

Anonymisierung personenbezogener Daten zum Zwecke der Datenweitergabe

HTW Berlin

Jasmin Raihani



Hochschule für Technik
und Wirtschaft Berlin

University of Applied Sciences

Gliederung

- 1 Personenbezogene Daten gem. Art. 4 Nr. 1 DS-GVO
- 2 Grundsätze der Datenverarbeitung Art. 5 DS-GVO
- 3 Pseudonymisierung
- 4 Anonymisierung
 - 4.1 Definition
 - 4.2 Vorgehensweise

1. Personenbezogene Daten

- **Art. 4 Nr. 1 DSGVO:** alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen
- **Identifizierbar** = direkte oder indirekte Identifizierung, insbesondere mittels Zuordnung zu
 - Namen, Kennnummer, Standortdaten, Online-Kennung oder Merkmale, die Ausdruck der physischen, psychischen, wirtschaftlichen, kulturellen, sozialen Identität sind
- Schließt sowohl Informationen über Intim-, Privatsphäre (zB. Gesundheitsdaten), als auch berufliche Betätigung und Einkommens- oder Vermögensverhältnisse ein also **den gesamten Lebensbereich** der Betroffenen
 - **Objektive** Informationen: Name, Anschrift, Geburtstag, körperliche Erscheinung, Alter etc.
 - **Subjektive** Informationen: Meinungen, Stellungnahmen, Beurteilungen

1. Personenbezogene Daten

- **Single-Out:** Eine Person ist identifiziert, wenn ein **Herausgreifen**/ Aussondern anhand der vorliegenden Informationen möglich ist
- Wie prüft ein Gericht:
 - Feststellung gem. ErwGr. 26 S.3 DS-GVO ob die betroffene Person unter Berücksichtigung aller zur **Verfügung stehender Mittel**, die von dem **Verantwortlichen oder einem Dritten** nach allgemeinem **Ermessen** angewandt werden könnten, identifizierbar ist.
 - Zuordnung des möglichen Zusatzwissen eines Dritten strittig, es spricht vieles für die Verwendung eines relativen Begriffs:
 - Verfügt der Verantwortliche über rechtliche Mittel, die es ihm erlauben die betreffende Person anhand Zusatzinformationen zu bestimmen
 - Identifizierung durch Eingrenzung einer bestimmten Gruppe zB Die Schule ist bekannt, hierdurch könnte das Wissen anderer Schulmitglieder dem Verantwortlichen zugeordnet werden, Gefahr des Herausgreifens

2. Grundsätze der Datenverarbeitung

- In Art. 5 DS-GVO werden die Grundsätze für die Verarbeitung personenbezogener Daten festgelegt:
 - Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
 - Zweckbindung
 - Datenminimierung
 - Richtigkeit
 - Speicherbegrenzung
 - Integrität und Vertraulichkeit
 - Rechenschaftspflicht
- **Lit.c** : Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die **Zwecke der Verarbeitung notwendige Maß beschränkt** sein („Datenminimierung“);
- **Lit.e**: in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen **nur so lange** ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, **erforderlich** ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische **Forschungszwecke** oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“);

3. Pseudonymisierung

- **Art. 4 Nr. 5 DS-GVO**
 1. Daten sind pseudonymisiert, wenn ehemals personenbezogene Daten **ohne Hinzuziehung zusätzlicher Informationen** nicht mehr einer spezifischen Person zugeordnet werden können
 2. Informationen werden **gesondert aufbewahrt ...** (technisch/ räumlich getrennte Aufbewahrung)
 3. ... und unterliegen technischen und organisatorischen **Maßnahmen**, die eine Zuweisung verhindern
 - zB Berechtigungskonzept mit getrennten technischen Rollen für je Zugriff auf pseudonymisierten Daten und Datenschlüssel
 - mehrschrittige Verfahren
 - Authentifizierungs- u. Sicherheitsmaßnahmen

Auch pseudonymisierte Daten = personenbezogene Daten und fallen unter Datenschutzvorgaben, gem. ErwGr. 26 DS-GVO

4.1 Anonymisierung - Definition

Ableitung aus **ErwGr. 26 S.5, Art. 89 Abs.1 Nr. 4 DS-GVO** und Bestimmungen zur Pseudonymisierung
Art. 4 DS-GVO:

- Ein mehr gegenüber der Pseudonymisierung
- Nicht oder nicht mehr mögliche Identifizierung

- Faktische/Absolute Anonymisierung
 - Personenbezug für jedermann unmöglich

- **Relative** Anonymisierung (ausreichend)
 - **Unverhältnismäßigkeit des Aufwandes** (Zeit, Kosten, Arbeitskraft, Ermittlung anhand einer Risikoprognose)
ErwGr. 26 S.3,4 (vgl. § 3 BDSG a.F.)
 - Zurechnung Zusatzwissen eines Dritten bei Kenntnis des Verantwortlichen über den Dritten

4.2 Anonymisierung - Vorgehensweise

- Vorgang der Anonymisierung fällt unter Begriff der Datenverarbeitung i.S.d. Art. 4 Nr. 2 DS-GVO
 - Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder **Veränderung**, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;
- Bedarf einer **Rechtsgrundlage**
 - Wirksame Einwilligung gem. Art. 6 Abs.1 lit.a
 - Berührt Rechte Betroffener selten/ in geringem Maße Art. 6 Abs.1 lit.f
 - Vereinbarkeit mit Erhebungszweck Art. 6 Abs.4
 - Bei älteren Datenbeständen Weiterverarbeitung vorhandener Garantien Art. 6 Abs.1 lit.e
 - Forschungszwecke Art. 5 Abs.1 lit.b iVm. Art. 89 Abs.1 DS-GVO
 - Vermutung der Vereinbarkeit mit Erhebungszweck
 - Regelmäßig nicht vorliegend bei Einsatz von K.I.

4.2 Anonymisierung - Vorgehensweise

- **Informationspflichten**

- Transparenz Art. 5 lit.a DS-GVO
- Grundsätzlich bereits bei Datenerhebung gem. Art. 13 DS-GVO, zB:
 - „Neben den geschäftlichen Zwecken anonymisieren wir Ihre Daten für statistische Zwecke und Zwecke der Datenteilung auf Grundlage der EU-Rechtsakte.“
- Ausnahme bei nachträglicher Anonymisierung, insb. zu Forschungszwecken.: Art. 14 Abs. 5 DS-GVO – **unverhältnismäßiger Aufwand + keine Gefahr für Persönlichkeits- oder Datenschutzrechte**
- Information über Anonymisierung, nicht mehr über Weitergabe anonymisierter Daten

- **Durchführung**

- Alle direkten, indirekten Identifikationsmerkmale sind zu entfernen
- Geeignete technische Anonymisierungsmethoden: zB. Generalisierung, Randomisierung

4.2 Anonymisierung - Vorgehensweise

Risikoanalyse

- Rechtliche Prüfpflicht, ErwGr. 26, S.3, 4 DS-GVO
- Berücksichtigung **aller Mittel, welche vernünftigerweise eingesetzt** werden können um anonymisierte Daten durch Datenverknüpfung/ Herausgreifen etc. einer natürlichen Person **nachträglich zuzuordnen**
- Angreifermodell (**Praxisleitfaden Stiftung Datenschutz**)
 - Bei Trainieren von Algorithmen: Angreifermodell ist auch auf den trainierten Algorithmus anzuwenden
- Regelmäßige Wiederholung der Risikoanalyse

4.2 Anonymisierung - Vorgehensweise

Weitergabe anonymisierter Daten

- Form der Zusammenarbeit bestimmen
 - Auftragsverarbeitung
 - Gemeinsame Verantwortliche i.S.d Art. 26 DS-GVO, klare Rollenbestimmung (Zugriff auf anonymisierten Datensatz / Zugriff auf zu anonymisierende Daten)

- nur für die Zwecke des Empfängers notwendige Daten weitergegeben (Datenminimierung)

Vielen Dank.

www.htw-berlin.de



**Hochschule für Technik
und Wirtschaft Berlin**

University of Applied Sciences



**Hochschule für Technik
und Wirtschaft Berlin**

University of Applied Sciences

www.htw-berlin.de