Rechtliche Grundlagen der Pseudonymisierung/Anonymisierung

Dr. Bernd Schütze

Berlin, 23. Mai 2016

HEALTHCARE SOLUTIONS

Was ist „pseudonym“, was „anonym“?

Begriffsbestimmung: Pseudonym, Anonym

§3 Abs. 6a: Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die **Bestimmung des Betroffenen auszuschließen** oder **wesentlich zu erschweren**	Art. 4 Abs. 5: "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**, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden
§3 Abs. 6: „Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse **nicht mehr** oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder **bestimmbaren natürlichen Person zugeordnet werden können**	- Keine Regelungen in der Verordnung, nicht einmal die Begriffsbestimmung - Ausschliesslich kurze Berücksichtigung in Erwägungsgrund 26

Genauer: was ist „anonym“ gemäß DS-GVO?

Anonyme Daten = Keine Re-Identifikation möglich

- EU DS-GVO
  - ErwGr. 26: Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten …Diese Verordnung betrifft somit nicht die Verarbeitung solcher anonymer Daten
  - Personenbezug Art. 4: …als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt …identifiziert werden kann
    - ErwGr. 26: „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
    - Indirekte Identifizierung = Pseudonym

Begrifflichkeit „anonym“: BDSG vs. DS-GVO

Relativer und absoluter Personenbezug

- BDSG
  - Anonymisieren ist Verändern, dass … Einzelangaben … nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand … einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden kann
  - In Deutschland etablierte sich daraus der „absolute“ (= nicht mehr) und der „relative“ (= unverhältnismäßig großer Aufwand) Personenbezug bzgl. Anonymität
- EU DS-GVO
  - Personenbezug Art. 4 i.V.m. ErwGr 26: ist eine natürliche Person direkt oder indirekt identifizierbar = personenbezogene Daten
  - Artikel-29-Datenschutzgruppe: keine relative Anonymität („keine Möglichkeit zur Re-Identifizierung“, WP 216)
  - ➢ Unter Berücksichtigung der Zusammensetzung des künftigen Datenschutz-Ausschusses und der Tatsache, dass die entsprechenden Regelungen der RL 95/46/EG denen der DS-GVO entsprechen…
  - ➢ DS-GVO spricht wohl von absoluter Anonymität

Was folgt daraus?

Folgerungen

- BDSG
  - Pseudonymisieren ist Ersetzen
  - Anonymisieren ist Verändern
  - Beides laut §3 Abs. 4 BDSG „Verarbeitung“ bzw. „Nutzung“
  - ➢ §4 Abs. 1 BDSG: Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind **nur zulässig**, soweit **dieses Gesetz** oder eine **andere Rechtsvorschrift** dies **erlaubt** oder anordnet oder der **Betroffene eingewilligt** hat.
- EU DS-GVO
  - Alles, was mit personenbezogenen Daten geschieht, ist Verarbeitung
  - Insbesondere auch die Pseudonymisierung oder Anonymisierung
  - Artt. 6,9: Verarbeitung nur mit Erlaubnistatbestand zulässig
- Im Folgenden Betrachtung bzgl. Verarbeitung von Gesundheitsdaten, genetischen Daten

Erlaubnistatbestand gefordert

Rechtsgrundlage erforderlich

→ Eine Pseudonymisierung oder Anonymisierung benötigt einen Erlaubnistatbestand

- ➢ Gesetzlicher Erlaubnistatbestand
- ➢ Betroffener willigt ein

– Mögliche heutige gesetzliche Erlaubnistatbestände

- Forschung mit Gesundheitsdaten
  (z.B. §28 Abs. 6 Ziff. 4 BDSG, Regelungen der Landeskrankenhausgesetze)
- Qualitätssicherung mit Gesundheitsdaten
  (z.B. SGB, Vorgaben der Landeskrankenhausgesetze)

☞ Problem: in BDSG und Landesdatenschutzgesetzen häufig Hinweis „erlaubt nur, wenn gesetzliche Schweigepflicht nicht verletzt wird“

☞ Entbindung Schweigepflicht erforderlich

Erlaubnistatbestand gefordert, aber woher nehmen?

Rechtsgrundlage erforderlich: was gilt unter der DS-GVO ab 25. Mai 2018?

→ Eine Pseudonymisierung oder Anonymisierung benötigt einen Erlaubnistatbestand

- ➢ Gesetzlicher Erlaubnistatbestand
- ➢ Betroffener willigt ein

– Mögliche Erlaubnistatbestände unter der EU DS-GVO

- ???
- Nationale Regeln erforderlich

Abgrenzung: Pseudonym vs. Anonym

Wann sind Daten anonym, wann pseudonym?

- Wann sind Daten als „anonym“ anzusehen, wann als pseudonym?
  - Definition „Pseudonym“ der EU DS-GVO beinhaltet, was Stand heute in Deutschland als „faktisch anonym“ angesehen wird
  - Artikel-29-Datenschutzgruppe
    - „Ein häufiger Irrtum liegt in der Annahme, dass pseudonymisierte Daten mit anonymisierten Daten gleichzusetzen seien“
    - „Pseudonymisierung verringert die Verknüpfbarkeit eines Datenbestands mit der wahren Identität einer betroffenen Person und stellt somit eine sinnvolle Sicherheitsmaßnahme, aber kein Anonymisierungsverfahren dar“
    - Häufiger Fehler: „Annahme, dass ein pseudonymisierter Datenbestand anonymisiert ist…“
    - „…Ergebnis der Anonymisierung … so dauerhaft sein sollte wie eine Löschung … es darf nicht möglich sein, die personenbezogenen Daten weiter zu verarbeiten“

Quelle: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf

Abgrenzung: Pseudonym vs. Anonym

Re-Identifikationspotential medizinischer Daten

- Medizinische Daten können in sich das Potential der Re-Identifikationsmöglichkeit beinhalten
  - Genetische Daten
  - Bilddaten, die eine 3D-Rekonstruktion identifizierender Merkmale erlauben
  - Medizinische Daten selbst, abhängig von der Gruppengröße (z.B.: „Der“ männliche Patient mit Brustkrebs)
- Diese Daten sind im Sinne der DS-GVO als pseudonym anzusehen, eine Anonymisierung erscheint kaum möglich

→ Ausführliche Besprechung der daraus resultierenden Herausforderungen nach der Mittagspause

Offene Fragen

Fragen, auf die Antworten gefunden werden müssen

→ Welche Rechtsgrundlage benötigt Deutschland für Anonymisierung/Pseudonymisierung
  - Forschung
  - Qualitätssicherung
  - Routineversorgung (z.B. Wartung von Informationssystemen)
  - …
  - ➢ Nationaler Erlaubnistatbestand zur Zweckänderung eine Herangehensweise?

→ Wann sind Daten eines Patienten als anonym anzusehen, wann „nur" als pseudonym?
  - Merke: pseudonyme Daten = personenbezogene Daten (ErwGr. 26 DS-GVO)

→ Wie gehen wir mit nationalen Regelungen um, wenn wir innereuropäisch international arbeiten wollen?
  - Kann uns der Datenschutz-Ausschuss unterstützen?
    (Stichwort: Kohärenz-Verfahren und einheitliche Auslegung der DS-GVO)