Protection by Design“ und „Data Protection by Default“ verstehen.

Wir diskutieren Maßnahmen und Werkzeuge – insbesondere für die Software-Entwicklung, an die sich der „by Default“-Ansatz richtet.

Im Anschluss präsentiere ich Überlegungen und Beispiele für den „by Default“-Ansatz und wir diskutieren verschiedene Szenarien.

Im Vortrag haben wir genug Zeit für Diskussionen und gerne auch Erfahrungsberichte aus dem Publikum.

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.

Begriffsbestimmung

Der Begriff „Privacy by design“ wurde von Ann Cavoukian geprägt. In den 90ern prägte sie das Konzept, für das sie sieben Grundprinzipien aufstellte (darunter „Privacy by Default“), und auf ihre Arbeit wird heute noch häufig Bezug genommen:

<https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf>

Die unterschiedlichen Denkweisen des Schutzes der Privatsphäre (privacy) bzw. des Datenschutzes (data protection) führen in den meisten Fällen zu den gleichen Ergebnissen. Die erste Denkweise eines „Privatsphäre-Schutzes“ ist eher im US-amerikanischen Raum vertreten, während in Europa eher der „Datenschutz“ vertreten wird.

Im Folgenden nutzen wir hauptsächlich den Begriff „Data Protection“.

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.

Die rechtliche Grundlage in der Datenschutz-Grundverordnung (DS-GVO)

[EU-Datenschutzgrundverordnung](#) (deutsch)

[EU-General Data Protection Regulation](#) (englisch)

- **Wichtig:** Die Deutsche Übersetzung ist mangelhaft – bspw. beim Titel des Artikels 25
 - deutsch:
Artikel 25: Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen
 - englisch:
Article 25: Data protection by design and by default
- Absatz 1 betrifft die Anforderung „Data Protection by Design“ und der Satz kann in drei Sinn-Abschnitte unterteilt werden
 - (rot) Zu berücksichtigende Rahmenbedingungen für die Anforderung, d.h. Abschätzung von Kosten, Aufwand und Risiko
 - (blau) Die Anforderung muss in der Planung und in der Durchführung berücksichtigt werden
 - (grün) Es müssen organisatorische und technische Maßnahmen ergriffen werden.

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.

Die rechtliche Grundlage in der Datenschutz-Grundverordnung (DS-GVO)

- Wichtig: Auch hier gibt es einen Übersetzungsfehler – das einschränkende Wort „grundsätzlich“ gibt es nur in der deutschen Übersetzung
- In Absatz 2 wird die Anforderung „Data Protection by Default“ beschrieben, ebenfalls unterschieden in drei Sinnabschnitte
 - (schwarz) Durch die Voreinstellungen muss ein möglichst hohes Datenschutz-Niveau gewährleistet werden
 - (dunkelrot) Dies gilt für alle Aspekte der Datenverarbeitung.
 - (grün) Es müssen technische und organisatorische Maßnahmen ergriffen werden.

Rechtliche Grundlagen Zertifizierung

Datenschutz-Grundverordnung – Artikel 25

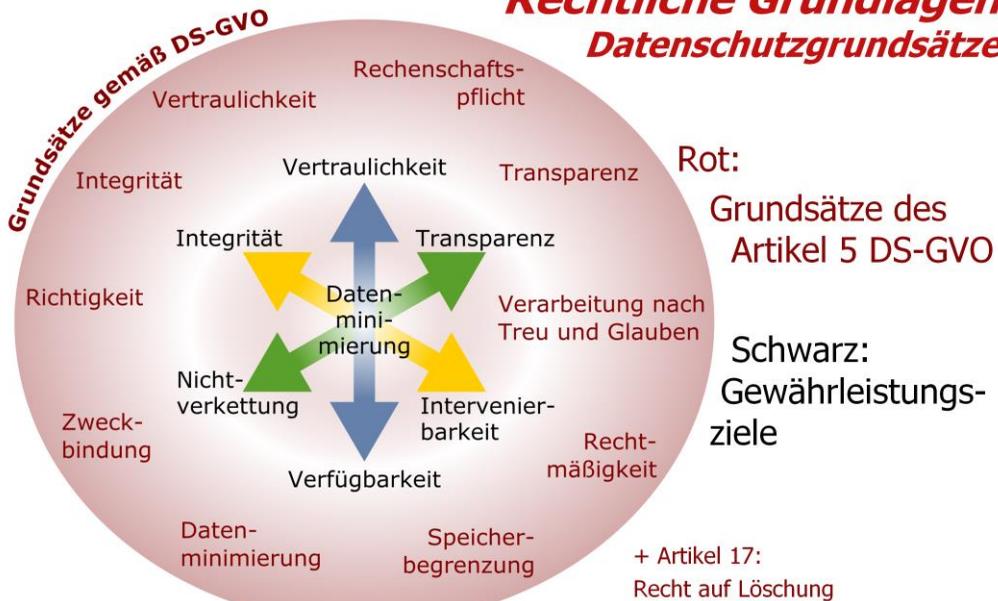
- (3) Ein **genehmigtes Zertifizierungsverfahren** gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in den Absätzen 1 und 2 des vorliegenden Artikels genannten Anforderungen **nachzuweisen**.

Die rechtliche Grundlage in der Datenschutz-Grundverordnung (DS-GVO)

In Zertifizierungsverfahren im Sinne der DS-GVO kann die Erfüllung der Anforderungen „Data Protection by Design“ und „Data Protection by Default“ nachgewiesen werden.

Konkret heißt das aber auch, dass der Nachweis dieser Anforderungen nicht ohne weiteres durch die Erfüllung anderer Normen (z.B. ISO, DIN) oder eigenständiger Siegel ohne DS-GVO-Bezug geführt werden kann.

Rechtliche Grundlagen Datenschutzgrundsätze



Die Grundsätze des Datenschutzes

Die Datenschutzgrundsätze der DS-GVO findet man in Artikel 5. Sie sind in der Grafik rot geschrieben. Hinzu kommt noch das „Recht auf Löschung“ (auch: Recht auf Vergessenwerden) in Artikel 17.

In Fachkreisen wurden in den letzten Jahren die Datenschutz-Gewährleistungsziele entwickelt, die zusammen mit dem Prinzip Datenminimierung ein theoretisches Fundament bilden.

Die Datenschutzgrundsätze der DS-GVO und die Gewährleistungsziele + Datenminimierung lassen sich gut ineinander überführen.

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.

Grundsatzfrage von „Data Protection by Design“: Wer soll es machen?

Artikel 25, Absatz 1

„Unter Berücksichtigung [...] trifft der Verantwortliche [...] geeignete technische und organisatorische Maßnahmen [...].“

(siehe Folie 4)

Die DS-GVO richtet sich in diesem Punkt klar an die Verantwortlichen, nicht an die Herstellerinnen und Hersteller.

Die Herstellerinnen und Hersteller von Software (die eigentlich „Data Protection by Default“ umsetzen müssten) können also nur auf dem Umweg adressiert werden.

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.

Wie sollen „Data Protection by Design“ und „Data Protection by Default“ denn umgesetzt werden?

Im Erwägungsgrund 78 der DS-GVO für den Artikel 25 werden einige Hinweise zur Umsetzung gegeben:

- Wann?
(hellblau) Die Anforderungen „Data Protection by Design“ und „Data Protection by Default“ müssen immer mit bedacht werden: Bei der Auswahl von Software, der Entwicklung, der Gestaltung und auch bei der Nutzung. Explizit wird erwähnt, dass man diese Anforderungen schon in öffentlichen Ausschreibungen berücksichtigen kann.
- Was?
(dunkelrot) Sofern personenbezogene Daten verarbeitet werden – das heißt in allen Anwendungen, Diensten und Produkten.
- Wer?
(dunkelblau) Neben den Verantwortlichen werden auch die Herstellenden erwähnt, die besonderen Einfluss auf die Entwicklung und Gestaltung haben (grün).

Eine rechtliche Verpflichtung, bei öffentlichen Ausschreibungen den Anspruch „Data Protection by Design and by Default“ vorzuschreiben gibt es bisher leider noch nicht.

Data Protection by Design Software-Technik

"Software engineering is the systematic application of scientific and technological knowledge, methods, and experience to the design, implementation, testing, and documentation of software."

IEEE Systems and software engineering – Vocabulary

Wachsende Komplexität der Software-Entwicklung erfordert methodisches, arbeitsteiliges Vorgehen:

- Anforderungsanalyse
- Entwurf und Entwicklung der Software
- Organisation und Strukturierung der Entwicklung, Projektmanagement
- Qualitätssicherung
- Betrieb und Wartung

Software-Technik / Software engineering

In der zweiten Hälfte des 20. Jahrhunderts haben einzelne Software-Projekte eine Größe und Komplexität erreicht, dass sie nicht mehr ohne Hilfsmittel geplant und gesteuert werden konnten.

Deshalb hat sich das (Forschungs-)Gebiet der Software-Technik entwickelt, auf dem Methoden und Techniken entwickelt werden, um Software planbar und sicher zu entwickeln und komplexen Anforderungen an Software gerecht zu werden.

Da die Anforderung „Data Protection by Design“ eine solch komplexe Anforderung ist, soll in Kürze in die Software-Technik eingeführt werden.

Data Protection by Design Software-Technik

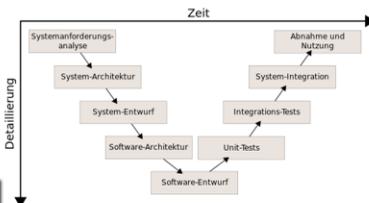
Beispiele für Vorgehensmodelle:



Wasserfallmodell

Ziele: Abgrenzung von Phasen, klare Kostenabschätzung

Grafik: Paul Hoadley, Paul Smith and Shmuel Csaba Otto Traian, CC BY-SA 3.0, <https://commons.wikimedia.org/w/index.php?curid=29119277>



V-Modell

Ziele: weniger Risiken, Qualitätssicherung (Validieren und Verifizieren)

Grafik: Von Michael Pätzold, S. Seyfert - Eigenes Werk (Originaltext: Selbst erstellt), CC BY-SA 3.0, <https://commons.wikimedia.org/w/index.php?curid=31080279>



Agile Software-Entwicklung

Ziele: flexibel, schnell
Beispielsweise Extreme Programming oder Scrum

Grafik: Paul Hoadley, Paul Smith and Shmuel Csaba Otto Traian, CC BY-SA 3.0, <https://commons.wikimedia.org/w/index.php?curid=29119277>

Vorgehensmodelle

Vorgehensmodelle dienen dazu, die Planung und Entwicklung von Software zu strukturieren und dadurch zu verbessern.

Neben den beispielhaft aufgeführten Vorgehensmodellen gibt es etliche mehr, wie beispielsweise Prototyping, Spiralmodell, iterative oder inkrementelle Vorgehensmodelle. Teilweise können diese auch miteinander kombiniert werden.

Das Wasserfallmodell ist ein relativ frühes Vorgehensmodell und dient im Wesentlichen der Abgrenzung von einzelnen Phasen des Entwicklungsprozesses.

Das V-Modell wurde entwickelt, um noch besser sicherzustellen, dass neben der Entwicklung auch die Qualitätssicherung einbezogen wird.

Zur Gruppe der Agilen Software-Entwicklung gehören verschiedene Vorgehensweisen wie z.B. Extreme Programming oder die Scrum-Methode. Der Agilen Software-Entwicklung ist gemein, dass sie prinzipiell auf Flexibilität und keine konkreten Vorfestlegungen setzen. Bei komplexen Anforderungen wie „Data Protection by Design“ muss dabei sichergestellt werden, dass sie den ganzen Prozess über nicht aus dem Blick verloren werden.

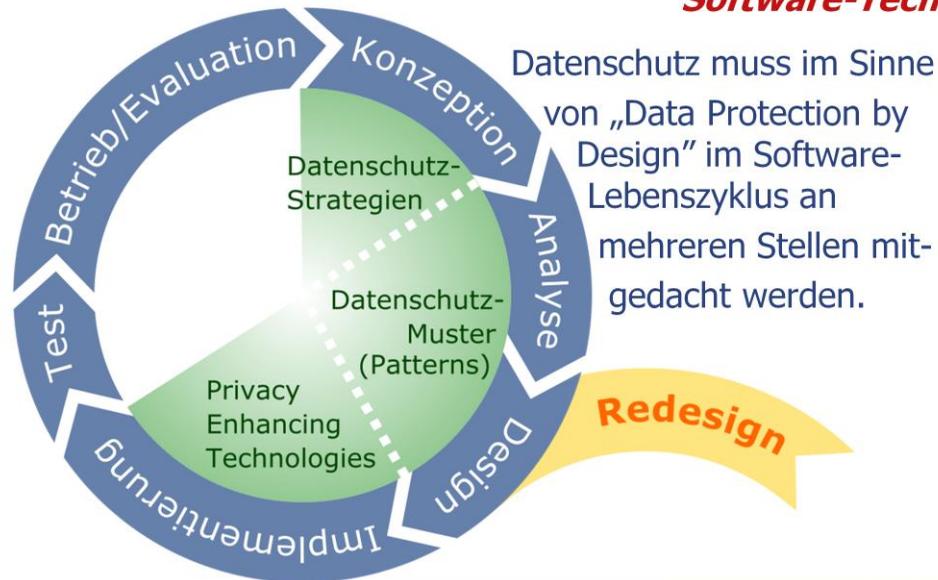
Data Protection by Design ***Software-Technik***

Diskussion

- Wie kann die Anforderung *Data Protection by Design* in dem Prozess der Software-Entwicklung berücksichtigt werden?
 - Welche Erfahrungen haben Sie in Software-Projekten gemacht, wie könnte man *Data Protection by Design* in solchen Prozessen umsetzen?
- 

Software-Technik - Diskussion

Data Protection by Design Software-Technik



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

13

„Data Protection by Design“ in der Software-Entwicklung

Eine klassische Sicht auf Software-Entwicklung ist die (zyklische) Aufteilung nach Phasen. Die folgenden Überlegungen können auch auf verschiedene Entwurfsstrategien (einfach: Wasserfall, V-Modell; komplexer: Agile Programming, DDD) übertragen werden.

„Data Protection by Design“ als begleitenden Prozess der Software-Entwicklung wollen wir hier in drei Phasen unterteilen:

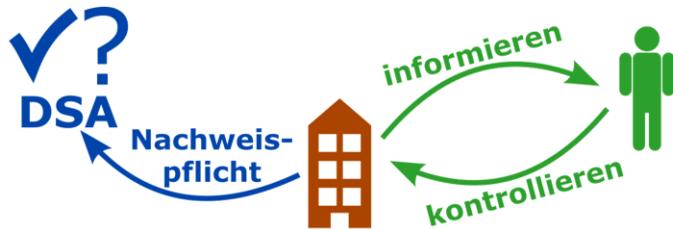
- Datenschutz-Strategien (privacy strategies)
- Datenschutz-Muster (privacy patterns)
- Konkrete Datenschutztechnologien (Privacy Enhancing Technologies)

Die Perspektive eines „Redesigns“ darf dabei nicht aus den Augen verloren werden, denn an vielen Stellen kann es effektiver sein, vorhandene Software zu überarbeiten.

Data Protection by Design Software-Technik

Datenschutz-Strategien (nach Hoepman)

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



Durchsetzen von Datenschutz



Datenschutz-Strategien

Jaap-Henk Hoepman hat acht Datenschutz-Strategien herausgearbeitet:

- Minimieren von Daten, z.B. durch Nichterheben oder Löschen
- Verstecken, z.B. durch Pseudonymisierung, Mischen
- Verteilen von Daten, physisch oder logisch um Verkettbarkeit zu erschweren
- Abstrahieren, z.B. Daten gruppieren oder generalisieren
- Informieren, d.h. Personen über Datenerhebung und –verarbeitung informieren
- Kontrolle, d.h. Recht auf Löschen bzw. Bearbeitung
- Durchsetzen der (rechtlichen) Anforderungen
- Nachweisen der Einhaltung von rechtlichen Vorgaben und der getroffenen Maßnahmen

Die Strategien *Verteilen* und *Verstecken* dienen dazu, die Eintrittswahrscheinlichkeit von Datenschutzverstößen zu verringern, die Strategien *Abstrahieren* und *Minimieren* zielen darauf ab, dass die möglichen Auswirkungen gering sind.

Quelle: <http://www.cs.ru.nl/~jhh/publications/iwpe-privacy-strategies.pdf>

Data Protection by Design Software-Technik

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/>

Datenschutz-Muster (privacy patterns)

In der Software-Entwicklung werden immer wieder Entwurfsmuster (design pattern) benutzt, da sie als Lösungs-Schablonen für immer wieder auftauchende Entwicklungsprobleme genutzt werden können.

Bekannte Entwurfsmuster sind

- Model-View-Controller (Trennung von Daten, Ansicht und Verarbeitung)
- Observer (Weitergabe von Änderungen an einem Objekt)
- Factory (Erzeugen eines Objekts durch Aufrufen einer Methode)

Die Datenschutz-Muster folgen den Datenschutz-Strategien und bieten Lösungsansätze für typische Probleme.

Die Sammlung von Mustern auf www.privacypatterns.org ist bei weitem nicht vollständig, bietet aber einen guten ersten Überblick.

Ergänzend kann auch ein Blick auf Anti-Pattern helfen, um überhaupt Datenschutz-Risiken zu erkennen. Nick Doty und Mohit Gupta haben hierzu ein Paper geschrieben:

https://cups.cs.cmu.edu/soups/2013/trustbusters2013/Privacy_Design_Patterns-Antipatterns_Doty.pdf

Data Protection by Design Software-Technik

Pattern

„Verschlüsselung auf Seite des Nutzers“

☺ Problem:

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

→ Lösung:

Verschlüsselung der Daten auf dem Nutzungsgerät
(Schlüssel bleiben im persönlichen Besitz).



Beispiele:

Online Backup-Systeme
Online Passwort-Speicher

Strategien:
Verteilen, Verstecken

„Verschlüsselung auf Nutzer-Seite“ / „Encryption with user-managed keys“

Problem: Das Speichern von personenbezogenen Daten soll bei Online-Diensten oft verschlüsselt erfolgen, um den Schaden im Fall eines Datenlecks gering zu halten.

Lösungsidee: Die Verschlüsselung erfolgt bereits auf Seite des Nutzers, sodass nicht das Problem entsteht, dass verschlüsselte Daten und Schlüssel am selben Ort zu finden sind.

Berücksichtigte Strategien: Verteilen, Verstecken

Beispiele: Online-Backups, die vor der Übertragung verschlüsselt werden.

<https://privacypatterns.org/patterns/Encryption-user-managed-keys>

Data Protection by Design Software-Technik

Pattern

„Meta-Daten löschen“

☹ Problem:

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

→ Lösung:

Meta-Daten sofort löschen oder standardmäßig verbergen.



Beispiele:

Twitter und Flickr löschen/ verbergen EXIF-Daten.

Strategien:

Minimieren, Verstecken, Kontrolle

„Meta-Daten löschen“ / „Strip invisible Metadata“

Problem: Bei der Nutzung von digitalen Geräten fallen oft diverse Meta-Daten an, von denen die meisten unbemerkt verarbeitet werden und der Nutzer nur durch besondere Fachkenntnis von der Existenz erfährt.

Lösungsidee: Sofern die Meta-Daten nicht benötigt werden, werden sie gelöscht oder standardmäßig vor Dritten verborgen.

Berücksichtigte Strategien: Minimieren, Verstecken, Kontrolle

Beispiele:

EXIF-Daten von Bild-Dateien (z.B. Datum/Uhrzeit als ein Foto aufgenommen wurde) werden von Twitter beim Hochladen gelöscht und bei Flickr können sie verborgen werden, sodass Dritte sie nicht sehen können.

<https://privacypatterns.org/patterns/Strip-invisible-metadata>

Data Protection by Design Software-Technik

Pattern

„Datenschutz-Verletzungen melden“

☹ Problem:

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

→ Lösung:

Monitoring-System einrichten, das Verstöße erkennt und meldet.

✦ *Noch sehr theoretischer Ansatz, keine Umsetzung bekannt.*



Siehe auch:

ISO/IEC 29100

Strategien:

Informieren, Nachweispflicht

„Datenschutz-Verletzungen melden“ / „Data Breach Notification Pattern“

Problem: Beispielsweise bei unbefugtem Zugriff auf Daten muss (innerhalb einer gewissen Frist) informiert werden – bspw. das beauftragende Unternehmen, die betroffenen Personen oder eine Aufsichtsbehörde (siehe Artikel 33 DS-GVO).

Lösungsidee: Ein Monitoring-System protokolliert Zugriffe auf Daten und sofern ein Verstoß nicht sofort verhindert aber (nachträglich) erkannt wird, meldet es die Verstöße an die vorab definierten Adressaten.

Berücksichtigte Strategien: Informieren, Nachweispflicht

<https://privacypatterns.org/patterns/Data-breach-notification-pattern>

[Modellierung von Sigrid Gürgens \(SIT/Fraunhofer\)](#)

Data Protection by Design Software-Technik

Pattern

„Erhebung von Nutzdaten einschränken“

- ☺ Problem:
Datenübertragung vom Nutzungsgerät zur Zentrale kann risikoreich sein.
- Lösung:
Verarbeitung personenbezogener Daten ausschließlich in vertrauenswürdige Umgebung (eigene Geräte) verlagern.

Beispiel:
Intelligente Wasserzähler

Strategien:
Abstrahieren, Minimieren

„Erhebung von Nutzdaten einschränken“ / „User data confinement pattern“

Problem: Daten, die bspw. aus Abrechnungsgründen fortwährend von einzelnen Nutzern an eine zentrale Stelle übertragen werden, erhöhen Datenschutz-Risiken.

Lösungsidee: Sofern möglich, sollte die Verarbeitung oder ein Aggregieren von Daten vor Ort passieren. Die Anzahl an Übertragungen wird verringert und auch die Informationen werden weniger aussagekräftig.

Berücksichtigte Strategien: Abstrahieren, Minimieren

Beispiel: Intelligente Wasserzähler: An Stelle der Verbrauchsdaten-Übertragung eines Kunden an eine zentrale Abrechnungsstelle können bereits im Ablesegerät alle Abrechnungen erstellt werden. Dadurch verlassen die sensiblen Daten (Gewohnheiten bei Aufstehen und Zubettgehen, Rückschlüsse auf verwendete Geräte, ...) niemals die Wohnung.

<https://privacypatterns.org/patterns/User-data-confinement-pattern>

Data Protection by Design Software-Technik

Privacy Enhancing Technologies

„Privacy-Enhancing Technologies ist ein IKT-System, das den Schutz der informationellen Privatsphäre durch die Eliminierung oder Minimierung personenbezogener Daten misst und dadurch eine unnötige oder unerwünschte Verarbeitung personenbezogener Daten verhindert, ohne dass die Funktionalität des Informationssystems verloren geht.“

van Blarckom, Borking & Olk 2003

Werkzeuge und Services mit folgenden Eigenschaften:

- Schutz von personenbezogenen Daten
- Kontrolle über persönliche Daten (Selbstdatenschutz)

Datenschutz-Technologien (Privacy Enhancing Technologies)

Der Begriff „Privacy Enhancing Technologies“ (PET) ist weit verbreitet, weswegen an dieser Stelle „Privacy“ statt „Data Protection“ genutzt wird.

Als PET werden solche konkreten Werkzeuge und Services bezeichnet, die dabei helfen, Datenschutz zu unterstützen.

Zum einen durch einen Einsatz in Software bzw. Hardware, um den Schutz von personenbezogenen Daten zu verbessern.

Zum anderen aber auch zur Unterstützung des Selbstdatenschutzes, indem Nutzerinnen und Nutzern Werkzeuge zugänglich gemacht werden, mit denen sie mehr Kontrolle über ihre persönlichen Daten erhalten.

Data Protection by Design Software-Technik

Beispiele für Privacy Enhancing Technologies

- Verschlüsselung
Ende-zu-Ende-Verschlüsselung, Forward Secrecy, Let's encrypt
- Anonymisierung in Datenbanken
k-Anonymität, I-Diversität, Differential Privacy
- Datenschutzerhaltende Berechnungen
homomorphe Verschlüsselung, Multi-Party Computation
- PET-Werkzeuge bei der Nutzung
(„by design“ Kompatibilität sicherstellen, z.B. NoScript)

Datenschutz-Technologien – Beispiele

Beim Begriff PET werden unterschiedliche Ansätze verstanden

- Perspektive der Software-Entwicklung: Konkrete Technologien, die erprobt sind und eingesetzt werden können, z.B.
 - Verschlüsselung (Messenger, HTTPS)
 - Anonymisierung (kryptografische/mathematische Ansätze)
 - Berechnungen auf verschlüsselten Daten – insbesondere auf verschiedenen Rechnern
- Werkzeuge, die den Nutzerinnen und Nutzern die Möglichkeit bieten, mehr Souveränität über ihre Daten zu erlangen (Ad-Blocker, datenschutzfreundliche Suchmaschinen)
siehe auch: <http://cyberlaw.stanford.edu/wiki/index.php/PET>

Weiterführende Literatur und Links:

[„Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies“](#)

[“Privacy Enhancing Technologies: Evolution and State of the Art”](#)

<http://app-pets.org/home/>

<http://cyberlaw.stanford.edu/wiki/index.php/PET>

Data Protection by Design ***Software-Technik***

Diskussion

- Wie schätzen Sie die Umsetzung der Anforderung *Data Protection by Design* ein? Welche Herausforderungen und Risiken sehen Sie?
 - Welche Werkzeuge, Anleitungen oder Konzepte sind aus Ihrer Sicht notwendig, um *Data Protection by Design* in der Praxis umzusetzen?
- 

Software-Technik - Diskussion

Data Protection by Default ***Datenschutzfreundliche Voreinstellungen***

Idee von *Data Protection by Default* :

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

In der DS-GVO wird gefordert: Datenschutz von Anfang an (siehe Folie 5)

Ziel ist dabei:

- Möglichst wenig Daten werden erhoben.
- Möglichst wenig Daten werden verarbeitet.
- Daten werden nur so lange gespeichert wie erlaubt / vorgeschrieben.
- Daten sollen grundsätzlich nicht Dritten zugänglich gemacht werden

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 entscheidet? Nicht die Verantwortlichen?
- Dies ist gemeint:
 - englischer Text *„without the individual's intervention“*
 - „Soziale-Netze-Regelung“:
Nicht alles ist für alle bestimmt!

„by Default“ benötigen keinen Nutzer-Eingriff

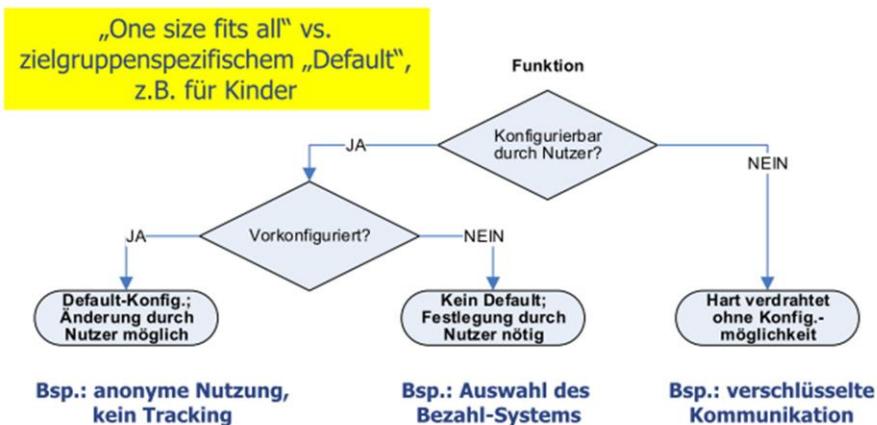
Die Standard-Einstellung soll ohne Eingreifen „der Person“ gelten – hier bezieht sich die DS-GVO auf das Individuum, dessen personenbezogene Daten verarbeitet werden.

Beim Veröffentlichen von Daten darf auch in Sozialen Netzwerken nicht automatisch davon ausgegangen werden, dass diese grundsätzlich für alle Personen bestimmt sind.

Beispielsweise bedeutet dies, dass standardmäßig nur die direkt verbundenen Kontakte („Freunde“, „Follower“, ...) einen neuen Beitrag sehen können.

Data Protection by Default Wired-in or by default?

Fragestellung bei der Implementierung:



Was genau ist „by Default“?

Nicht in jedem Fall ist sofort klar, was als eine Standard-Einstellung („Default“) betrachtet werden kann.

In der Grafik wird verdeutlicht, dass in unterschiedlichen Anwendungsfällen ein „Default“ unterschiedlich eingeschätzt werden kann – oder es keinen Default gibt wie z.B. bei Bezahl-Systemen.

Data Protection by Default ***Wired-in or by default?***

Beispiel 1: Webserver und Verschlüsselung

Verschlüsselte Verbindungen zu Webservern bieten mehr Datenschutz. Wie ist eine Default-Konfiguration?

- nur http (unverschlüsselt)
- http + https (unverschlüsselt + verschlüsselt)
- nur https (verschlüsselt, http wird automatisch zu https)
→ Dadurch werden ggf. einzelne Browser/Systeme ausgeschlossen ...

Einfluss von Dritten: Ranking bei Suchmaschinen

Was genau ist „by Default“? – Beispiel 1

Zwei HTTPS-Beispiele werden vorgestellt, die diese Problematik illustrieren: Soll ein Webserver nur HTTPS-Zugriffe zulassen oder diese nur bevorzugen?

Ggf. würden einzelne Browser/Systeme bei einer strengen HTTPS-Pflicht ausgeschlossen ...

Markant ist dabei, dass der Einfluss von Dritten (hier: Suchmaschinen) auf die verbreitete Nutzung von HTTPS am größten eingeschätzt wird. Es gibt z.B. Suchmaschinen, die HTTPS-Seiten bevorzugen und dadurch einen Umstellungsdruck erzeugen.

Data Protection by Default Wired-in or by default?

Beispiel 2: Browserkonfiguration und Verschlüsselung

Kann auf der anderen Seite der Aufruf von verschlüsselten Seiten unterstützt werden?

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



Was genau ist „by Default“? – Beispiel 2

Mit dem Plugin HTTPS Everywhere gibt es eine Möglichkeit, den Browser – wenn möglich – zum Verwenden des verschlüsselten HTTPS-Datenverkehrs zu zwingen.

Eine Standard-Einstellung könnte daher sein, dass ein Browser mit diesem Plugin installiert werden soll.

Data Protection by Default Grenzen

Wo sind die Grenzen von *Data Protection by Default*?

Problemfelder

- Ist eine Anwendung möglicherweise völlig unbenutzbar, wenn sie "per default" keinerlei Daten verarbeitet?
Beispiel: App für Soziale Netzwerke
- Ist eine Konfiguration mit unbegrenzter Datenverarbeitung dann nur einen Mausklick entfernt?
Default: keine Datenübertragung
sonst: alles erlauben

Wo sind die Grenzen von „Data Protection by Default“?

Problematisch ist, dass einige Anwendungen (z.B. Soziale Netzwerke) mit einer konsequenten „by Default“-Regel nicht sinnvoll nutzbar sind. Gerade in diesem Beispiel ist schließlich das Erfahren von (veröffentlichten) Informationen Dritter von Interesse.

Eine strenge „by Default“-Regel, die zunächst alle (ungewollten und gewollten) Datenübertragungen ausschließt, allerdings mit einem Klick alle Datentransfers zugelassen werden können, kann aus Datenschutz-Sicht nicht die Lösung sein.

Data Protection by Default Grenzen

Wo sind die Grenzen von *Data Protection by Default*?

Technische Lösung:

- Konfigurationsprofile mit Konfigurationen für typische Anwendungsfälle

Beispiele:

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

Wo sind die Grenzen von „Data Protection by Default“?

„by Default“ sollte daher im Einzelfall technisch so umgesetzt werden, dass mit unterschiedlichen Profilen bzw. situationsabhängig der „Default“ festgelegt wird – beispielsweise in Sozialen Netzwerken durch Gruppen von Kontakten, die einzeln ausgewählt werden können, bevor ein Beitrag veröffentlicht wird.

Beispielhaft dafür sind Standard-Konfigurationen von Firewalls, bei denen z.B. Internetzugriffe von typischen Browser- oder E-Mail-Anwendungen standardmäßig zugelassen werden.

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

Einsatzbeispiel: Zertifikatsprotokolle

Um die Authentizität eines (Web-)Servers nachzuweisen, kann sich dieser beim Verbindungsaufbau mit einem Zertifikat ausweisen. Solche Zertifikate können (aus unterschiedlichen Gründen) ablaufen bzw. verworfen werden, sodass eine Prüfung von Zertifikaten notwendig ist.

Früher wurden zu diesem Zweck Sperrlisten der nicht mehr gültigen Zertifikate angeboten, die z.B. von einem Browser heruntergeladen und später Zertifikate damit geprüft werden konnten. Der zeitliche Verzug wurde jedoch als Sicherheitsproblem gesehen.

Mit einem neuen Protokoll wurde festgelegt, dass ein einzelnes Zertifikat bei jedem Zugriff bei einer zentralen Stelle geprüft wird – wodurch jedoch diese zentralen Stellen die Online-Aktivitäten von einzelnen Personen hätten verfolgen können.

Die datenschutzfreundliche Lösung ist nun, dass die Gültigkeit eines Zertifikats vom Zertifizierten selbst nachgewiesen wird, indem er einen aktuellen signierten Gültigkeitsnachweis der Zertifizierungsstelle bereitstellt – so erfährt die Zertifizierungsstelle lediglich, dass ein Webserver kontaktiert wurde, nicht jedoch von wem.

Damit einher geht allerdings wieder ein (kleinerer) zeitlicher Verzug, da zwischen zwei Gültigkeitsnachweisen ein Missbrauch der Zertifikate theoretisch möglich wäre.

Austausch und Fazit

Diskussion

- Wie schätzen Sie die Umsetzung der Anforderung *Data Protection by Default* ein? Welche Herausforderungen und Risiken sehen Sie?
 - Haben Sie noch Fragen?
 - Was ist ihr Fazit? Haben *Data Protection by Design* und *Data Protection by Default* eine Chance?
- 

Diskussion zum Abschluss

Vielen Dank

