


Dr. rer. oec. Katja Gehrke,
Institut für deskriptive Gesundheitsdatenanalyse OHG (DGDA)
ORCID 0000-0001-5516-457X
Dr. jur. Joachim Jung
Möhrle Happ Luther Rechtsanwälte

EuGH-Urteil: Neue Freiheiten für GKV-Daten

>> Mit § 25b SGB V hat der Gesetzgeber den Kranken- und Pflegekassen erlaubt, vorhandene Daten zum Schutz der Gesundheit ihrer Versicherten auszuwerten. Ziel ist es, Risiken früher zu erkennen und Versicherte auf passende Vorsorge- und Behandlungsangebote hinzuweisen. Damit ändert sich die Rolle von Sozialdaten. Sie dienen nicht mehr nur der Abrechnung oder der Dokumentation. Sie können auch helfen, künftige Risiken zu erkennen. Nicht erst die Krankheit, sondern schon das Risiko wird zum Anlass für eine Ansprache der Versicherten.

Was § 25b SGB V erlaubt

§ 25b SGB V ist keine allgemeine Erlaubnis zur freien Datennutzung, sondern hat einen klaren Zweck: den Gesundheitsschutz der Versicherten. Krankenkassen dürfen Daten auswerten, wenn dies dazu dient, Risiken zu erkennen und Versicherte auf geeignete Angebote hinzuweisen.

Die Norm nennt dafür konkrete Fälle. Dazu gehören seltene Erkrankungen, Krebserkrankungen, Gefahren durch Arzneimittel, ähnlich schwere Gesundheitsrisiken, Impfindikationen und die Erkennung einer noch nicht festgestellten Pflegebedürftigkeit. Der Gesetzgeber will also nicht irgendeine Datennutzung erlauben. Er will eine frühere und bessere Versorgung ermöglichen.

Zugleich setzt § 25b SGB V Grenzen. Versicherte müssen informiert werden und widersprechen können. Die Nutzung darf nicht dazu dienen, Risiken zu selektieren oder Leistungen zu verweigern. Hinweise sollen helfen, nicht stigmatisieren. Ein Score darf nicht zum verdeckten Mittel der Steuerung werden.

Gerade deshalb ist § 25b SGB V ein wichtiger Testfall. Die Norm zeigt, wie ein solidarisches System mit Prognosen umgehen kann. Daten sollen genutzt werden, aber nicht gegen die Versicherten.

Warum externe Dienstleister wichtig sind

Die Auswertung nach § 25b SGB V setzt belastbare Modelle voraus. Solche Modelle entstehen nicht von selbst. Sie müssen entwickelt, geprüft und laufend verbessert werden. Krankenkassen haben die Daten. Externe Dienstleister haben oft das nötige Wissen zu Statistik, Software und Validierung von Modellen. Es liegt daher nahe, dass Kassen solche Dienstleister beauftragen.

Datenschutzrechtlich geschieht dies in der Regel über eine Auftragsverarbeitung. Das ist in § 25b Abs. 2 Satz 5 SGB V ausdrücklich angelegt. Die Kasse bleibt rechtlich voll verantwortlich. Der Dienstleister darf die erhaltenen Daten ausschließlich für die Entwicklung der Modelle verwenden, ohne sie für andere Zwecke zu nutzen.

Damit ist ein erster Punkt wichtig: Externe Entwickler konnten Risikomodelle nach § 25b SGB V schon bisher für Krankenkassen entwickeln. Für diese Entwicklung braucht der Dienstleister die Identität der Versicherten in der Regel nicht. Ein Modell lernt aus Mustern. Es wertet zum Beispiel Diagnosen, Arzneimittel, Krankenhausaufenthalte, Hinweise zur Pflege oder später eintretende Ereignisse aus. Namen, Anschriften oder Versichertennummern helfen dabei regelmäßig nicht. Entscheidend ist, ob sich aus vielen Fällen ein verlässliches Muster ergibt.

Daraus folgt die zentrale Frage: Muss der externe Entwickler überhaupt personenbezogene Daten erhalten? Oder genügt ein Datensatz, bei dem die Kasse die direkte Zuordnung zu einer Person entfernt und den Schlüssel zur Re-Identifikation zurückhält?

Was der EuGH ändert

An dieser Stelle wird das Urteil des Gerichtshofs der Europäischen Union vom 4. September 2025 in der Rechtssache C-413/23 P wichtig. Der EuGH hat klargestellt, dass pseudonymisierte Daten nicht zwingend für jede Person und für jeden Empfänger personenbezogene Daten sein müssen, die den strengen datenschutzrechtlichen Vorgaben unterfallen.

Entscheidend ist der Blick auf den konkreten Empfänger: Kann dieser die betroffene Person mit Mitteln bestimmen, die ihm vernünftigerweise zur Verfügung stehen, bleiben die Daten für ihn personenbezogen. Hat er aber keinen Zugriff auf den Schlüssel und auch sonst keine rechtlich und tatsächlich nutzbaren Mittel zur Re-Identifikation, kann der Personenbezug aus seiner Sicht fehlen.

Das ist der Kern des sogenannten „relativen Personenbezugs". Es kommt nicht allein auf den Datensatz an. Es kommt auch darauf an, wer ihn erhält und welche Mittel diese Stelle tatsächlich und rechtlich nutzen kann.

Mehr als Auftragsverarbeitung

Für § 25b SGB V ist diese Unterscheidung praktisch bedeutsam. Die Entwicklung eines Modells als Auftragsverarbeiter war bereits

Literatur

1. Urteil des Gerichtshofs (Erste Kammer) vom 4. September 2025, Rechtssache C-413/23 P, abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:62023CJ0413
2. Stoklas, J. (2025) EuGH: Personenbezug – absoluter oder relativer Ansatz bei pseudonymisierten Daten? In ZD-Aktuell, Jahrgang 15, Nr. 20, 01442, 31.10.2025
3. Grosmann, P./ Luh, C. (2025) Datenschutzrecht: Regeln zur Weitergabe pseudonymisierter Daten, EuZW, S. 1103
4. Golland, A. (2025) Regeln zur Weitergabe pseudonymisierter Daten mit Personenbezug, NJW, S. 3415
5. Gesetz zur verbesserten Nutzung von Gesundheitsdaten (GDNG) 2024, Bundesgesetzblatt 2024 I Nr. 21 vom 25. März 2024, abrufbar unter: https://www.recht.bund.de/bgbl/1/2024/101/VO.html?utm_source=chatgpt.com
6. Kühling, J./Buchner, B. (2024) Datenschutz-Grundverordnung/BDSG. Kommentar. 4. Auflage, München: C.H. Beck
7. He, Z. (2023): From Privacy Enhancing to Health Data Utilisation: The Traces of Anonymisation and Pseudonymisation in EU Data Protection Law. European Journal of Law and Technology, 2, Art. 17. DOI: 10.1007/s44206-023-00043-5, abrufbar unter: https://doi.org/10.1007/s44206-023-00043-5
8. Bundesministerium für Gesundheit (2026) Referentenentwurf eines Gesetzes für Daten und digitale Innovationen im Gesundheitswesen (GeDIG), abrufbar unter: https://www.bundesgesundheitsministerium.de/service/gesetze-und-verordnungen/detail/gedig

Zitationshinweis

Gehrke, K., Jung, J.: „EuGH-Urteil: Neue Freiheiten für GKV-Daten", „Monitor Versorgungsforschung" (05/26), S. 56–57.
http://doi.org/10.24945/MVF.05.26.1866-0533.2860

möglich. Neu ist die Frage, ob der externe Dienstleister pseudonymisierte Daten auch über den einzelnen Auftrag hinaus nutzen kann, weil die von der Kasse übermittelten Daten für ihn außerhalb des Datenschutzrechts liegen.

Solche weiteren Nutzungen können etwa darin liegen, eigene Modelle zu verbessern, neue Verfahren zu testen oder allgemeine Werkzeuge für die Risikoerkennung zu entwickeln. Das geht deutlich weiter als die klassische Auftragsverarbeitung.

Die EuGH-Rechtsprechung kann hier neue Spielräume eröffnen. Voraussetzung ist aber, dass der Dienstleister die Versicherten vernünftigerweise nicht identifizieren kann. Dann können die Daten für ihn außerhalb des Datenschutzrechts liegen. Er wäre dann nicht deshalb gebunden, weil es sich für ihn um personenbezogene Daten handelt.

Das bedeutet gleichwohl nicht, dass die Daten beliebig genutzt werden dürfen. Auch dann bleiben Verträge, Sozialrecht, Geheimnisschutz und das Vertrauen der Versicherten wichtig. Die Kasse muss außerdem erklären können, warum sie Daten in dieser Form weitergibt und welche Zwecke damit verfolgt werden. Die EuGH-Entscheidung ist daher kein Freibrief. Sie schafft aber einen neuen Raum für rechtlich saubere Modelle der Zusammenarbeit.

Warum das für Innovation wichtig ist

Genau hier kann die EuGH-Rechtsprechung neue Spielräume schaffen. Die klassische Auftragsverarbeitung bleibt der sichere Standardfall für die primäre Entwicklung von § 25b-Algorithmen. Neu ist aber eine zweite Möglichkeit: Übermittelt die Krankenkasse Datensätze in einer Form, in der der externe Dienstleister den Personenbezug vernünftigerweise nicht wiederherstellen kann, dann kann der Empfänger diese Datensätze frei für weitere Innovations- oder Qualitätssicherungszwecke nutzen, da er nicht an datenschutzrechtliche Vorgaben gebunden ist. Diese Freiheit in der weiteren Datennutzung besteht nur, sofern die Krankenkasse die Nutzung für andere Zwecke nicht eingeschränkt hat.

Daraus kann eine neue Rolle der Dienstleister entstehen – nicht mehr nur verlängerter Arm der Kasse, sondern Partner für bessere Verfahren. Das kann die Versorgung verbessern. Denn viele Modelle werden besser, wenn sie mit größeren und vielfältigeren Datenbeständen entwickelt und geprüft werden. Fehlalarme können sinken. Risiken können früher erkannt werden. Auch Verzerrungen lassen sich besser prüfen, etwa wenn ein Modell bei bestimmten Altersgruppen oder Versichertengruppen schlechter funktioniert.

Pseudonymisierung muss belastbar sein

Diese neue Möglichkeit steht und fällt mit der Qualität der Pseudonymisierung. Ein Datensatz ist nicht schon deshalb unproblematisch, weil er als pseudonymisiert bezeichnet wird. Es muss geprüft werden, ob der Empfänger die Personen wirklich nicht bestimmen kann.

Dafür sind einfache, aber wichtige Fragen zu stellen: Enthält der Datensatz seltene Diagnosen, kleine Gruppen oder auffällige Verläufe? Können Alter, Region und Behandlungsweg zusammen eine Person erkennbar machen? Hat der Dienstleister Zugriff auf weitere Daten, die eine Zuordnung erleichtern? Gibt es klare Verbote der Re-Identifikation? Werden diese Verbote technisch abgesichert? Wird geprüft, ob Mitarbeitende des Dienstleisters andere Quellen nutzen könnten?

Je sensibler die Daten sind, desto strenger muss diese Prüfung ausfallen. Gesundheitsdaten sind besonders schutzbedürftig. Auch wenn sie für den Dienstleister keinen Personenbezug mehr haben, bleibt das Vertrauen der Versicherten entscheidend. Eine Kasse muss zeigen können, dass keine verdeckte Zweckverschiebung stattfindet.

Klare Regeln statt Datenfreigabe

Für die Praxis empfiehlt sich daher eine klare Trennung. Im ersten Schritt kann der externe Entwickler als Auftragsverarbeiter ein Modell für die Kasse entwickeln. Diese Verarbeitung bleibt eng an § 25b SGB V gebunden. Im zweiten Schritt kann geprüft werden, ob ein Datensatz so aufbereitet werden kann, dass der Dienstleister die Versicherten nicht mehr identifizieren kann. Nur dann kommen weitere Nutzungen in Betracht.

Diese Trennung sollte nicht nur technisch, sondern auch vertraglich abgesichert werden. Der Schlüssel zur Zuordnung darf nicht beim Dienstleister liegen. Der Zugriff auf Zusatzdaten muss ausgeschlossen sein. Die erlaubten Zwecke müssen klar beschrieben werden. Außerdem sollte dokumentiert werden, warum eine Re-Identifikation vernünftigerweise nicht zu erwarten ist.

Daneben bleiben weitere Regeln wichtig. Je nach Zweck und Einsatz kann auch die KI-Verordnung eine Rolle spielen. Wird ein System für medizinische Zwecke eingesetzt, kann zudem das Medizinprodukterecht relevant werden. Datenschutzrechtliche Entlastung bedeutet also nicht, dass keine Regeln mehr gelten. Sie verschiebt nur den Schwerpunkt: weg von der bloßen Frage des Personenbezugs hin zu Qualität, Kontrolle und Verantwortung.

Ausblick

Der § 25b SGB V zeigt, wohin sich die Nutzung von Sozialdaten bewegt. Daten sollen nicht nur vergangene Leistungen abbilden. Sie sollen helfen, Risiken früher zu erkennen und Versorgung besser zu planen.

Externe Dienstleister werden dabei eine wichtige Rolle spielen. Als Auftragsverarbeiter konnten sie entsprechende Modelle schon bisher entwickeln. Die neue EuGH-Rechtsprechung kann darüber hinaus neue Wege eröffnen. Werden Daten so übermittelt, dass der Entwickler die Versicherten vernünftigerweise nicht bestimmen kann, kann der Personenbezug aus Sicht der Luxemburger Richter entfallen. Dann kommen auch Nutzungen in Betracht, die über den einzelnen Auftrag hinausgehen.

Die Chance liegt in besseren Modellen und mehr Innovation. Das Risiko liegt in unklaren Zwecken, schwacher Kontrolle und verlorenem Vertrauen. Die Aufgabe der nächsten Jahre wird daher nicht nur sein, Daten nutzbar zu machen. Sie wird auch darin bestehen, klare Regeln für ihre Nutzung zu schaffen. Nur dann kann § 25b SGB V zu einem Instrument werden, das Risiken früh erkennt, die Versorgung verbessert und zugleich die Versicherten schützt.

Darüber hinaus zeigen verschiedene aktuelle gesetzgeberische Entwicklungen, dass unter bestimmten Voraussetzungen die vorhandenen Daten verstärkt genutzt werden sollen und können, was künftig zu einer verbesserten Gesundheitsversorgung und Steuerung beitragen kann. <<