Stellungnahme
der Bundesärztekammer

zum Verordnungsvorschlag COM(2025)837 „Digital Omnibus Datenschutz“ der Europäischen Kommission

vom 19.11.2025

Berlin, 15.09.2026

Korrespondenzadresse:

Bundesärztekammer
Herbert-Lewin-Platz 1
10623 Berlin

Brüsseler Büro:

Rue Montoyer 25
6. Etage
1000 Brüssel

Inhaltsverzeichnis

1. Vorbemerkung

Die Europäische Kommission hat am 19.11.2025 den Verordnungsvorschlag COM(2025)837 (*Digital Omnibus Datenschutz*) vorgelegt, der Änderungen u.a. der Datenschutzgrundverordnung (EU)2016/679 (DSGVO) vorsieht.

Vor dem Hintergrund, dass die Weitergabe anonymisierter oder pseudonymisierter Daten im Zuge der Gesundheitsversorgung regelmäßig vorkommt, möchte die Bundesärztekammer die vorgeschlagene Änderung der Definition personenbezogener Daten hervorheben, vorbehaltlich einer eventuellen Kommentierung weiterer Aspekte zu einem späteren Zeitpunkt.

Die Bundesärztekammer verweist außerdem auf die ausführlichere Stellungnahme von CPME European Doctors vom 21.03.2026, die weitere wichtige Aspekte des *Digital Omnibus Datenschutz* behandelt.

2. Stellungnahme im Einzelnen

Änderung der Definition personenbezogener Daten

Die Bundesärztekammer weist darauf hin, dass die von der Europäischen Kommission vorgeschlagene Änderung der Definition personenbezogener Daten in Artikel 4 (1) (a) DSGVO nicht, wie von der Kommission dargestellt, eine bloße Kodifizierung des Urteils des Europäischen Gerichtshofs (EuGH) vom 04.09.2025 in der Rechtssache C-413/23, *SRB*, ist, sondern in einer Weise darüber hinausgeht, die geeignet ist, den Schutz sensibler Patientendaten zu gefährden. Die Änderung wird daher abgelehnt.

In der Frage, ob anonymisierte oder pseudonymisierte Daten als personenbezogene Daten zu betrachten sind, stellt der EuGH auf eine relative Betrachtungsweise ab: Verfügt ein Verantwortlicher über keine Möglichkeit, anonymisierte oder pseudonymisierte Daten mit realistischem Aufwand wieder Personen zuzuordnen, und kann er sich eine solche Zuordnungsmöglichkeit nicht verschaffen (etwa durch einen Rechtsanspruch, diese Daten zu erhalten), so gelten die betreffenden Daten für ihn als nicht personenbezogen.

Jedoch präzisiert der EuGH in dem Urteil in der Rechtssache C-319/22, *Scania*, dass Daten auch für eine Person ohne Zuordnungsmöglichkeit indirekt personenbezogen sein können, wenn diese die Daten einer Person mit Zuordnungsmöglichkeit zur Verfügung stellt. Diese wichtige Klarstellung und Einschränkung wird im Vorschlag der Kommission nicht berücksichtigt.

Wenn einzelne Intermediäre die Daten als nicht personenbezogen behandeln dürfen, stellt sich die Frage, wie die Einhaltung datenschutzrechtlicher Anforderungen über die gesamte Datenkette hinweg kontrolliert werden kann. Somit würde die Pseudonymisierung, die den Schutz der Patienten vor und Identifizierbarkeit bewirken soll, diesen Schutz im Ergebnis mindern.

Folgende Beispiele aus dem Gesundheitswesen sind u.a. denkbar:

- Ein Krankenhaus A übermittelt pseudonymisierte Daten an einen Datenverarbeiter B. Dieser gibt sie an einen weiteren Dienstleister C weiter. Der weitere Dienstleister C verarbeitet zugleich Daten einer gesetzlichen oder privaten Krankenversicherung und verfügt über zusätzliche Identifikatoren, die eine Re-Identifizierung ermöglichen.

- Ein Krankenhaus übermittelt pseudonymisierte Behandlungsdaten an einen Cloud-Dienstleister. Dieser speichert die Daten bei einem Infrastrukturanbieter. Der Infrastrukturanbieter betreibt zugleich eine digitale Gesundheitsplattform, über die dieselben Patienten Termine vereinbaren oder Laborbefunde abrufen. Aufgrund der dort vorhandenen Kontodaten kann der Infrastrukturanbieter einzelne Datensätze re-identifizieren.

- Ein Universitätsklinikum A übermittelt pseudonymisierte Daten an einen Cloud-Dienstleister B. Dieser nutzt einen Subunternehmer C für die Speicherung. C verarbeitet daneben weitere Datenbestände aus dem Gesundheitsbereich, die ihm eine Re-Identifizierung einzelner Patienten ermöglichen. Er könnte z.B. Daten eines bundesweiten Krankheitsregisters oder eines Krebsregisters verwalten. Hiermit verfügt C über zusätzliche Informationen, mit denen einzelne Patienten identifiziert werden können.

In diesen Fällen ist es zum Schutz der Daten wichtig, dass die Daten auch für die jeweiligen Personen B ihre Eigenschaft als personenbezogene Daten nicht verlieren, damit der durchgehende Schutz dieser Daten gewährleistet wird. Es sollte daher eine anonyme Verarbeitung erfolgen, wo dies unter Berücksichtigung des wirtschaftlichen und personellen Aufwandes möglich und hinsichtlich der Schutzbedürftigkeit der Betroffenen notwendig ist.

Der EuGH hat diese Problematik in seinem o.g. Urteil in der Rechtssache *Scania* auf Basis der geltenden DSGVO bereits differenziert berücksichtigt. Eine Anpassung der Definition personenbezogener Daten in der DSGVO ist daher nicht notwendig.

Sofern jedoch eine Änderung der Definition in der DSGVO vorgenommen wird, sollte sie nicht nur das Urteil in der Rechtssache C-413/23, *SRB*, sondern auch das Urteil in der Rechtssache C-319/22, *Scania* berücksichtigen. Unbedingt abzulehnen ist der letzte Satz der von der Kommission vorgeschlagenen Definition, der im klaren Widerspruch zur Rechtsprechung des EuGH steht.

Daher schlagen wir folgende Änderung vor:

Verordnungsvorschlag *Digital Omnibus Datenschutz*
Artikel 3 – Nr. 1 – lit. a
Verordnung (EU) 2016/679 (DSGVO)

Artikel 4(1)(a)

Änderung der Verordnung (EU) 2016/679 (DSGVO)	
Definition personenbezogener Daten	
Vorschlag der Kommission	Vorschlag der BÄK
Article 4 is amended as follows: *a) in point 1, the following sentences are added:* *‘Information relating to a natural person is not necessarily personal data for every other person or entity, merely because another entity can identify that natural person.*	Streichung des Artikel 3 Nr.1 lit. a, d.h. Verzicht auf die Änderung der Definition personenbezogener Daten. Hilfsweise: *Article 4 is amended as follows:*

Information shall not be personal for a given entity where that entity cannot identify the natural person to whom the information relates, taking into account the means reasonably likely to be used by that entity. Such information does not become personal for that entity merely because a potential subsequent recipient has means reasonably likely to be used to identify the natural person to whom the information relates.'	*a) in point 1, the following sentences are added:* *'Information relating to a natural person is not necessarily personal data for every other person or entity, merely because another entity can identify that natural person. Information shall not be personal for a given entity where that entity cannot identify the natural person to whom the information relates, taking into account the means reasonably likely to be used by that entity.* ***It shall be considered personal data for an entity that makes the information available to a subsequent recipient who*** *has means reasonably likely to be used to identify the natural person to whom the information relates.'*