Privatheit und Datenschutz

https://iuk.one/2913.pdf

Clemens H. **Cap**
ORCID: 0000-0003-3958-6136

Department of Computer Science
University of **Rostock**
Rostock, Germany
clemens.cap@uni-rostock.de

16. 1. 2025

Übersicht

1. Privatheit
2. DatenSchutzGrundVerOrdnung
3. DSGVO Praxis
4. Standard-Datenschutzmodell
5. Technische Maßnahmen
6. Weitere wichtige Aspekte

1. Privatheit

Was ist das und warum ist das wichtig?

Entwicklung und 4 Doktrinen (1)

Lange Tradition: Beichtgeheimnis, Hippokratischer Eid

Privacy in Private Doktrin: Grundsätzliches Recht auf Privatheit

- "The right to be left alone."
- Wichtiges Gerichtsurteil anläßlich neuer Technologie (Fotographie)
- Publikation von Louis Brandeis, 1890, Harvard Law Review
- Binäre, schwarz/weiß Einteilung der Welt in public/ private

Privacy in Public Doktrin: Informationelle Selbstbestimmung

- Bahnbrechendes Urteil: Volkszählungsurteil 1983
- "Das Recht darüber zu bestimmen, welche Daten über sich von anderen gebraucht werden und welche Daten auf einen selbst einwirken dürfen."
- Feiner dosierte Abgrenzung
- Informationelle Selbstbestimmung
  - nach innen — Also auch Recht auf eigenes Nicht-Wissen
  - und außen — Dritter, incl. des Staates, über mich

Volkszählungsurteil

Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, [...] kann in seiner Freiheit wesentlich gehemmt werden. [...]

Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen.

Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte verzichten.

(Quelle: BVerfG: Volkszählungsurteil BVerfG, Urteil v. 15.12.1983, Az. 1 BvR 209, 269, 362, 420, 440, 484/83)

4 Doktrinen (2)

Interpersonal Privacy Doktrin

- Austausch von Informationen so, daß es maximal sozial nützlich erscheint
- Privatheit als ökonomisches / soziales Gut, das getauscht werden kann (vgl: Google, Facebook)
- Problem: Fehlende ökonomische "Augenhöhe", fehlende Transparenz.
  - Datensubjekt kann Preis nicht einschätzen. Bsp: Facebook User.
  - Datennutzer kann Preis sehr gut einschätzen. Bsp: Facebook selber.

Zero Privacy Doktrin

- You have zero privacy – get over it (Scott McNealy, CEO Sun)
- Privatheit als verloren gegangene Eigenschaft
- These der "Post-Privacy Society"
- Frage: Will ein demokratische Gesellschaft das akzeptieren.

Konzeptuelles Modell der Soziologie: Panopticon von Bentham

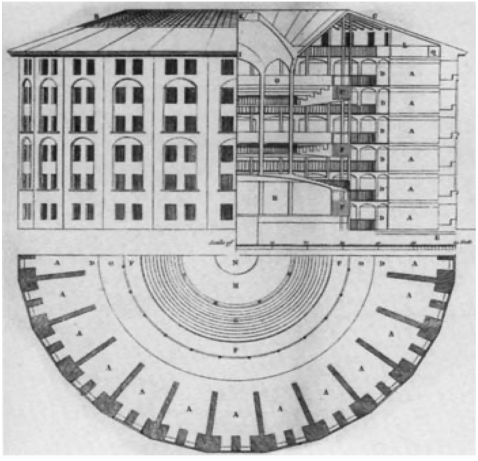


Abb. 1: Plan des Panopticons von Jeremy Bentham. Rechte s. Anhang.

Presidio Modelo (1)

Abb. 2: Realisierung des Panopticons auf Kuba. Rechte s. Anhang.

Presidio Modelo (2)

Abb. 3: Realisierung des Panopticons auf Kuba. Rechte s. Anhang.

Theorie des Panopticons

Situation:

- Gefängnisarchitektur
- Ein Wächter kann alle Gefangenen sehen
- Gefangener weiß nicht, ob er beobachtet wird

These

Bereits die Fantasie beobachtet zu werden führt zu Verhaltensanpassung in Richtung der vom Beobachteten beim Beobachter vermuteten Erwartungshaltung.

Praxis des Panopticons

These

Datensammlungen führen allein durch ihr Bestehen bereits zu einer Verhaltensänderung.

Der Veränderungsdruck *kann* gesellschaftlich erwünscht sein.

Frage: Ist er demokratisch legitimiert?

Antwort: Unklar und problematisch.

Frage: Ist der Druck wirklich so groß, wie behauptet?

Antwort: Ja – viele soziologische Studien.

Bsp: Konformitätsexperiment von Ash
Bsp: Augenposterexperimente

Konformitätsexperiment von Solomon Ash, 1951 (1)

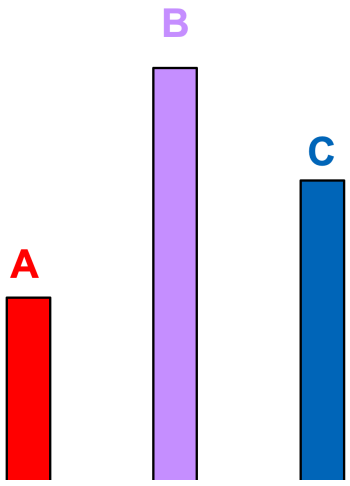


Abb. 4: Skizze des Konformitätsexperiments Rechte s. Anhang.

Konformitätsexperiment von Solomon Ash, 1951 (2)

Ablauf des Experiments:

1. Klare Aufgabenstellung mit klarer Antwort
2. Zu gegebener Testlinie eine gleichlange Referenzlinie angeben
3. 8 eingeweihte Personen geben Antwort, dann jeweils eine Testperson
4. Zuerst: Aufwärmrunde, dann geben Eingeweihte konsistent Falschantworten
5. Nur 33% der VP verweigern Konformität in die offenkundig falsche Antwort

Konformitätsexperiment von Solomon Ash, 1951 (3)

Schlußfolgerung von Ash in den Originalarbeiten:

The tendency to conformity in our society is so strong that reasonably intelligent and well-meaning young people are willing to call white black. This is a matter of concern.

It raises questions about our ways of education and about the values that guide our conduct.

When his subjects were later interviewed, most of them said that they did not really believe their conforming answers, but had gone along with the group for fear of being ridiculed or thought "peculiar."

A few of them said that they really did believe the group's answers were correct.

Augenposterexperiment von Daniel Nettle: Variante Kaffee

Abb. 5: Das Augenposter.

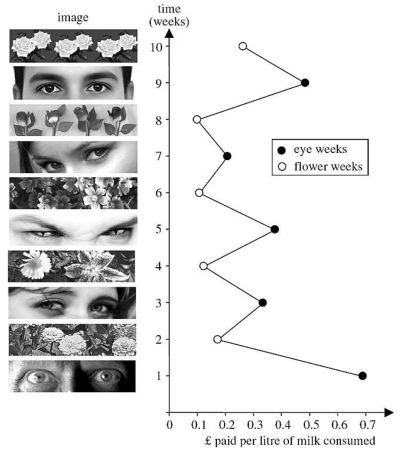


Abb. 6: Das Ergebnis des Experiments.

Augenposterexperiment: Variante Stellplätze.

Experiment: Poster an Fahrrad Stellplätzen der Uni.

Ergebnis:
Wo plaziert: Diebstähle um 62% reduziert
Wo nicht plaziert: Diebstähle um 63% gestiegen

Folge: These der Verlagerung

Beispiele für bedenklichen Verlust von Privacy

4 wichtige Beispiele:

1. Im ökonomischen Raum durch die Erstellung von Profilen.
2. Im öffentlichen Raum durch das Registrieren abweichenden aber zulässigen Verhaltens.
3. Auf digitalen sozialen Medien durch den Massenwahn der Selbstpreisgabe.
4. Im digitalen Raum durch digitale Angreifer.

Problem der Asymmetrie:
Angreifer weiß mit Daten mehr anzufangen als der Angegriffene versteht.

Künftiges Problem

GPT-4 Outperforms Humans in Persuasion by 82% in This New Study

Zia Muhammad 4/07/2024 03:30:00 AM

A recent study conducted by researchers at Swiss Federal Institute of Technology Lausanne, or EPFL for short, suggested that GPT-4 is better at persuasion than human beings by a margin of just under 82%, or 81.7% to be precise. The study involved conducting debates between 820 people around a wide range of topics. These topics included highly charged subjects such as whether or not race should be considered in the admission criteria of colleges, as well as low risk topics like whether or not the penny should continue to be circulated as legal tender.

Abb. 7: AI kann Menschen sehr gut vom Gegenteil ihrer Meinung überzeugen, insbesondere wenn AI die Grundposition der Menschen kennt. Rechte s. Anhang.

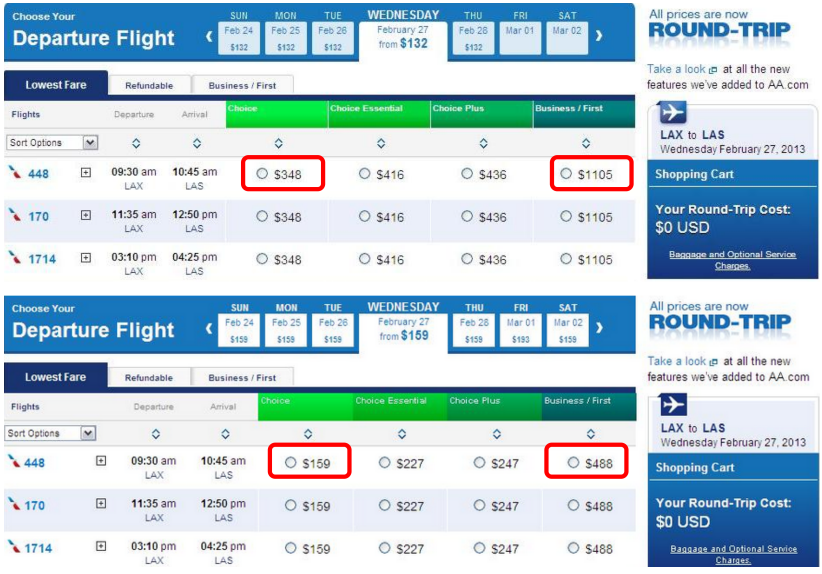


Abb. 8: Screenshot Rechte s. Anhang.

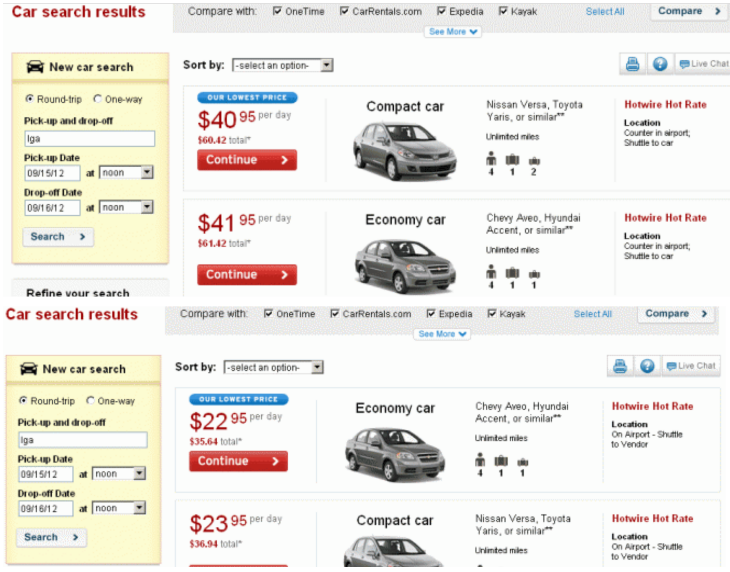
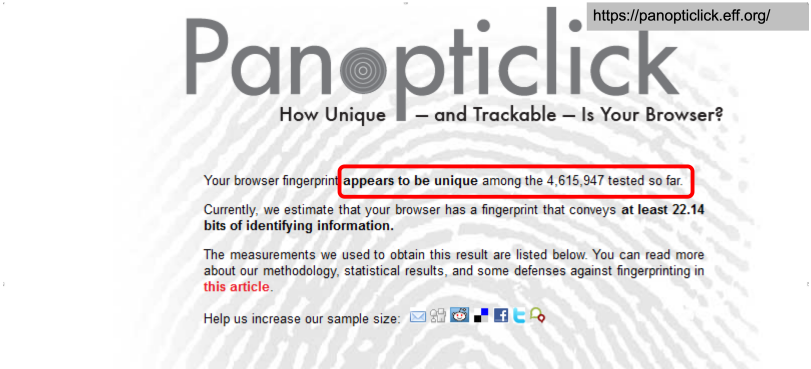


Abb. 9: Screenshot Rechte s. Anhang.



Browser Characteristic	bits of identifying information	one in x browsers have this value	value
User Agent	7.41	170.66	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:26.0) Gecko/20100101 Firefox/26.0
HTTP_ACCEPT Headers	7.57	189.86	text/html, */* gzip, deflate en-gb,en;q=0.5
			Plugin 0: Adobe Acrobat; Adobe PDF Plug-In For Firefox and Netscape 11.0.07; nppdf32.dll; (Acrobat Portable Docu application/pdf; pdf) (Adobe PDF in XML Format; application/vnd.adobe.pdfxml; pdfxml) (Adobe PDF in XML application/vnd.adobe.x-mars; mars) (Acrobat Forms Data Format; application/vnd.fdf; fdf) (XML Version of Acrobat Forn application/vnd.adobe.xfdf; xfdf) (Acrobat XML Data Package; application/vnd.adobe.xdp+xml; xdp) (Adobe FormFlo

Abb. 10: Screenshot Rechte s. Anhang.

Problematik

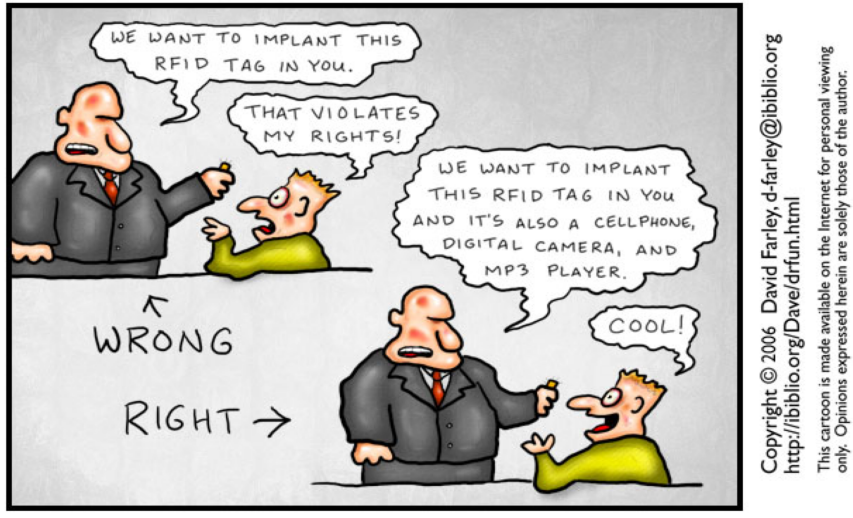
Cartoon: Zwei Schweine auf der Farm.

Schwein 1: Isn't it great? We have to pay nothing for the barn.

Schwein 2: Yeah! And even the food is free.

Untertitel

Facebook and You. If you are not paying for it, you're not the customer but the merchandise being sold.



http://www.ibiblio.org/Dave/Dr-Fun/df200601/df20060116.jpg

Abb. 11:

International Privacy Index

Siehe: http://chartsbin.com/view/by8

2. DatenSchutzGrundVerOrdnung

Überblick über die Rechtslage, soweit sie für den Informatiker wichtig ist.

Üblicher Disclaimer: Ich bin kein Jurist, kenne mich nur oberflächlich aus, das ist keine Rechtsberatung, Argumente werden oft nur verkürzt dargestellt.

Was ist die DSGVO?

Die DSGVO enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.

Gültig ab 2018.

Enthält umfassende **Sorgfalts- und Dokumentationspflichten** zur Verarbeitung (auch: Speicherung) personenbezogener Daten durch den dafür **Verantwortlichen** oder den **Auftragnehmer** der Verarbeitung.

Anwendungsbereich

Die DSGVO gilt **sachlich** für

1. ganz oder teilweise automatisierte Verarbeitung **personenbezogener Daten** – und
2. für die nichtautomatisierte Verarbeitung **personenbezogener Daten**, die in einem Dateisystem gespeichert sind.

Wichtige Ausnahmen: Strafverfolgung, Haushaltsprivileg und andere.

Die DSGVO gilt **räumlich** in der EU. Also wenn

1. Niederlassung eines Verantwortlichen oder eines Verarbeiters in der EU
2. betroffene Person in der EU ist und mit ihr dort interagiert wird

Haushaltsprivileg

Datenverarbeitungen durch **(1) natürliche Personen** zur Ausübung **(2) ausschließlich (3) persönlicher und familiärer** Tätigkeiten unterliegen nicht der DSGVO.

Typische Beispiele:

1. privater Schriftverkehr
2. Anschriften-/Telefonverzeichnisse
3. Nutzen sozialer Netzwerke
4. Online-Tätigkeiten
5. Führen eines Tagebuchs
6. Aufnahme von Urlaubsbildern

Aber Abgrenzung: Wenn Daten dann auch für die Vereinsverwaltung genutzt werden, unterliegen sie wieder der DSGVO.

Personenbezogene Daten

Personenbezogene Daten sind

alle Informationen, die sich auf eine identifizierte oder identifizierbare **natürliche** Person beziehen.

Abgrenzung: Gilt nicht für juristische Personen.

identifizierbar

wenn eine natürliche Person **direkt oder indirekt** identifiziert werden kann.

Typischerweise: Kennung, Name, Kennnummer, Standortdaten, Online-Kennung, besondere Merkmale der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person.

Besondere Kategorie von personenbezogenen Daten

Besondere Klassifizierung von besonders "heiklen" Daten:

1. Rassische und ethnische Herkunft
2. Politische, religiöse oder weltanschauliche Überzeugung
3. Gewerkschaftszugehörigkeit
4. Genetische Daten
5. Biometrische Daten zur Identifizierung
6. Gesundheitsdaten
7. Daten zu Sexualleben oder sexueller Orientierung

Verarbeitung ist verboten, bei wenigen Ausnahmen, unter anderem:

1. Zustimmung liegt vor für einen festgelegten Zweck
2. Rechtlich erforderlich
3. Zweckgebundener Verein
4. Von der Person selbst offensichtlich öffentlich gemacht Daten
5. Öffentliches Interesse
6. Gesundheitsvorsorge, Arbeitsmedizin

Rechtmäßigkeit der Verarbeitung

Mindestens eine der folgenden Bedingungen:

1. **Einwilligung** für einen bestimmten Zweck wurde gegeben
2. Für Erfüllung eines **Vertrags** erforderlich
3. Für Erfüllung einer **rechtlichen Verpflichtung** erforderlich
4. Zum Schutz **lebenswichtiger Interessen** Dritter
5. Zur Wahrung **berechtigter Interessen** Dritter

Anforderungen an die Einwilligung:

- **Widerruf**: Kann jederzeit ohne Gründe widerrufen werden.
- **Nachweis**: Datenverarbeiter muß nachweisen können.
- **Freiwilligkeit**: Keine Koppelung der Einwilligung für Nutzung zusätzlicher Daten über die notwendigen hinaus an das eigentliche Geschäft.

3. DSGVO Praxis

Was bedeutet das für die Praxis?

Eine knappe, unvollständige Übersicht.
Wieder greift der Disclaimer von zuerst.

Verarbeitungsverzeichnis

Ist auf Verlangen der Aufsichtsbehörde vorzulegen.

Bei kleineren (weniger als 250) Unternehmen nicht erforderlich.
Aber: Etliche Ausnahmen

1. Identifikation der Verantwortlichen
2. Zweck der Verarbeitung
3. Kategorien von personenbezogenen Daten
4. Kategorien von Empfängern von Daten (intern / extern)
5. Übermittlung von Daten in Drittländer
6. Löschfristen von Daten
7. Benutzte technische und organisatorische Maßnahmen

Strafen: Bis 10 Millionen oder 2% weltweiter Jahresumsatz.

Genaueres:
https://www.datenschutz-mv.de/static/DS/Dateien/DS-GVO/HilfsmittelzurUmsetzung/VVT/HinweisezumVerzeichnisvonVerarbeitungstaetigkeiten.pdf

Datenschutz- und IT-Sicherheitskonzept

Dient dem Nachweis von Maßnahmen für die Gewährleistung von

(1) Informationssicherheit

1. Vertraulichkeit — **C**onfidentiality
2. Integrität — **I**ntegrity
3. Verfügbarkeit — **A**vailability

(2) Datenschutz

1. Nichtverkettung
2. Transparenz
3. Intervenierbarkeit
4. Datenminimierung

Begriffe (1): CIA Triade

Grundsätzlich bereits bekannt.
Hier: Wiederholung nach dem Text und spezifischen Zweck der DSGVO.

Vertraulichkeit: Keine unbefugte Person darf personenbezogene Daten zur Kenntnis nehmen oder nutzen.

Integrität: Personenbezogene Daten dürfen nur in einer Weise verarbeitet werden, die einen Schutz vor

1. unbeabsichtigtem Verlust,
2. unbeabsichtigter Zerstörung oder
3. unbeabsichtigter Schädigung

gewährleisten.

Geeignete technische und organisatorische Maßnahmen sind zu nutzen.

Veränderungen an den gespeicherten Daten durch unberechtigte Dritte muß ausgeschlossen werden oder so erkennbar gemacht werden, daß sie korrigiert werden können.

Verfügbarkeit: Der Zugriff auf personenbezogene Daten sowie ihre Verarbeitung müssen unverzüglich möglich sein.

Begriffe (2)

Nichtverkettung: Zu unterschiedlichen Zwecken erhobene personenbezogene Daten dürfen nicht zusammengeführt, d. h. verkettet werden.

Transparenz: Es muss erkennbar sein,

1. welche Daten
2. wann
3. für welchen Zweck verarbeitet werden,
4. welche Systeme und Prozesse genutzt werden,
5. wohin die Daten zu welchem Zweck fließen und
6. wer die rechtliche Verantwortung für die Daten und Systeme besitzt.

Begriffe (3)

Intervenierbarkeit: Betroffene müssen ihre Rechte an ihren personenbezogenen Daten wahrnehmen können.

Diese **Rechte** sind:

1. **Auskunft** erhalten
2. **Korrekturen** vornehmen lassen
3. **Sperren** lassen
4. **Löschen** lassen

Die Datenverarbeitungsprozesse müssen das ermöglichen.

Datenminimierung: Verarbeitung personenbezogener Daten ist auf das dem Zweck angemessene, erhebliche und notwendige Maß zu beschränken.

4. Standard-Datenschutzmodell

Leitfaden, wie das nach dem aktuellen Stand der Technik praktisch umzusetzen ist.

Standard-Datenschutzmodell

Frage: Wie löst man diese Anforderungen konkret?

Arbeitsgruppe der Datenschutzkonferenz entwickelt das **Standard-Datenschutzmodell (SDM)**.

Was ist das Standard-Datenschutzmodell (SDM)?

Eine Vorgehensweise, mit der die rechtlichen Anforderungen aus der Datenschutzgrundverordnung (DSGVO) in **konkrete technische und organisatorische Maßnahmen** übersetzt werden können.

Quelle: https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/

Im folgenden ausgewählte, verkürzte Beispiele.

Anwendung mit Augenmaß: Einwohnermeldeamt vs. Kaninchenzüchterverein.

Dokumentieren

Dokumentieren

Beschreibung der Verarbeitung, insbesondere unter Ausweis des Zwecks der Verarbeitungstätigkeit und der Zweckbindung der verarbeiteten Daten.

Es dient dem dauerhaften Nachweis der Rechtmäßigkeit der Verarbeitung für (1) die Organisation selbst, für (2) andere Organisationen, für (3) Datensubjekte und (4) gegenüber Aufsichtsbehörden.

Protokollieren

Protokollieren

Den Zweck, eine Verarbeitungstätigkeit, die in der Vergangenheit stattfand, prüfbar machen.

(1) Wann hat **(2) wer (3) welche** Daten von **(4) welchem Ist**-Zustand auf **(5) welchen Soll**-Zustand geändert und **(6) warum**?

Protokolle sind gegen böswillige Veränderung zu schützen.

Berichtigung

Berichtigung

Personenbezogene Daten müssen (1) sachlich richtig und (2) auf dem neuesten Stand sein.

Betroffene Personen haben das Recht, eine Richtigstellung zu verlangen.

Konkret: Daten müssen

- berichtigt werden
- auf den neuesten Stand gebracht werden – oder
- gelöscht werden

Unvollständige Daten gelten als sachlich falsch, **wenn** durch das Fehlen bestimmter Angaben ein im Hinblick auf den Verarbeitungszweck falscher Eindruck entstehen könnte.

Einschränkung der Verarbeitung

Einschränkung der Verarbeitung

Einschränkung der Verarbeitung bedeutet das Markieren gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung – zumindest vorübergehend – einzuschränken.

Abgrenzung:

- Bedeutet **nicht** die Pflicht zum Löschen
- Bedeutet **aber**, daß aktuell als alleinige Verarbeitung nur die Speicherung erlaubt ist

Einschränkung der Verarbeitung muß auch bei Backup und Restore ersichtlich bleiben.

Pflicht zur Einschränkung der Verarbeitung

Pflicht zur Einschränkung besteht:

1. Richtigkeit der personenbezogenen Daten von der betroffenen Person bestritten, bis die Richtigkeit überprüft wurde
2. Verarbeitung unrechtmäßig und betroffene Person hat Löschung abgelehnt und die Einschränkung der Nutzung verlangt
3. Daten für die Zwecke der Verarbeitung nicht länger benötigt, betroffene Person benötigt sie aber zur Geltendmachung von Rechtsansprüchen (also keine Löschung)
4. Betroffene Person hat Widerspruch gegen die Verarbeitung eingelegt und Abwägen dagegenstehender Gründe ist noch nicht erfolgt.

Löschen

Löschen

Löschen ist das Unkenntlichmachen gespeicherter personenbezogener Daten.

Löschens muss bewirken, dass nach dem Löschen keine Daten mehr vorhanden sind, mit denen eine natürliche Person identifiziert werden kann.

Gelöschte Daten dürfen nicht mehr reproduzierbar sein.

Umfassende Löschung bedeutet: Die Pflicht zur Löschung betrifft

- Aktiver Datenbestand
- Replikation des Datums (Kopien)
- Sicherungskopien (Backup)
- Protokolldaten, wenn diese personenbezogene Daten enthalten.
- Daten bei Auftragsverarbeitern

Nicht ausreichende Formen des Löschens

Wenn die Daten reproduzierbar sind.

Wichtige Beispiele:

- Austragen einer Datei aus Verzeichnissen oder directories
- Schnellformatieren von Datenträgern
- Aussprechen eines Nutzungsverbots der Daten
- Zusage, die Daten nicht mehr zu verwenden

Vernichten

Vernichtung

Vernichtung beschreibt die Zerstörung des Datenträgers, unabhängig davon, ob es sich um analoge Datenträger oder digitale Datenträger handelt.

Hinweis: Vernichtung ist eine unwiderrufliche Form des Löschens.

Pflicht zur Löschung

Wann müssen Daten gelöscht werden?

1. Auf Verlangen der betroffenen Person, wenn keine andere Rechtsgrundlage
2. Notwendigkeit oder Zweck der Verarbeitung entfallen
3. Einwilligung zur Speicherung wurde widerrufen und keine andere Rechtsgrundlage
4. Widerspruch der betroffenen Person und keine andere Rechtsgrundlage
5. Daten wurden unrechtmäßig verarbeitet
6. Ablauf einer gesetzlich vorgegebenen maximalen Speicherfrist

Identifikation von Betroffenen

Problem: Wer verlangt da seine DSGVO Rechte?

Lösung

Hat der Verantwortliche begründete Zweifel an der Identität der natürlichen Person, die den Antrag gemäß den Artikeln 15 bis 21 stellt, so kann er zusätzliche Informationen anfordern, die zur Bestätigung der Identität der betroffenen Person erforderlich sind.

5. Technische Maßnahmen

Was muß der Informatiker tun?

Typische Verfahren für die CIA Triade (1)

Vertraulichkeit (Confidentiality)

1. Rollen und Rechtekonzepte: Wer darf was?
2. Sichere Authentisierung der Nutzer: Wer ist auf den Systemen?
3. Verschlüsselung bei Transport und Speicherung
4. Zuverlässiges und qualifiziertes Personal: Bis hin zu Sicherheitsüberprüfung
5. Kontrolle organisatorischer Abläufe: Dokumentation und Audit
6. Eingeschränkter Zugang zur Hardware: Zutrittskontrolle, Video-Überwachung

Integrität (Integrity):

1. Schreib- und Änderungsrechte: Wann darf wie geändert werden?
2. Rollen und Rechtekonzepte: Wer darf ändern?
3. Prüfsummen, digitale Signaturen: Änderungen erkennen.
4. Kontrolle organisatorischer Abläufe: Dokumentation und Audit
5. Eingeschränkter Zugang zur Hardware: Zutrittskontrolle, Video-Überwachung

Typische Verfahren für die CIA Triade (2)

Verfügbarkeit (Availability):

1. Schutz vor äußeren Einwirkungen: Schadsoftware, Sabotage, Naturkatastrophen
2. Redundanz von Hardware, Software, Infrastruktur
3. Vertretungsregelung für Personal
4. Backup / Restore
5. Getestete Notfall- und Wiederherstellungsprozesse
6. Regelmäßige Wartung. Bsp: Updates von Systemen

Typische Verfahren für den Datenschutz (1)

Nichtverkettung:

1. Einschränkung von Verarbeitungs-, Nutzungs- und Übermittlungsrechten
2. Minimierung der Zugangsschnittstellen
3. Trennung nach Organisationseinheiten und Abteilungen
4. Rollen und Rechtekonzepte
5. Anonymisierung und Pseudonymisierung in der Auswertung
6. Geregeltes Verfahren zur Änderung des Zwecks der Verarbeitung

Transparenz: Ist vor allem Dokumentation.

1. Dokumentation der Verarbeitungstätigkeit
2. Dokumentation der Geschäftsprozesse
3. Datenlexikon: Welche Daten in welcher Form und wofür.
4. Dokumentation von Einwilligungen und Widersprüchen
5. Dokumentation aller weiteren Maßnahmen: Bsp: Mitarbeiterschulung
6. Protokollieren und Auditieren von Zugriffen

Typische Verfahren für den Datenschutz (2)

Intervenierbarkeit

1. Dokumentierte Prozesse zur Einwilligung und Rücknahme von Einwilligungen
2. Datenfelder für Sperrung, Einwilligung, Widerspruch
3. Konzepte zur Umsetzung der Rechte (Löschen, Sperren, Auskunft, Berichtigung)
4. Identifizierung der Personen die ihre Rechte wahrnehmen wollen

Datenminimierung

1. Möglichst wenig Attribute erfassen
2. Möglichst wenig Verarbeitungsoptionen vorsehen
3. Automatisierte Sperr- und Löschroutinen
4. Verarbeitung, die eine Kenntnisnahme verarbeiteter Daten reduziert

6. Weitere wichtige Aspekte

Was sonst noch von Bedeutung sein kann.

Weitere Anforderungen

1. KRITIS: Gesetze und Verordnungen über krtische Infrastrukturen
2. Informationsfreiheitsgesetz
3. IT Sicherheitsgesetz (1.0 und 2.0)
4. NIS Richtlinie der EU für Netzwerk und Informationssicherheit
5. ...

Kritis: Abstrakte Sichtweise

Definition

Kritische Infrastrukturen (kurz: KRITIS) sind **Organisationen oder Einrichtungen** mit **wichtiger** Bedeutung für das **staatliche Gemeinwesen**, bei deren Ausfall oder Beeinträchtigung **nachhaltig wirkende Versorgungsengpässe**, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden

Kritis: Konkrete Sichtweise

Die 10 Kritis Sektoren (Stand 2021) sind:

1. Wasserversorgung
2. Energieversorgung
3. Lebensmittelversorung
4. Finanz- und Versicherungswesen
5. Gesundheit
6. Telekommunikation
7. Abfallentsorgung
8. Medien und Kultur
9. Staat und Verwaltung
10. Transport und Verkehr

Gefahren für KRITIS

Für den **Informatiker** wichtig:

1. Systemversagen
2. Schadprogramme
3. Cyberangriffe

Andere:

1. Naturkatastrophen
2. Epidemien
3. Unfälle
4. Terrorismus
5. Krieg
6. ...

Zentrale Themen

Dominoeffekte: Einzelne Ausfälle haben Folge-Effekte.

Beispiel:

1. Strom fällt aus
2. Aufzug fällt aus
3. Benachrichtigungswege fallen aus
4. Wasserversorgung fällt aus (Pumpen)
5. Lebensmittelversorgung fällt aus
6. ...

Interdependenzen: Systeme sind wechselseitig abhängig

Beispiel:

1. DNS Single Sign On fällt aus.
2. Restore kann nicht mehr angesprochen werden, da auf `restore.firma.com`
3. DNS kann *also auch* nicht mehr wiederaufgesetzt werden, da kein Restore.

KRITIS Aufgaben für den Informatiker

Für den Informatiker folgen daraus diverse Pflichten

1. Identifikation kritischer Systeme und ihrer Abhängigkeiten
2. Implementierung von Sicherheitsmaßnahmen (Updates, Firewall, Verschlüsselung)
3. Meldepflicht bei Sicherheitsvorfällen binnen 24 Stunden an das BSI.
4. Erstellung von Plänen für Notfall und Wiederherstellung
5. Sensibilisierung und Schulung von Mitarbeitern
6. Umsetzung branchenspezifischer Sicherheitsstandards
7. Seit kurzem: Besonderer Schutz von Kundendaten im Web

Informationsfreiheit

Das **Informationsfreiheitsgesetz** regelt in Deutschland den Anspruch auf Zugang zu amtlichen Informationen.

Voraussetzungsloser Rechtsanspruch auf Zugang zu amtlichen Informationen von Bundesbehörden.

Diverse **Einschränkungen**:

1. Nur abgeschlossene und dokumentierte Vorgänge
2. Schranken für behördliche Entscheidungsprozesse
3. Schranken für besondere öffentliche Belange
4. Schranken für personenbezogene Daten (Bsp: Personalakte)
5. Schranken für betriebsbezogene Daten (Bsp: Betriebsgeheimnisse)

Anhang

Übersicht

Verzeichnis aller Abbildungen (1/2)

Rechtsnachweise

Abb. 1 Quelle: Wikipedia, public domain.

Abb. 2 Quelle: https://en.wikipedia.org/wiki/Presidio_Modelo Friman. CC BY-SA 3.0

Abb. 3 Quelle: https://en.wikipedia.org/wiki/Presidio_Modelo Friman. CC BY-SA 3.0

Abb. 4 Eigene Skizze

Abb. 7 Quelle: https://www.digitalinformationworld.com/2024/04/gpt-4-outperforms-humans-in-persuasion.html

Abb. 8 Screenshot

Abb. 9 Screenshot

Abb. 10 Screenshot

Rechtliche Hinweise (1)

Die hier angebotenen Inhalte unterliegen deutschem Urheberrecht. Inhalte Dritter werden unter Nennung der Rechtsgrundlage ihrer Nutzung und der geltenden Lizenzbestimmungen hier angeführt. Auf das Literaturverzeichnis wird verwiesen. Das Zitatrecht in dem für wissenschaftliche Werke üblichen Ausmaß wird beansprucht. Wenn Sie eine Urheberrechtsverletzung erkennen, so bitten wir um Hinweis an den auf der Titelseite genannten Autor und werden entsprechende Inhalte sofort entfernen oder fehlende Rechtsnennungen nachholen. Bei Produkt- und Firmennamen können Markenrechte Dritter bestehen. Verweise und Verlinkungen wurden zum Zeitpunkt des Setzens der Verweise überprüft; sie dienen der Information des Lesers. Der Autor macht sich die Inhalte, auch in der Form, wie sie zum Zeitpunkt des Setzens des Verweises vorlagen, nicht zu eigen und kann diese nicht laufend auf Veränderungen überprüfen.

Alle sonstigen, hier nicht angeführten Inhalte unterliegen dem Copyright des Autors, Prof. Dr. Clemens Cap, ©2020. Wenn Sie diese Inhalte nützlich finden, können Sie darauf verlinken oder sie zitieren. Jede weitere Verbreitung, Speicherung, Vervielfältigung oder sonstige Verwertung außerhalb der Grenzen des Urheberrechts bedarf der schriftlichen Zustimmung des Rechteinhabers. Dieses dient der Sicherung der Aktualität der Inhalte und soll dem Autor auch die Einhaltung urheberrechtlicher Einschränkungen wie beispielsweise Par 60a UrhG ermöglichen.

Die Bereitstellung der Inhalte erfolgt hier zur persönlichen Information des Lesers. Eine Haftung für mittelbare oder unmittelbare Schäden wird im maximal rechtlich zulässigen Ausmaß ausgeschlossen, mit Ausnahme von Vorsatz und grober Fahrlässigkeit. Eine Garantie für den Fortbestand dieses Informationsangebots wird nicht gegeben.

Die Anfertigung einer persönlichen Sicherungskopie für die private, nicht gewerbliche und nicht öffentliche Nutzung ist zulässig, sofern sie nicht von einer offensichtlich rechtswidrig hergestellten oder zugänglich gemachten Vorlage stammt.

Use of Logos and Trademark Symbols: The logos and trademark symbols used here are the property of their respective owners. The YouTube logo is used according to brand request 2-9753000030769 granted on November 30, 2020. The GitHub logo is property of GitHub Inc. and is used in accordance to the GitHub logo usage conditions https://github.com/logos to link to a GitHub account. The Tweedback logo is property of Tweedback GmbH and here is used in accordance to a cooperation contract.

Rechtliche Hinweise (2)

Disclaimer: Die sich immer wieder ändernde Rechtslage für digitale Urheberrechte erzeugt ein nicht unerhebliches Risiko bei der Einbindung von Materialien, deren Status nicht oder nur mit unverhältnismäßig hohem Aufwand abzuklären ist. Ebenso kann den Rechteinhabern nicht auf sinnvolle oder einfache Weise ein Honorar zukommen, obwohl deren Leistungen genutzt werden.

Daher binde ich gelegentlich Inhalte nur als Link und nicht durch Framing ein. Lt EuGH Urteil 13.02.2014, C-466/12 (Pressemitteilung, Blog-Beitrag, Urteilstext). ist das unbedenklich, da die benutzten Links ohne Umgehung technischer Sperren auf im Internet frei verfügbare Inhalte verweisen.

Wenn Sie diese Rechtslage stört, dann setzen Sie sich für eine Modernisierung des völlig veralteten Vergütungs- und Anreizsystems für urheberrechtliche Leistungen ein. Bis dahin klicken Sie bitte auf die angegebenen Links und denken Sie darüber nach, warum wir keine für das digitale Zeitalter sinnvoll angepaßte Vergütungs- und Anreizsysteme digital erbrachter Leistungen haben.

Zu Risiken und Nebenwirkungen fragen Sie Ihren Rechtsanwalt oder Gesetzgeber.

Weitere Hinweise finden Sie im Netz hier und hier oder hier.

Zitierweise dieses Dokuments

Wenn Sie Inhalte aus diesem Werk nutzen oder darauf verweisen wollen,
zitieren Sie es bitte wie folgt:

Clemens H. Cap: Privatheit und Datenschutz. Electronic document. https://iuk.one/2913.pdf
16. 1. 2025.

Bibtex Information: https://iuk.one/2913.pdf.bib

```
@misc{doc:2913.pdf,
   author       = {Clemens H. Cap},
   title        = {Privatheit und Datenschutz},
   year         = {2025},
   month        = {1},
   howpublished = {Electronic document},
   url          = {https://iuk.one/2913.pdf}
}
```

Typographic Information:
Typeset on ?today?
This is pdfTeX, Version 3.14159265-2.6-1.40.21 (TeX Live 2020) kpathsea version 6.3.2
This is pgf in version 3.1.5b
This is preamble-slides.tex myFormat©C.H.Cap

Verzeichnis aller Folien

Legende:
Fortsetzungsseite
Seite ohne Überschrift
Bildseite