Datenschutz

Fragen zur Umsetzung der DSGVO

16.06.2021

Dr. Kurt Einzinger

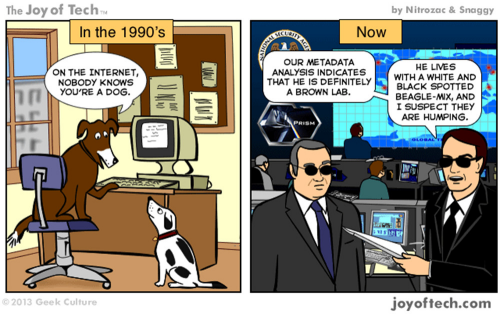
Dr. Kurt Einzinger

- Technologisches Gewerbe Museum (TGM) Wien, Fachbereich Atomenergietechnik
- Doktorat Ethnologie Universität Wien (Diss: Sikhs in Indien)
- EDV-Leiter einer politischen Partei (1989 – 1996)
- EDV-Abteilungen von Banken (GiroCredit, EB, OeKB)
- Generalsekretär der ISPA (Internet Service Providers Austria) – EuroISPA (Brüssel)
- Mitglied des Österreichischen Datenschutzrates (seit 1990)
- Member of Permanent Stakeholders Group of ENISA (European Network and Information Security Agency) (2004-2008, 2017-2020)
- Cyber Security Forschungsprojekte (CAIS, CIIS,CISA)
- netelligenz – Datenschutz und Cyber Security Beratung
- Externer Datenschutzbeauftragter

Disclaimer

On the Internet,
Nobody Knows You're a Dog

page 61 of July 5, 1993 issue of The New Yorker, (Vol.69 (LXIX) no. 20)



Haftungsausschluß: Die Thesen und Ausführungen des Vortrags stellen ausschließlich die Meinung und Ansichten des Vortragenden dar. Für deren Inhalt wird keinerlei Haftung übernommen. Die darin enthaltenen Informationen stellen keine Rechts-, Anlage- oder sonstige Beratung dar, noch sollten auf Grund dieser Angaben Anlage- oder sonstige Entscheidungen gefällt werden, sondern sie gelten lediglich als unverbindliche Information.

Inhalt

- Worum geht‘s ?
- Grundbegriffe des Datenschutzes
- Speicherbegrenzung / Löschung
- Pseudonymisierung vs. Anonymisierung
- Die Umsetzung der Cookie Regeln
- Datenschutz in Zeiten von Covid-19

Wozu Datenschutz?

- Schutz der Privatsphäre
- Missbrauch verhindern
- Informatielle Selbstbestimmung
  - Ausdrückliche Einwilligung
  - Informationspflichten und Transparenz
  - Betroffenenrechte
  - Beschwerderecht und Schadenersatz
- gleiches Recht in Europa

Datenschutz-Bestimmungen

- Datenschutz-Grundverordnung (DSGVO)
- Datenschutzgesetz (DSG)
- Datenschutzanpassungsgesetze
- Materiengesetze (TKG, ECG etc.)
- E-Privacy Richtlinie (bald Verordnung)
- Gerichtsurteile (EUGH, VwGH, Verwaltungsgerichte)
- Entscheidungen der Datenschutzbehörde
- Rechtsvorrang der EU-Bestimmungen

personenbezogene Daten

alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; (Art 4 lit 1 DSGVO)

Verarbeitung

bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten (Art 4 lit 2 DSGVO)

Verantwortlicher

Jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet

Auftragsverarbeiter

Jeder, der personenbezogene Daten im Auftrag eines Verantwortlichen verarbeitet

Sensible Daten - Art.9 DSGVO

Daten, über die **rassische** und **ethnische** Herkunft**, politische Meinungen**, **religiöse oder weltanschauliche Überzeugungen** oder die **Gewerkschaftszugehörigkeit**.

Genetische Daten, **biometrische** Daten zur eindeutigen Identifizierung einer natürlichen Person, **Gesundheitsdaten** oder Daten zum **Sexualleben oder der sexuellen Orientierung**

sind besonders geschützt.

 9

Anwendungsbereich

ganz oder teilweise automatisierte und nicht-automatisierte Verarbeitung personenbezogener Daten natürlicher Personen, die in einem **Dateisystem** gespeichert sind oder gespeichert werden sollen,… § 4 (1) DSG

Nicht Anwendbar

- Bei ausschließlich persönlichen oder familiären Tätigkeiten, (Art 2 DSGVO)
- Daten juristischer Personen
- Daten Verstorbener (keine natürliche Person)
- Anonymisierte Daten

 10

Grundsätze für die Verarbeitung personenbezogener Daten (Art 5 DSGVO)

1. Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz;
2. Zweckbindung;
3. Datenminimierung;
4. Richtigkeit;
5. Speicherbegrenzung – nur so lange als nötig;
6. Integrität und Vertraulichkeit - Sicherheit;
7. Rechenschaftspflicht

Rechtmäßigkeit der Verarbeitung

a) Einwilligung (Nachweispflicht)

b) Erfüllung eines Vertrags, oder vorvertragliche Maßnahmen

c) Erfüllung einer rechtlichen Verpflichtung

d) lebenswichtige Interessen der Person

e) öffentliches Interesse oder Ausübung öffentlicher Gewalt

f) berechtigte Interessen des Verantwortlichen, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen, insbesondere bei Kindern.

Speicherbegrenzung - Löschung

Personenbezogene Daten müssen unwiderruflich gelöscht oder anonymisiert werden wenn

a) sie für den Zweck der Verarbeitung nicht mehr benötigt werden (keine Rechtsgrundlage)
b) keine gesetzliche Verpflichtung zur Aufbewahrung besteht,
c) die Einwilligung widerrufen wird (bei auf Einwilligung beruhenden Verarbeitungen)
d) das Recht auf Löschung (Art 17 DSGVO) geltend gemacht wird und Punkt a und b zutrifft

 13

Arten der Löschung

- Einschränkung der Verarbeitung (ErwG 67 DSGVO, § 4 (2) DSG)
- Anonymisierung – Personenbezug ist nicht mehr vorhanden
- Physische Löschung - Vernichtung
- Recht auf Vergessenwerden – Empfänger und Auftragsverarbeiter
- Automatische – Manuelle Löschung

 14

Löschung - Einschränkung

§ 4 (2) DSG

Kann die **Berichtigung oder Löschung** von automationsunterstützt verarbeiteten personenbezogenen Daten **nicht unverzüglich erfolgen**, weil diese aus wirtschaftlichen oder technischen Gründen nur zu bestimmten Zeitpunkten vorgenommen werden kann, so ist die Verarbeitung der betreffenden personenbezogenen Daten mit der Wirkung nach Art. 18 Abs. 2 DSGVO bis zu diesem Zeitpunkt **einzuschränken.**

Löschkonzept

Es sind folgende Punkte zu beachten:

- Erfassung der Datenkategorien (in Verbindung mit dem Verarbeitungsverzeichnis)
- Ort der physischen Speicherung der Daten
- Speicherdauer /Löschfrist je Datenkategorie
- Art der Löschung entsprechend den technischen Möglichkeiten
- Löschorganisation festlegen:
  a) Automatisch (Batch jobs)
  b) Inventur (festgesetzte Löschtage)
  c) Auftragsverarbeiter anweisen

Pseudonymisierung vs. Anonymisierung

Die technischen Verfahren und Prozesse sind bei Pseudonymisierung und Anonymisierung im Grunde dieselben.

Eine Anonymisierung ist eigentlich eine Pseudonymisierung wobei die ursprünglichen Daten (Beziehungen) nicht mehr wieder hergestellt werden können.

Bei Pseudonymisierung wird der Auflösungs-Algorithmus, -Schüssel oder -Tabelle aufgehoben, bei Anonymisierung wird er vernichtet.

Pseudonymisierung

die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können (Art 4 lit 5 DSGVO)

Einer Pseudonymisierung unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, sollten als Informationen über eine identifizierbare natürliche Person betrachtet werden. (Erwägungsgrund 26 DSGVO)

Pseudonymisierung (2)

Die Pseudonymisierung wird verwendet als Sicherheitsmaßnahme bei Datenspeicherung

- in mobilen Geräten
- Datenträgern
- Cloud

Pseudonymisierte Daten sind nach wie vor personenbezogen und unterliegen dem Datenschutz

Pseudonymisierungstechniken

1. **Deterministische Pseudonymisierung**: in allen DB und bei jedem Vorkommen, wird Id immer mit denselben Pseudonym $pseudo$ ersetzt.
2. **Zufällige Pseudonymisierung**: jedes mal wenn Id in einer DB vorkommt wird es mit einem unterschiedlichen Pseudonym ($pseudo1$, $pseudo2$,...) ersetzt; aber, die gleiche Id wird immer mit dem gleichen ($pseudo1$, $pseudo2$) in allen DBs ersetzt.
3. **Vollständig Zufällige Pseudonymisierung**: Jedes Vorkommen von Id wird mit einem unterschiedlichen Pseudonym ($pseudo1$, $pseudo2$) ersetzt.

Pseudonymisierungstechniken (2)

1.Zähler: Id wird mit fortlaufender Zahl ersetzt (nur für kleine DBs)

2.Random Number Generator (RNG): jeder Id wird durch eine Zufallszahl ersetzt.

3.Cryptographic hash function: wird für jeden Id angewandt -> Ein-Weg und kollisionsfrei – kann durch brute force oder Dictionary Attacken kompromittiert werden

4.Message authentication code (MAC): wie hash function nur wird noch ein geheimer Schlüssel eingesetzt.

5.Symmetric encryption: Eine Blockverschlüsselung wird verwendet, um eine Kennung mit einem geheimen Schlüssel zu verschlüsseln, der sowohl das Pseudonymisierungs-geheimnis als auch das Wiederherstellungsgeheimnis ist.

Anonymisierung

Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d.h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann.
(Erwägungsgrund 26 DSGVO)

Anonymisierung (2)

Aus Bescheid der Datenschutzbehörde (DSB)

„Die Entfernung des Personenbezugs („Anonymisierung“) von personenbezogenen Daten kann somit grundsätzlich ein mögliches **Mittel zur Löschung** iSv Art. 4 Z 2 iVm Art. 17 Abs. 1 DSGVO sein. Es muss jedoch sichergestellt werden, dass weder der Verantwortliche selbst, noch ein Dritter ohne unverhältnismäßigen Aufwand einen Personenbezug wiederherstellen kann.“
(GZ: DSB-D123.270/0009-DSB/2018 vom 5.12.2018)

Dr. Kurt Einzinger

Anonymisierung (3)

Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern.
Alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, sollten herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind

Dr. Kurt Einzinger

Anonymisierung (4)

Zwei Denkschulen:

- **Fundamentalistische**: es darf keine theoretische Möglichkeit mehr geben um den Personenbezug wiederherstellen zu können
- **Praktische**: Personenbezug darf mit rechtlich zulässigen Mitteln und ohne unverhältnismäßigem Aufwand nicht wiederherstellbar sein. (z.B. Einweg-Hash mit secret key)

Dr. Kurt Einzinger

Cookies

Unter Cookies wird verstanden:

- Kleine Textdatei, die im Browser des Benutzers gespeichert (abgelegt) wird.
- Jede Art von Identifikationskennzeichnung wie auch z.B. Fingerprinting
- Java script code, der Cookies setzt und Verhaltensdaten überträgt (z.B. fbpixels)
- Übertragung von Nutzerdaten an Dritte (z.B. SaS, Embeddings an Social Media)
- 3 Arten: Essentiell - Analyse - Marketing
- Kleine süße Backwaren

Dr. Kurt Einzinger

Cookie Detection

Festzustellen, ob eine Webseite Cookies setzt, ist sehr einfach und kann sowohl bei Besuch der Webseite als auch von extern gemacht werden.

Bei Besuch der Webseite

1. Im Cookie Container des Browsers nachsehen (z.B. bei Chrome: chrome://settings/siteData)
2. Mit Browser PlugIns (z.B. Cookie Editor bei Chrome)
3. Facebook Pixel Helper (PlugIn von facebook)

Mit externen Programmen

1. https://www.cookieserve.com
2. https://cookiemetrix.com
3. https://cookiepedia.co.uk/
4. https://www.cookiebot.com/
5. http://urlscan.io (umfangreiche Website Analyse)

Cookie Rechtslage

Bei der Verwendung von Cookies sind grob drei Verarbeitungsvorgänge, für die eine Rechtsgrundlage gegeben sein muss, üblich.

Verarbeitungsvorgänge bei Verwendung von Cookies

1. Das Cookie in den Container des Browsers setzen
2. Das Cookie auslesen und die Daten verarbeiten (Analyse, Tracking)
3. Die Daten des Cookies (und mehr) an Dritte übertragen

Für jede Verarbeitung ist eine Rechtmäßigkeit notwendig und der Benutzer muss darüber informiert werden.

1. Fürs Cookie-Setzen: e-Privacy RL / § 96 Abs 3 TKG – Ausdrückliche Einwilligung (außer für essentielle Cookies)
2. Fürs Tracking: Art 6 lit a – Ausdrückliche Einwilligung
3. Für Datenübertragung: wie 2 plus der Problematik bei Drittstaaten muss gleiches Datenschutzniveau sein.

Cookies – Was ist zu tun ?

Essentielle/Funktionale Cookies

- nur Information darüber (Cookie-Banner oder Datenschutzerklärung)

Marketing Cookies

- klare und umfassende Informationen über die Zwecke der Verarbeitung
- ausdrückliche Einwilligung (EU Rechtsvorrang)
- Zustimmung muss zuerst erfolgt sein, erst dann darf Cookie gesetzt werden
- Personen, die diese Zustimmung nicht erteilen, dürfen deshalb keine Nachteile erleiden
- die Zustimmung muss jederzeit und einfach widerrufbar sein -> Cookie ist zu entfernen

 29

Analyse Cookies – Was ist zu tun ?

Analyse Cookies

- Wenn die Daten selbst verarbeitet und aggregiert werden (Statistik z.B. Matomo) -> Information
- Wenn die Daten vor Übermittlung anonymisiert werden (nur statistische Daten) -> Information
- Wenn dadurch personenbezogene Daten an Dritte übermittelt werden (z.B. Google Analytics) -> Information & ausdrückliche Zustimmung
- bei Personen, die diese Zustimmung nicht erteilen, dürfen keine Cookies gesetzt werden und sie dürfen deshalb keine Nachteile erleiden
- die Zustimmung muss jederzeit und einfach widerrufbar sein -> Cookie ist zu entfernen

 30

Der Cookie-Banner

Das Mittel zur Einhaltung der Cookie-Bestimmungen

- Beinhaltet die Information zu allen Cookies
- Die Einwilligung muss aktiv gesetzt werden
- Als Default gilt die Nicht-Einwilligung (Ablehnung)
- Auf der Hauptseite soll der Einwilligungs- und Ablehnungs-Button in gleicher Art ausgeführt sein
- Die Ablehnung aller Cookies darf nicht schwerer oder komplizierter sein als die Einwilligung
- Ohne Einwilligung darf kein Cookie gesetzt werden.
- Der Banner sollte nicht Funktionalitäten der Seite behindern (z.B. Links überdecken)
- Es muss eine einfache Möglichkeit geben um eine einmal erteilte Zustimmung jederzeit zu widerrufen.
- Laufende Aktion von noyb

 31

noyb Cookie-Banner Aktion

https://noyb.eu/en/noyb-aims-end-cookie-banner-terror-and-issues-more-500-gdpr-complaints

 32

Facebook Pixel

Das Facebook Pixel ist ein von der Firma Facebook zu Verfügung gestellter code (javascript), der vom Website Betreiber in den Header der Webseite eingefügt wird. Wenn ein Browser diese Seite mit dem Facebook Pixel lädt, wird dessen javascript code ausgeführt. Dadurch lädt der Browser weiteren javascript code (fbevents.js) vom Facebook Server, der ebenfalls vom Browser des Nutzers ausgeführt wird.

Es wird ein Cookie im Browser des Nutzers gesetzt und die Daten des Browsers (IP-Adresse, referrer, browser-Einstellungen, page location, document, und Person, die den Browser benutzt) werden an Facebook übermittelt

Aktivitäten außerhalb von Facebook

Als Aktivitäten außerhalb von Facebook bezeichnet Facebook Informationen zu deinen Interaktionen mit Unternehmen und Organisationen, die letztere mit uns teilen.

Auf Facebook Konto gehen und folgendes klicken:

- Einstellungen
- Deine Facebook Informationen
- Aktivitäten außerhalb von Facebook (Ansehen)
- Deine Aktivitäten außerhalb von Facebook verwalten
- Passwortabfrage

Facebook Off-Activities

Anzahl der erhaltenen Interaktionen: Interaktionen sind Handlungen, die du auf einer Website oder in einer App vorgenommen hast. Hier sind einige Beispiele für Interaktionen:

- Das Öffnen einer App
- Das Einloggen in eine App mit Facebook
- Das Ansehen von Inhalten
- Die Suche nach Artikeln
- Das Hinzufügen eines Artikels zum Einkaufswagen
- Der Kauf eines Artikels
- Das Spenden eines Geldbetrags

Facebook Custom Audiences

Facebook bietet noch weitere Möglichkeiten des Nutzer-trackings und der Erweiterung von Zielgruppen an. Dies wird von Facebook als „Custom Audiences“ und „Lookalike Audiences“ (Erweiterter Abgleich) bezeichnet. Dazu muss der Website Betreiber in das Facebook pixel der jeweiligen Seite eintragen welche Daten bei welchen Aktionen an Facebook geschickt werden sollen. (Button Click Data)

Was Facebook genau mit diesen Daten macht, ist nicht dokumentiert. Seinen Anzeigenkunden bietet Facebook an, sogenannte „Custom Audiences“ zusammenzustellen. Das sind Gruppen von Personen (Facebook Nutzern), denen man als Zielgruppe Werbung schalten kann.

Verwendung Facebook Pixel

- Information der Betroffenen über Funktionalität des Facebook Pixels
- Wenn Button-Click-Data übertragen werden -> Information der Betroffenen welche Daten übertragen werden.
- **ausdrückliche Einwilligung** vor dem Setzen des Cookies und Ausführung des js-codes notwendig. Dazu muss der js-code erweitert werden

Es dürfen auf keinen Fall sensible Daten mittels Button-Click-Data übertragen werden.

Privacy by Design

Privacy by Design stützt sich auf die Auffassung, dass Datenschutz nicht allein durch die Einhaltung von Rechtsvorschriften gewährleistet werden kann. Vielmehr sollte idealerweise die Gewährleistung des Datenschutzes zum Standardbetriebsmodus jeder Organisation werden.

1. Proaktiv, nicht reaktiv; als Vorbeugung und nicht als Abhilfe
2. Datenschutz als Standardeinstellung
3. Der Datenschutz ist in das Design eingebettet
4. Volle Funktionalität – eine Positivsumme, keine Nullsumme keine falschen Dichotomien wie Datenschutz versus Sicherheit
5. Durchgängige Sicherheit - Schutz während des gesamten Lebenszyklus
6. Sichtbarkeit und Transparenz – Für Offenheit sorgen
7. Die Wahrung der Privatsphäre der Nutzer – Für eine nutzerzentrierte Gestaltung sorgen

Das gelindeste Mittel

Im Artikel 1 (Verfassungsbestimmung) des DSG wird normiert, dass der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden darf.

Das verpflichtet den Verantwortlichen zu überprüfen ob der gleiche oder ähnliche Effekt nicht auch durch eine datenschutzrechtlich gelindere Maßnahme durchgeführt werden kann.

Covid-19 Datensammlungen

- Register der anzeigepflichtigen Krankheiten (§4 Epidemiegesetz) – bestand schon
- Statistik Register (§ 4a Epidemiegesetz) - neu
- Zentrales Impfregister (§ 24c Gesundheitstele-matikgesetz) - neu
- EPI-Service für Covid-19 Zertifikate -3G (§ 4b Abs 3 Epidemiegesetz) - neu
- Register für Screeningprogramme (§ 5b Epidemigesetz) - neu

Register der anzeigepflichtigen Krankheiten

Im Register (§ 4 Epidemiegesetz) werden folgende Daten verarbeitet:

- Daten zur Identifikation von Erkrankten, einer Erkrankung Verdächtigen, Gebissenen oder Verstorbenen (Name, Geschlecht, Geburtsdatum, Wohnsitz, Telefonn., E-Mail, SVN und bPK
- gegebenenfalls Sterbedaten (Datum, Todesursache, Autopsiestatus),
- die für die anzeigepflichtige Krankheit relevanten klinischen Daten (Vorgeschichte, Krankheitsverlauf) + neg. Testergebnisse SARS-CoV-2.
- Daten zum Umfeld des Erkrankten, soweit sie in Bezug zur anzeigepflichtigen Erkrankung stehen, Daten zur Identifikation von Kontaktpersonen (Name, Telefonnummer, E-Mail, Wohnsitz)
- Daten zu den getroffenen Vorkehrungsmaßnahmen.

Die Daten im Register sind zu löschen, sobald sie zur Erfüllung der Aufgaben der Bezirksverwaltungsbehörden im Zusammenhang mit der Erhebung über das Auftreten und im Zusammenhang mit der Verhütung und Bekämpfung einer anzeigepflichtigen Krankheit nach diesem Bundesgesetz nicht mehr erforderlich sind.

 41

Covid-19 Daten beim Arbeitgeber

- Rechtsgrundlage: Fürsorgepflicht im ArbeitnehmerInnen-schutzgesetz (ASchG)
- Ermittlung der Risikoarbeitnehmer (Angehörige der Risikogruppen)
- Bei verordneter Quarantäne: Anspruch auf laufendes Entgelt nach Entgeltfortzahlungsgesetzes (EFZG)
- Home-Office Anpassung in verschiedenen Gesetzen (ab 1.4.2021)
- Organisation von Impfprogrammen
- 3 G Status der Beschäftigten

Zu beachten: Datenminimierung und gelindestes Mittel

 42

Danke

Dr. Kurt Einzinger
ke@netelligenz.at