IHK - Webinar

Pseudonymisierung, Anonymisierung und Löschung von personenbezogenen Daten - Datenschutzanforderungen und praktische Vorteile

RA Dr. Carsten Siara

Löschung, Anonymisierung und Pseudonymisierung im Datenschutzrecht

Gliederung

A. Grundsätzliches

B. Löschung

1. Um welche personenbezogenen Daten geht es?
2. Warum muss man Daten löschen
3. Was ist der Zweck, der zur Speicherung berechtigt?
4. Gesetzliche Aufbewahrungspflichten
5. Beispiele für gesetzliche Aufbewahrungspflichten
6. Zusammenfassung
7. Löschkonzept
8. Wie funktioniert Löschung?

C. Anonymisierung

1. Grundsätzliches zur Anonymisierung
2. Wer braucht‘s?
3. Methoden der Anonymisierung
4. Anwendungsfall Bewerberdaten
5. Anwendungsfall KI-Training

D. Pseudonymisierung

1. Pseudonymisierte Daten als personenbezogene Daten
2. Wofür braucht man Pseudonymisierung?
3. Verfahren zur Pseudonymisierung (Beispiele)

E. Fundstellen

A. Grundsätzliches

Im Datenschutzrecht dreht sich alles um den Begriff der **personenbezogenen Daten (pD)**.

> Art. 4 Nr. 1 DSGVO: alle Informationen, die sich auf eine **identifizierte oder identifizierbare** natürliche Person (im Folgenden „betroffene Person“) beziehen.

Entscheidend ist das Merkmal „identifizierbar“, das weit ausgelegt wird:

1) Alle (technischen) Mittel zur Identifikation , die **irgendwo auf der Welt zur Verfügung** stehen und

2) die die Verantwortlichen oder andere Stellen **wahrscheinlich nutzen**, d. h. Identifizierung darf keinen unverhältnismäßig hohen Aufwand (Zeit, Geld, Arbeitskraft) verursachen.

Z. B. EuGH im Urteil C-582/14 („Breyer“): **Dynamische IP-Adressen** sind personenbezogene Daten, auch wenn die zur Identifizierung der Personen erforderlichen Zusatzinformationen bei einem Dritten (nämlich Internet Access Provider) liegen.

A. Grundsätzliches

In diesem Zusammenhang haben die Begriffe Löschung, Anonymisierung und Pseudonymisierung im Datenschutzrecht große Bedeutung.

Zum Teil definieren sie die Reichweite des Datenschutzrechts, zum Teil dienen sie als technische Maßnahmen zur Datensicherheit. Gemeinsam ist den drei Konzepten, dass sie der Begrenzung der Datenverarbeitung und der Sicherung gegen unbefugte Zugriffe dienen.

Wir wollen zeigen,

- was die einzelnen Begriffe bedeuten,
- wo im Datenschutz sie relevant werden,
- wie praktische Umsetzungen aussehen.

A. Grundsätzliches

Löschen: „Prozess, durch den personenbezogene Daten derart irreversibel verändert werden, dass sie nach dem Vorgang nicht mehr vorhanden oder unkenntlich sind und nicht mehr verwendet oder rekonstruiert werden können.“ (DIN 66398:2016-05).

Anonymisierung: Verändern der Daten in solch einer Art und Weise, dass ein Rückschluss auf die Person gar nicht oder zumindest nur noch mit unverhältnismäßig hohem Aufwand möglich ist.

Pseudonymisierung: Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt und gesichert werden (Art. 4 Nr. 5 DSGVO)

B. Löschung

1. Um welche personenbezogenen Daten geht es?

Unternehmen speichern und verarbeiten – je nach Unternehmensgegenstand – unterschiedliche personenbezogener Daten:

- Beschäftigtendaten (z. B. Name, Anschrift, Telefonnummer, Entgeltdaten, Arbeitszeitkonten, Krankendaten)
- Kundendaten
- Lieferantendaten
- Geschäftliche Korrespondenz
- Vertragsunterlagen
- E-Mails
- LogFiles: Server speichern automatisch Systemzugriffe; darin können personenbezogene Daten enthalten sein (z. B. IP-Adressen, Teile von Benutzerkennungen)

Die Daten werden idR benötigt, um den Geschäftsbetrieb ordnungsgemäß zu führen.

B. Löschung

2. Warum muss man Daten löschen?

Grundprinzip: Verbot mit Erlaubnisvorbehalt, Art. 6 Abs. 1 S. 1 DSGVO

Zweckbindung, Art. 5 Abs. 1 lit. b DSGVO

Datenmini-mierung, Art. 5 Abs. 1 lit c DSGVO

Richtigkeit, Art. 5 Abs. 1 lit. d DSGVO

Speicherbe-grenzung, Art. 5 Abs. 1 lit. e DSGVO

ErwGrund 39 S. 7 u. 8 DSGVO: Die personenbezogenen Daten sollten für die Zwecke, zu denen sie verarbeitet werden, (…) auf das für die Zwecke ihrer Verarbeitung notwendige Maß beschränkt sein. Dies erfordert insbesondere, dass die Speicherfrist für personenbezogene Daten auf das unbedingt erforderliche Mindestmaß beschränkt bleibt.

B. Löschung

Daraus folgt:
Personenbezogene Daten sind nach dem Wegfall oder Erreichen des Zwecks, für den sie erforderlich waren, zu löschen.
=> s. a. Art. 17 Abs. 1 lit a DSGVO

> Übrigens: **Rechtsgrundlage für die Löschung** ist Art. 6 Abs. 1 lit c DSGVO: Insbesondere Grundsätze der Zweckbindung, Datenminimierung und Speicherbegrenzung begründen rechtliche Verpflichtungen zur Datenlöschung.

Alles klar, oder?

B. Löschung

3. Was ist der Zweck, der zur Speicherung berechtigt?

Voraussetzungen für die Verarbeitung von pD:

a. Rechtsgrundlage muss vorliegen (z. B. Art. 6 Abs. 1 lit. c oder lit. f DSGVO).

b. Daraus leitet sich der Zweck für die Verarbeitung ab.

Solange ein **legitimer Zweck** die Datenverarbeitung rechtfertigt (und keine überwiegenden Interessen auf Seiten des Betroffenen entgegenstehen), besteht keine Verpflichtung zur Löschung der personenbezogenen Daten.

Im Gesetz nicht definiert. Erfasst sind nach allgemeiner Ansicht grundsätzlich alle Zwecke, die im weitesten Sinne rechtskonform sind (so bereits Artikel-29-Datenschutzgruppe WP 203, S. 20).

B. LÖSCHUNG

Beispiele für legitime Zwecke und Aufbewahrungsrechte

Unterlagen zur Berechnung des Handelsvertreterausgleichsanspruchs, § 89b HGB	Grundsätzlich Aufbewahrungsrecht, solange Möglichkeit der Geltendmachung besteht, d. h. bis zum Ablauf der Verjährungsfrist, §§ 195, 199 Abs. 1 BGB. Kürzer z. B., wenn abschließender Vergleich geschlossen wurde.
Arbeitsverträge und vergleichbare wesentliche Unterlagen	Aufbewahrungsrecht zum Zweck der Wahrung eigener Rechte: Während des Bestehens des Arbeitsverhältnisses sowie danach bis zum Ablauf der Verjährung (max. 10 Jahre, vgl. § 199 Abs. 3 Nr. 1 BGB).
Nachweise zur Erfüllung von Ansprüchen aus Arbeitsverhältnissen (z. B. Fehlzeitennachweise zur Abrechnung von Entgeltfortzahlungen)	Aufbewahrungsrecht bis zum Ablauf der gesetzlichen Verjährung nach §§ 195, 199 Abs. 1 BGB.
Speicherung biometrischer Daten (Fingerprintsystem) zum Zweck der Abrechnungin einer Kantine	Löschung der Daten muss unmittelbar nach Begleichung des Rechnungsbetrags erfolgen!

B. LÖSCHUNG

4. Gesetzliche Aufbewahrungspflichten

Neben den legitimen Zwecken, die zur Aufbewahrung von Daten berechtigen, sind aber auch **gesetzliche Aufbewahrungspflichten** zu beachten.

Art. 6 Abs. 1 lit. c DSGVO gibt dem Verantwortlichen das Recht zur Verarbeitung von pD zur Erfüllung rechtlicher Verpflichtungen.

Art. 6 Abs. 2 DSGVO erlaubt Mitgliedsstaaten, dafür spezifischere Regelungen einzuführen.

Hiervon hat der Gesetzgeber ausgiebig Gebrauch gemacht, z. B. im Steuerrecht, Handelsrecht, Arbeitsrecht und Sozialrecht.

B. LÖSCHUNG

5. Beispiele für gesetzliche Aufbewahrungspflichten

Handels- und Geschäftsbriefe (d. h. sämtl. geschäftliche Korrespondenz, soweit sie sich auf Vorbereitung, Durchführung oder Rückgängigmachung eines Handelsgeschäfts bezieht)	Aufbewahrungspflicht: 6 Jahre – Steuerrechtl.: § 147 Abs. 1 Nr. 2 AO – Handesrechtl.: § 257 Abs. 1 Nr. 2 HGB
Bücher und diesbez. Aufzeichnungen, Inventare, Jahresabschlüsse, Lageberichte und Eröffnungsbilanz	Aufbewahrungspflicht: 10 Jahre – Steuerrechtl.: § 147 Abs. 1 Nr. 1 AO – Handesrechtl.: § 257 Abs. 1 Nr. 1 HGB
Arbeitsschutz im Unternehmen Dokumentation von Erste-Hilfe-Leistungen	Aufbewahrungspflicht: 5 Jahre § 24 Abs. 6 DGUV Vorschrift 1
Sozialversicherungsrechtliche Abrechnungsunterlagen	Sozialversicherungsrechtlich: Ablauf des auf die letzte Prüfung durch die RV folgenden Kalenderjahrs, § 28 f SGB IV
Unterlagen aus gesetzlicher Unfall-versicherung, die für Beitragsrechnun-gen relevant sind.	5 Jahre (§ 165 Abs. 4 SGB VII)

B. LÖSCHUNG

6. Zusammenfassung

Maßgeblich für die Löschfristen sind also

Aufbewahrungsrechte: Bestimmen sich nach dem jeweiligen Zweck der Verarbeitung => Verantwortlicher darf Unterlagen mit pD aufbewahren, kann sie aber auch vorher löschen.

Aufbewahrungspflichten, die sich aus Gesetz ergeben. Dies sind Mindestaufbewahrungsfristen, eine vorherige Löschung wäre rechtswidrig. Minimumfristen für Aufbewahrung.

Lösung:

- [ ] Jeden Tag alle personenbezogenen Daten durchgehen und entscheiden, ob sie gelöscht werden müssen?
- [X] Implementierung eines Löschkonzepts?

B. LÖSCHUNG

7. Löschkonzept

a) Was sind die Vorteile eines Löschkonzepts?

- Ermöglicht Implementierung standardisierter Löschregeln in Abhängigkeit von Datenarten.
- Ermöglicht die Einführung automatisierter Verfahren.
- Wird als zulässige Methode angesehen, um Komplexität zu reduzieren.
- Dokumentation der Löschregeln => macht Aufsichtsbehörden froh!

b) Auf welche Dateneinheit bezieht sich die Löschpflicht?

- Grds.: Einzelnes personenbezogenes Datum
- Sind mehrere Daten in einem Datenträger vorhanden, die nicht ohne weiteres isoliert löschbar sind (z. B. Schreiben, E-Mail, Schriftsatz, Blockchaintechnik), ist gesamtes Dokument Objekt der Löschung. Umgekehrt bestimmen sich aber auch legitimer Zweck und Aufbewahrungspflicht anhand des Gesamtdokuments.

B. LÖSCHUNG

Wie erstellt man ein Löschkonzept?

- Datenverantwortlicher (interne Zuständigkeit)
- Kategorien personenbezogener Daten und der Dokumente
- Schutzklassen der Daten: Relevant für Anforderungen an Löschung
- Verwendungszweck und Verarbeitungsprozess
- Verarbeitungsorte
- Klassifizierung der Systeme und Speicherorte
- Definition gesetzlicher Aufbewahrungspflichten
- Definition von Aufbewahrungsrechten
- Festlegung der Verarbeitungsvorgänge
- Festlegung der Löschungsvorgänge

Viele Softwarelösungen (z. B. MS 365, PVS) bieten die Möglichkeit, Löschvorgaben direkt einzupflegen.

B. LÖSCHUNG

Beispiel für ein Löschkonzept:

1.	Datum/Version des Löschkonzepts			
2.	Bezeichnung Verwendungszweck/Datenverarbeitungs prozess			
3.	Verantwortlicher			
4.	zuständig für Aktualisierung des Löschkonzeptes			
5.	interne/externe Zuständigkeit für Löschung (zuständiger Fachbereich, Mitarbeiter, Auftragsverarbeiter)			
6.	Weisungsgeber (Weisungsbefugter für die Anweisung zur Löschung)			
7.	Verarbeitungsorte			
8.	Speicherorte			
9.	Sicherungsdateien (zB ausgelagerte Backup-Dateien etc)			
10.	Datenträger			
11.	Auftragsverarbeiter			
12.	weitere Auftragsverarbeiter			
13.	Datenschutzbeauftragter			
14.	Kategorien personenbezogener Daten			
15.	Schutzklasse der Daten			

B. LÖSCHUNG

Festlegung der Verarbeitungsdauer		
16.	Aufbewahrungspflicht	
17.	Aufbewahrungsrecht	
18.	längere Verwendung iSv Art. 5 Abs. 1 lit. e, 17 Abs. 3 DS-GVO	
19.	konkrete Verarbeitungsdauer	
20.	Anlässe für Löschungen vor Ablauf der Verarbeitungsdauer	
Löschungsvorgang		
21.	Löschung	
22.	zu löschende Daten	
23.	Löschungsort	
24.	Soweit ein Transport erforderlich ist, sind Sicherungsmaßnahmen gegen Datenschutzverletzungen bei dem Transport zu dokumentieren.	
25.	Verantwortlicher für den Transport	
26.	Löschungsmethode	
27.	Verantwortung für Löschung	
28.	Dienstleister für Löschung	
29.	Verantwortung für Löschprotokoll	

[Quelle: Koreng/Lachenmann, Formularhandbuch Datenschutzrecht, 3. Auflage 2021]

B. LÖSCHUNG

8. Wie funktioniert Löschung?

Angesichts der technischen Möglichkeiten zur Rekonstruktion von Daten sind an Löschung hohe Anforderungen zu stellen.

Grundsätzlich zwei Alternativen:

(1) Physische Zerstörung des Datenträgers

(2) Magnetische Vernichtungsverfahren, idR durch Überschreiben => für effektives Löschen ist mehrfaches Überschreiben erforderlich.

Es geht bei Löschung nicht um absoluten Schutz, sondern darum, dass es **nach allgemeinem Ermessen unwahrscheinlich** ist, dass Zerstörung oder Überschreibung durch Unbefugte wieder rückgängig gemacht wird.

Je sensibler die Daten sind, desto höher sind die Anforderungen an den Löschvorgang.

Empfohlene Freeware (z. B.): „Darik‘s Boot and Nuke – DBAN“ oder „Parted Magic“

B. LÖSCHUNG

Detaillierte Hinweise zu Löschungsverfahren enthält **DIN 66399-1: 2012-10 (Kap. 5.1).**

Beispiele:

Papier, Microfiche, Microfilme	Schreddern Verbrennen
CD-ROM u. dgl.	Vollständiges Überschreiben physische Zerkleinerung: Partikel klein genug, um Rekonstruktion nach allgemeinem Ermessen unwahrscheinlich zu machen
Festplatte	mehrfaches vollständiges Überschreiben
RAM-/SRAM-Speicher	Trennung von der Stromversorgung bis zur vollständigen Entladung physische Zerkleinerung (empfohlene Partikelgröße $\leq$ 160 mm)
EPROM (z. B. elektronische Chipkarte)	Bestrahlung mit UV-Licht/Röntgenstrahlung vollständiges Überschreiben physische Vernichtung

C. ANONYMISIERUNG

1. Grundsätzliches zur Anonymisierung

Begriff (s. o.): Verändern der Daten in solch einer Art und Weise, dass ein Rückschluss auf die Person gar nicht oder zumindest nur noch mit unverhältnismäßig hohem Aufwand an Zeit, Kosten und Arbeitskraft möglich ist.

➡ Gegenteil von personenbezogenen Daten

Datenschutzrecht, insbesondere DSGVO nicht anwendbar

Anforderungen an fehlende Möglichkeit des Rückschlusses sind hoch:

- Maßgeblich sind nicht nur die Mittel und Kenntnisse des Verantwortlichen, sondern auch die Mittel und Kenntnisse anderer Stellen.
- Zu berücksichtigen ist der technische Fortschritt!

C. ANONYMISIERUNG

2. Wer braucht‘s?

Anders als bei Löschung sind noch Daten und Informationen vorhanden, mit denen man arbeiten kann, z. B.:

- Daten/Eigenschaften in einem Datensatz sollen weiter verwendet werden
- Weitergabe anonymisierter Daten
- Training von Algorithmen (z. B. KI!)
- Testen von Software

3. Methoden der Anonymisierung

Probleme stellen sich oft, wo es um eine Vielzahl von Datensätzen geht, die automatisiert anonymisiert werden müssen. Hier haben sich in der Praxis verschiedene Methoden etabliert, die oft in Kombination angewandt werden.

Personenbezug soll aufgehoben werden.

Statistische Eigenschaften der Daten sollen nicht verändert werden.

C. ANONYMISIERUNG

Veranschaulichung:

Guido Meier, Anwalt, 37 Jahre, wohnhaft in Baumstraße 11, 81375 München, Brillenträger

(1) [Name], Anwalt, 37 Jahre, wohnhaft in Baumstraße 11, 81375 München, Brillenträger

(2) [Name], Anwalt, 37 Jahre, wohnhaft in [81375], Brillenträger

(3) [Name], Anwalt, [30 bis 50 Jahre], wohnhaft in [81375], Brillenträger

Anonymisierung liegt idR nur dann vor, wenn **Originaldatensatz gelöscht** wird.

Es gibt **verschiedene Anonymisierungsmethoden** (s. nächstes Slide), die oft in Kombination eingesetzt werden.

TBC, welche Softwarelösungen, OSS-Lösungen oder Dienstleister verfügbar sind.

C. ANONYMISIERUNG

Vereinfachte Beispiele für Anonymisierungstechniken:

a) Stochastische Überlagerung:

Funktioniert nur bei nummerischen Werten. Dabei soll statistische Verteilung der ursprünglichen Werte erhalten bleiben.

Ursprünglicher Wert wird durch Anwendung eines zufälligen Werts aus einer gewissen Bandbreite verändert. Z. B.: ursprünglicher Wert + zufälliger Wert aus dem Bereich -15 bis +15 = veränderter Wert.

b) Vertauschung

Werte zwischen den Datensätzen werden vertauscht. Z. B. bei Beschäftigtendaten werden jeweils die Werte „Position“ und „Gehalt“ zwischen den Datensätzen 1, 2 und 3 getauscht, so dass der Bezug zwischen den Werten und der Person aufgehoben wird.

c) Generalisierung

Werte werden in ihrer Größenordnung vergröbert, z. B. Straßenname wird durch Postleitzahl ersetzt.

d) Aggregation

Datensätze werden zu Gruppen zusammengefasst, wobei sich Gruppen durch gleiche Merkmalswerte definieren. Z. B. Gehaltsdaten werden durch Intervalle „30.00 bis 40.000“ und „40.000 bis 50.000“ ersetzt.

C. ANONYMISIERUNG

CSW

4. Anwendungsfall Bewerberdaten

Bewerberdaten sind nach Einstellungsentscheidung und Ablauf der Verjährungsfrist für Ansprüche nach dem AGG zu löschen => Löschfrist beträgt wenige Monate.

Interesse der Personalabteilung: Messung des Vermittlungserfolgs und der Qualität der Bewerber über Jahre hinweg.

Lösung:

Anonymisierung der Daten in einer Weise, dass der Personenbezug zu dem jeweiligen Bewerber entfernt, aber die Informationen für die Auswertung noch vorhanden sind. Die Anonymisierung betrifft:

- Offensichtlich identifizierende Merkmale wie Name, Anschrift, Kontaktdaten werden entfernt/ersetzt.
- Weitere Merkmale wie Geburtsdatum, Geburtsort, schulische Laufbahn, Sprachkenntnisse, Staatsangehörigkeit oder mögliche Angaben zu Schwerbehinderung werden generalisiert oder durch Durchschnittswerte ersetzt.

C. ANONYMISIERUNG

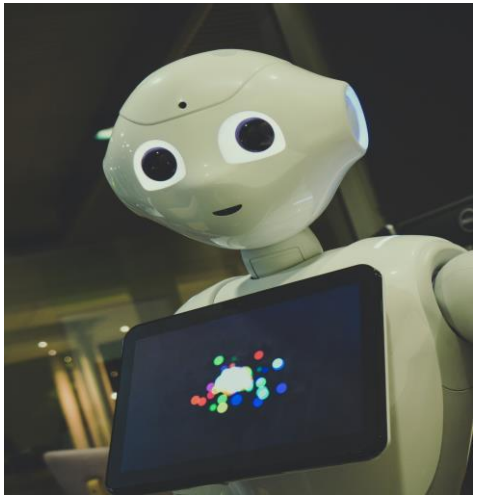
Personenbezogene Daten	Anonymisierung
Jahrgänge der Bewerber	Durchschnittswert über alle Bewerber im Jahre X für mehrere Jahre. (A)
Herkunft	Generalisierung der Herkunft nach Region (z.B. Mitteleuropa, Naher Osten, Nordamerika) (V)
Sprachkenntnisse	Durchschnittswert der Anzahl beherrschter Sprachen über alle Bewerber im Jahre x für mehrere Jahre. (A) Durchschnittswert der Anzahl der Bewerber, die Englisch auf dem Niveau C1 beherrschten im Jahre x für mehrere Jahre. (A)
Bildungsstand	Durchschnittswerte der erreichten Schulabschlüsse im Jahre x; Anzahl der Bewerber mit Bachelorabschluss. (A)
Abschlussnoten	Durchschnittsnote, aufgeteilt nach Jahren und Abschlüssen. (A)
Wohnort	Region des Wohnortes, z.B. Rheinland statt Bonn. (V)
Schwerbehinderung	Anteil Schwerbehinderter an den Bewerbern im Jahre x. (A)

Beispiele für personenbezogene Daten und die Ersetzung dieser durch geeignete Verallgemeinerungen (V) bzw. Aggregate (A).

Quelle: Praxisleitfaden zum Anonymisieren personenbezogener Daten der Stiftung Datenschutz

C. ANONYMISIERUNG

5. Anwendungsfall KI-Training



Problem: Training einer KI (z. B. Large Language Modell wie ChatGPT) erfordert Nutzung einer Vielzahl von Dateien (z. B. Texten), die oft offen im Internet zugänglich sind (Webscraping). Die darin enthaltenen pD gelangen dadurch in die Hände des KI-Anbieters.

Lösung: Ein zwischengeschalteter Datenanbieter sorgt dafür, dass auf die Datensätze ein Anonymisierungsverfahren angewandt wird, dass den Personenbezug evtl. pD aufhebt.

Anonymisierung muss so erfolgen, dass der relevante Aussagewert der Originaldateien nicht verändert wird.

Es gibt diverse Verfahren (z. B. Differential Privacy), die aber noch immer Gegenstand wissenschaftlicher Forschung sind.

D. PSEUDONYMISIERUNG

1. Pseudonymisierte Daten als personenbezogene Daten

Personenbezogenen Daten können ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden. Damit handelt es sich dennoch um Informationen über eine **identifi-zierbare natürliche Person**, also **personenbezogene Daten**.

Folge: Uneingeschränkte Geltung der DSGVO.

Man hat also normalerweise **zwei Datensätze**:

(1) Pseudonymisierte Daten.

(2) Zusätzliche Informationen, die man braucht, um Daten wieder den natürlichen Personen zuzuordnen.

Sinnvollerweise werden zusätzliche Informationen **gesondert aufbewahrt** und sind **nur wenigen Berechtigten zugänglich** (Art. 4 Nr. 5 DSGVO)!

D. PSEUDONYMISIERUNG

2. Wofür braucht man Pseudonymisierung?

Pseudonymisierung ist eine technische Maßnahme zum Schutz personenbezogener Daten (Art. 32 Abs. 2 lit. a DSGVO).

- Auswirkungen, wenn Rechtsgrundlage für Datenverarbeitung auf **Interessenabwägung** beruht (Art. 6 Abs. 1 lit. f DSGVO): Je stärker die Pseudonymisierung, desto stärker gewichtet die DSGVO die Interessen des Unternehmens.
- Bei **Datenschutzverstößen** (z. B. Datenpannen) muss betroffene Person nicht unterrichtet werden
- Bei Verarbeitung von pD im Bereich der medizinischen Forschung ist zumindest Pseudonymisierung der Daten erforderlich, da Gesundheitsdaten besonders sensible Daten darstellen.
- Nutzung der Daten im Rahmen allgemeiner Analysen leichter möglich, ErwG29 DSGVO
- EDSA: Pseudonymisierung kann Möglichkeit sein, um personenbezogene Daten in unsicheres Drittland zu übermitteln.

D. PSEUDONYMISIERUNG

CSW

3. Verfahren zur Pseudonymisierung (Beispiele)

a) Identifizierbare Daten werden durch **Zufallswerte** ersetzt. Gleichzeitig wird eine **Zuordnungsliste** (z. B. Referenztabelle) erstellt, die Zufallswerte den identifizierbaren Daten zuordnet.

Beispiel:

Guido Meier, verheiratet	wird ersetzt durch	37,8, verheiratet

Zuordnungsliste: 37,8 = Guido Meier

b) Aus dem identifizierbaren Datum wird mittels bestimmter Funktion ein Hashwert errechnet. Identifikationsdaten werden getrennt aufbewahrt. Mittels der gleichen Funktion kann aus gespeicherten Identifikationsdaten wiederum der Hashwert errechnet werden, der dann mit pseudonymisierter Tabelle abgeglichen werden kann.

F: x = y x 3. Angewandt auf

M	E	I	E	R
13.	5.	9.	5.	18

ergibt Hashwert 39.15.27.15.54

Pseudonymisierte Liste: „39.15.27.15.54, verheiratet“

Zuordnungsliste: „MEIER“

E. Fundstellen

DSK Kurzpapier Nr. 11: Recht auf Löschung / „Recht auf Vergessenwerden“

Der Bayerische Landesbeauftragte für den Datenschutz, Wann ist eine natürliche Person identifizierbar?, Aktuelle Kurz-Information 53

Stiftung Datenschutz: Praxisleitfaden zum Anonymisieren personenbezogener Daten (Dezember 2022)

Vielen Dank für Ihre Aufmerksamkeit!