GDV Gesamtverband der Versicherer

STELLUNGNAHME

Stellungnahme

des Gesamtverbandes der
Deutschen Versicherungswirtschaft
ID-Nummer 6437280268-55

zur Konsultation des Europäischen Datenschutzausschusses
zu den Leitlinien 2/2026 zur Anonymisierung

GDV

Gesamtverband der Deutschen Versicherungswirtschaft e. V.
Wilhelmstraße 43 / 43 G, 10117 Berlin
Postfach 08 02 64, D-10002 Berlin
Telefon: +49 30 2020-5000 · Telefax: +49 30 2020-6000

Rue du Champ de Mars 23, B-1050 Brüssel
Telefon: +32 2 28247-30 · Telefax: +49 30 2020-6140
ID-Nummer 6437280268-55
www.gdv.de

Ansprechpartner
Recht/Compliance/Verbraucherschutz

E-Mail
data-protection@gdv.de

Inhalt

1. Zusammenfassung 3

2. Einzelanmerkungen 4

2.1 Wahrscheinlichkeitsmaßstab, relevante Akteure und Identifizierungsketten 4

2.2 Empfängerperspektive bei weisungsgebundener Verarbeitung 5

2.3 Gewichtung gesetzlicher und vertraglicher Verbote 5

2.4 Zukunftsmaßstab und periodische Neubewertung 6

2.5 Vereinfachter Ansatz: Vermeidung eines faktischen Standards 7

2.6 Anonymisierungsprozess, Transparenz und Dokumentation 7

2.7 Drei Kriterien: Gesamtbetrachtung notwendig 8

2.8 Tarifierung, Risikobewertung und versicherungsmathematische Modelle 9

1. Zusammenfassung

Die deutsche Versicherungswirtschaft begrüßt die Möglichkeit, sich an der Konsultation des Europäischen Datenschutzausschusses (EDSA) zu seinen neuen Leitlinien 02/2026 zur Anonymisierung zu beteiligen.

Positiv ist insbesondere, dass die Leitlinien sich grundsätzlich zu dem vom EuGH in der Rechtssache SRB (C-413/23 P) bestätigten relativen Ansatz des Personenbezugs bekennen. An mehreren Stellen wird der Maßstab jedoch derart weit ausgelegt, dass die maßgebliche Empfängerperspektive praktisch entwertet zu werden droht. Für die Versicherungswirtschaft sind wirksame und verlässliche Anonymisierungen insbesondere für Schadenstatistik, Tarifierung, Risikobewertung und versicherungsmathematische Modelle von großer Bedeutung. Damit die Leitlinien nicht nur ein hohes Schutzniveau gewährleisten, sondern für Unternehmen auch praktisch anwendbar bleiben, sollte neben dem EuGH-SRB-Urteil auch Erwägungsgrund 26 der DSGVO durchgehend als Maßstab angelegt werden.

Allein ausschlaggebend muss sein, ob eine Identifizierung unter Berücksichtigung aller objektiven Umstände und der konkret verfügbaren Mittel vernünftigerweise zu erwarten ist. Das Verlangen der Berücksichtigung unwahrscheinlicher Identifizierungsmöglichkeiten, unüberschaubarer Identifizierungsketten oder stark abstrakter Risiken rechtswidriger Zugriffe darf diesen Maßstab nicht faktisch durch ein Erfordernis vollständiger Risikofreiheit ersetzen.

Die nachfolgenden Anmerkungen benennen aus Sicht der deutschen Versicherungswirtschaft bestehenden Klarstellungs- und Anpassungsbedarf und enthalten Vorschläge, um den relativen Ansatz des Personenbezugs praxistauglich auszugestalten und so eine rechtssichere Anwendung der Leitlinien zu ermöglichen.

2. Einzelanmerkungen

2.1 Wahrscheinlichkeitsmaßstab, relevante Akteure und Identifizierungsketten

Fundstellen: Rn. 8, 9, 20, 21 f., 26 bis 35, 88 bis 90 und 94

Die Leitlinien betonen zutreffend, dass für die Beurteilung der Identifizierbarkeit auf die tatsächliche Wahrscheinlichkeit einer Identifizierung oder Re-Identifizierung abzustellen ist (Rn. 8, 22 und 26). Gleichzeitig stellt Rn. 21 aber darauf ab, dass personenbezogene Daten vorliegen sollen, wenn eine Übermittlung an einen Dritten vernünftigerweise wahrscheinlich ist und nicht ausgeschlossen werden kann, dass dieser über Identifizierungsmittel verfügt. Der von den Leitlinien selbst vorgegebene Wahrscheinlichkeitsmaßstab verkommt so faktisch zu einem Maßstab des „Nicht-Ausschließen-Könnens“.

Zudem beziehen Rn. 20 sowie Rn. 28 ff. auch mehrstufige Identifizierungsketten und Mittel verschiedener Akteure in die Bewertung ein. Dies erscheint so weitgehend, dass praktisch kaum eine Anonymisierung erreicht werden kann. Insbesondere in komplexen Datenübermittlungsstrukturen, wie sie etwa im Versicherungs- und Rückversicherungsbereich üblich sind, lässt sich regelmäßig nicht mit Sicherheit ausschließen, dass irgendein möglicher Folgeempfänger oder sonstiger Akteur über zusätzliches Wissen verfügen könnte. Werden zudem Identifizierungsmöglichkeiten verschiedener Akteure entlang mehrerer hypothetischer Ereignisse miteinander verknüpft, besteht die Gefahr, dass auch fernliegende Szenarien als relevante Identifizierungsrisiken behandelt werden müssen.

Rn. 28 bis 30 der Guidelines verlangen zudem, dass nahezu alle denkbaren Mittel der potenziell an die Daten gelangender Dritter zu betrachten sind. Genannt werden unter anderem unbefugte Beschäftigte, Freunde und Nachbarn, investigative Journalisten, in- und ausländische Nachrichtendienste, unethische Unternehmen und Cyberkriminelle. Nach Beispiel 22 sollen diese Mittel auch dann berücksichtigt werden, wenn Cybersicherheitsmaßnahmen nach dem neuesten Stand der Technik und weitere technische Mittel zur Verhinderung eines unbefugten Zugriffs eingesetzt werden.

Zwar kann die Berücksichtigung unbefugter Zugriffe oder rechtswidriger Handlungen im Einzelfall gerechtfertigt sein. Die Leitlinien selbst stellen in Rn. 33 zutreffend darauf ab, dass hierfür konkrete Anhaltspunkte vorliegen müssen. Zudem bestimmt Rn. 89, dass bei angemessenen Sicherheitsmaßnahmen grundsätzlich autorisierte Nutzer zu berücksichtigen sind. Demgegenüber erscheinen die o. g. Anforderungen als deutlich zu weitgehend.

Anregung an den EDSA: Die Leitlinien sollten konsequent klarstellen, dass für die Beurteilung die Gesamtwahrscheinlichkeit einer Re-Identifizierung maßgeblich ist. Unbefugte Akteure, Datenabflüsse und die Verfügbarkeit zusätzlicher Informationen sollten nur berücksichtigt werden, wenn konkrete objektive und fallspezifische Anhaltspunkte dafür bestehen, dass sowohl der Zugriff auf die betreffenden

Daten als auch auf die für eine Identifizierung erforderlichen Zusatzinformationen tatsächlich vernünftigerweise zu erwarten sind. Zudem sollte Rn. 21 dahingehend präzisiert werden, dass nicht die bloße Möglichkeit vorhandener Identifizierungsmittel, sondern deren realistischer Einsatz unter Berücksichtigung aller objektiven Umstände entscheidend ist.

2.2 Empfängerperspektive bei weisungsgebundener Verarbeitung

Fundstellen: Rn. 15; Beispiel 3; Beispiel 7 zu Rn. 28.

Nach Rn. 15 sollen Informationen bei einer Verarbeitung im Auftrag auch für die verarbeitende Stelle als personenbezogene Daten gelten, wenn sie für den Verantwortlichen personenbezogen sind. Das kann so verstanden werden, dass in solchen Konstellationen die Identifizierungsmöglichkeiten des Verantwortlichen pauschal auch dem Dienstleister zugerechnet werden. Damit droht die Bedeutung datenschutzfreundlicher Verarbeitungsarchitekturen in den Hintergrund zu treten.

In der Versicherungspraxis können ausgelagerte Analyse-, Cloud-, Modellierungs- oder KI-Leistungen jedoch so ausgestaltet werden, dass der Dienstleister ausschließlich pseudonymisierte Daten erhält und aus seiner eigenen Perspektive über keine realistischen Identifizierungsmöglichkeiten verfügt. Hierzu können insbesondere eine wirksame Schlüsseltrennung, technisch beschränkte Ausgabekanäle sowie vertragliche und organisatorische Re-Identifizierungsverbote beitragen.

Aus Sicht der deutschen Versicherungswirtschaft sollten konsequent die tatsächlichen Re-Identifizierungsmittel und -möglichkeiten des jeweiligen Akteurs in die Bewertung einbezogen werden.

Anregung an den EDSA: In Rn. 15 sollte eine differenzierte Prüfung des Personenbezugs der vom Auftragnehmer verarbeiteten Daten vorgesehen werden. Maßgeblich sein sollten die tatsächlichen und rechtlichen Zugriffsmöglichkeiten, der Inhalt der Weisungen, mögliche Ausgabekanäle, die Rückspielbarkeit von Ergebnissen, die Schlüsseltrennung und realistische Kooperationspfade. Datenschutzrechtliche Pflichten des Auftragsverarbeiters sollten anhand des kontextbezogenen Ansatzes und der Grundsätze des SRB-Urteils vorgenommen werden dürfen, während die Pflichten des Verantwortlichen unberührt bleiben.

2.3 Gewichtung gesetzlicher und vertraglicher Verbote

Fundstellen: Rn. 32 bis 34

Wir begrüßen, dass die Leitlinien anerkennen, dass gesetzliche Verbote die Nutzung bestimmter Identifizierungsmittel wirksam ausschließen können (Rn. 32 f.). Kritisch zu sehen sind jedoch die sehr weit gefassten Anhaltspunkte in Rn. 33, die Hinweise auf rechtswidriges Verhalten seien. Es sollte zunächst grundsätzlich davon ausgegangen werden können, dass gesetzliche Vorgaben eingehalten werden. Als Hinweise auf rechtswidriges Verhalten sollten nur konkrete Anhaltspunkte gewertet werden, nicht z. B. allein ein Kostenvorteil oder eine unzureichende Rechtsdurchsetzung durch die zuständigen Behörden. Und eine grundsätzliche

Annahme rechtmäßigen Verhaltens der Akteure sollte auch für vertragliche Verbote gelten. Die in Rn. 34 zu findende geringere Gewichtung vertraglicher Verbote gegenüber gesetzlichen Verboten, die nur ergänzend zu technischen Maßnahmen wirksam seien, ist daher nicht nachvollziehbar.

Gerade in der Versicherungswirtschaft beruhen Datenübermittlungen an Rückversicherer, Schadendienstleister, Gutachter, IT-Dienstleister oder gemeinsame Datenpools regelmäßig auf langjährigen und eng überwachten Geschäftsbeziehungen. Dabei werden gesetzliche Vorgaben typischerweise durch vertragliche Zweckbindungs- und Re-Identifizierungsverbote sowie technische und organisatorische Schutzmaßnahmen ergänzt. Aus Sicht der deutschen Versicherungswirtschaft sollte deshalb sowohl bei gesetzlichen als auch bei vertraglichen Regelungen eine Gesamtschau maßgeblich sein.

Anregung an den EDSA: Der EDSA sollte anerkennen, dass sowohl gesetzliche Verbote als auch vertragliche Verbote zusammen mit technischen und organisatorischen Maßnahmen ein gleichberechtigtes starkes Indiz für empfängerbezogene Anonymität bilden können. Entscheidend sollten deren Wirksamkeit, Überprüfbarkeit, Durchsetzbarkeit und Beständigkeit sein, nicht die formale Einordnung als gesetzliches oder vertragliches Verbot.

2.4 Zukunftsmaßstab und periodische Neubewertung

Fundstellen: Fußnote zu Rn. 2; Rn. 35, 41 f.

Die Leitlinien weisen darauf hin, dass technische Entwicklungen, zusätzliche Datenquellen, Datenlecks und steigende Rechenleistung die Wahrscheinlichkeit einer Re-Identifizierung künftig erhöhen können. Ist diese Wahrscheinlichkeit nicht mehr lediglich insignifikant, sollen die Daten aus Sicht der jeweiligen Stelle wieder als personenbezogen gelten. Rn. 35 bezeichnet eine periodische Neubewertung insoweit als gute Praxis. Demgegenüber verlangt Erwägungsgrund 26 DSGVO lediglich, die zum Zeitpunkt der Verarbeitung verfügbare Technologie und vernünftigerweise vorhersehbaren technischen Entwicklungen zu berücksichtigen.

Die Leitlinien benennen für diese Anforderungen weder einen angemessenen Prognosezeitraum noch eine Erheblichkeitsschwelle. Eine zeitlich unbegrenzte Betrachtung sämtlicher denkbarer technischer Fortschritte wäre jedoch uferlos und daher nicht praktikabel.

Maßgeblich sollte vielmehr sein, ob eine Entwicklung im konkreten Verarbeitungs- und Nutzungskontext vorhersehbar ist und die Wahrscheinlichkeit einer Identifizierung wesentlich verändert. Eine Pflicht zur Neubewertung kann allenfalls ab vernünftigerweise zu erwartender Kenntnis eines wesentlichen neuen Risikos entstehen, beispielsweise nach einem Sicherheitsvorfall, wie Rn. 42 auch verlangt. Sie kann jedoch nur für Datenbestände in Betracht kommen, die von der jeweiligen Stelle noch vorgehalten oder genutzt werden.

Ferner dürfen zunächst nicht vorhersehbare technische Möglichkeiten nicht dazu

führen, dass eine bei damaliger Sachlage rechtmäßige Verarbeitung rückwirkend als rechtswidrig gilt. Maßgeblich muss die dokumentierte, zeitpunktbezogene Bewertung bleiben.

Anregung an den EDSA: Die Leitlinien sollten einen angemessenen, zweck- und lebenszyklusbezogenen Prognosezeitraum vorsehen. Eine Neubewertung sollte als risikobezogene gute Praxis und nicht als anlasslose Dauerpflicht beschrieben werden.

2.5 Vereinfachter Ansatz: Vermeidung eines faktischen Standards

Fundstelle: Rn. 48 und Fußnote 36.

Rn. 48 erkennt an, dass der vereinfachte Ansatz über den rechtlichen Maßstab hinausgehen und tatsächlich anonyme Daten als personenbezogen behandeln kann. Nach Fußnote 36 wird er als besonders sicherer und bequemer Einstieg in die Prüfung dargestellt.

Dass in Form eines sog. „vereinfachten Ansatzes“ der Versuch unternommen wird, einen praktikablen Weg zur schnellen Prüfung aufzuzeigen, ob Daten Personenbezug aufweisen oder als anonym anzusehen sind, erkennen wir grundsätzlich an. Es droht jedoch die Gefahr, dass ein solches, zunächst freiwilliges Vorsichtsmodell zur Vereinfachung oder Beschleunigung von Auditierungen oder externen Datenschutzprüfungen zum faktischen Erwartungsstandard wird. Unternehmen müssten dann entweder den strengeren Ansatz übernehmen oder aufwendig begründen, weshalb sie die gesetzlich vorgesehene kontextbezogene Prüfung anwenden.

Betrachtet man zudem die im Rahmen des „kontextbezogenen Ansatzes“ sehr weitreichenden Anforderungen an die Berücksichtigung möglicher Akteure, Identifizierungsketten und zusätzlichen Informationen, könnte man die Andienung des „vereinfachten Ansatzes“ als Versuch deuten, die von den Datenschutzaufsichtsbehörden bisher vertretene absolute Betrachtung des Personenbezugs weiterhin zum praktischen Maßstab zu machen.

Anregung an den EDSA: Es sollte noch deutlicher hervorgehoben werden, dass der vereinfachte Ansatz ein ausschließlich freiwillig anzuwendendes Hilfsmittel ist. Seine Anwendung darf nicht zu einer Beweislastverschiebung oder einem faktischen Stand der Technik führen. Dafür sollte auch klargestellt werden, dass ein negatives Ergebnis im vereinfachten Ansatz für sich genommen keine Aussage über das Vorliegen eines Personenbezugs oder die datenschutzrechtliche Zulässigkeit der Verarbeitung zulässt.

2.6 Anonymisierungsprozess, Transparenz und Dokumentation

Fundstellen: Rn. 38 bis 41.

Die Leitlinien stellen klar, dass der Anonymisierungsprozess eine Verarbeitung personenbezogener Daten darstellt, solange dabei personenbezogene Daten verarbeitet werden. Nach Auffassung des EDSA bedarf es daher einer

Rechtsgrundlage nach Art. 6 DSGVO und bei besonderen Kategorien personenbezogener Daten zusätzlich einer Ausnahme nach Art. 9 Abs. 2 DSGVO. Die bisherige Rechtsgrundlage und gegebenenfalls die bisherige Ausnahme einer Verarbeitung sollen fortgelten, wenn die Anonymisierung Teil derselben Verarbeitung für denselben Zweck ist (Rn. 38). Zudem leitet der EDSA aus den bestehenden Transparenz- und Rechenschaftspflichten Anforderungen an die Information der betroffenen Personen und die Dokumentation des Anonymisierungsprozesses ab.

Zutreffend ist, dass die Verarbeitung bis zum Abschluss der Anonymisierung den Anforderungen der DSGVO unterliegt. Daraus folgt jedoch nicht, dass für die Anonymisierung für einen weiteren Zweck stets eine eigenständige neue Rechtsgrundlage erforderlich ist. Erfolgt sie zu einem anderen Zweck als die ursprüngliche Verarbeitung, ist auch die Vereinbarkeitsprüfung nach Art. 6 Abs. 4 DSGVO zu berücksichtigen. Bei einem vereinbarten Zweck kann die ursprüngliche Rechtsgrundlage die Weiterverarbeitung inclusive der Anonymisierung dafür tragen.

Für die Praxis bleibt offen, unter welchen Voraussetzungen die Anonymisierung noch Teil derselben Verarbeitungstätigkeit ist und demselben Zweck dient. Ebenso fehlt ein Maßstab für die Dauer der Aufbewahrung der Anonymisierungsdokumentation und es sollten aus den allgemeinen Transparenz- und Rechenschaftspflichten keine zusätzlichen, speziell für die Anonymisierung geltenden Informations- oder Dokumentationspflichten abgeleitet werden. Umfang und Aufbewahrungsdauer der Dokumentation müssen sich auf das zur Erfüllung der bestehenden Nachweispflichten Erforderliche beschränken.

Anregung an den EDSA: Soweit die Leitlinien die Rechtsgrundlage der Anonymisierung behandeln, sollte Art. 6 Abs. 4 DSGVO berücksichtigt werden. Die Leitlinien sollten keine über die DSGVO hinausgehenden Anforderungen an Rechtsgrundlage, Transparenz oder Dokumentation begründen. Der mit der Anonymisierung verbundene Gewinn für den Datenschutz darf nicht durch zusätzliche Anforderungen geschmälert werden.

2.7 Drei Kriterien: Gesamtbetrachtung notwendig

Fundstellen: Rn. 52 ff.

Die Leitlinien verwenden „No Record Isolation“, „No Linkage“ und „No Inference“ als technische Prüfkriterien für die Anonymität. Sie stellen zwar klar, dass die Nichterfüllung eines Kriteriums nicht automatisch das Vorliegen personenbezogener Daten bedeutet. Aufgrund der hervorgehobenen Stellung der Kriterien und einzelner verkürzter Formulierungen kann jedoch der Eindruck entstehen, es handele sich um eigenständige kumulative Voraussetzungen der Anonymität. Maßgeblich bleibt demgegenüber allein, ob eine natürliche Person nach Art. 4 Nr. 1 und Erwägungsgrund 26 DSGVO unter Einsatz vernünftigerweise zu erwartender Mittel identifizierbar ist.

Besonders wichtig ist die Unterscheidung zwischen der Isolierbarkeit eines Datensatzes und der Identifizierbarkeit einer Person. Ein Datensatz kann zwar aufgrund

einer nur einmal vorkommenden Merkmalskombination einzigartig und damit isolierbar sein. Daraus ergibt sich jedoch noch nicht, welcher natürlichen Person er zuzuordnen ist oder dass diese auf seiner Grundlage individuell behandelt werden kann. Erst wenn die Merkmale mit vernünftigerweise verfügbaren Zusatzinformationen einer Person zugeordnet werden können oder auf andere Weise deren gezielte Unterscheidung ermöglichen, kann eine Identifizierbarkeit vorliegen, wie die Rn. 98 bis 100 und Beispiel 24 zutreffend zeigen.

Anregung an den EDSA: Die drei Kriterien sollten noch deutlicher als technische Indikatoren und nicht als eigenständige kumulative Tatbestandsvoraussetzungen dargestellt werden. Ihre Nichterfüllung sollte ausdrücklich nur Anlass für die weitergehende, kontextbezogene Gesamtprüfung sein. Insbesondere sollte deutlicher hervorgehoben werden, dass die Einzigartigkeit oder Isolierbarkeit eines Datensatzes für sich genommen noch keinen Personenbezug begründet.

2.8 Tarifierung, Risikobewertung und versicherungsmathematische Modelle

Fundstellen: Rn. 16, 50 und 67 bis 71; Beispiel 14.

Die deutsche Versicherungswirtschaft begrüßt die Klarstellungen in den Rn. 67 bis 71 und in Beispiel 14. Danach führt die Anwendung allgemeiner Erkenntnisse aus einem historischen Kreditdatenbestand auf die Risikoeinschätzung eines neuen Antragstellers nicht dazu, dass das Kriterium „No Inference“ verletzt ist. Denn wenn der Antragsteller nicht Teil des ursprünglich ausgewerteten Datenbestandes war, beruht die Schlussfolgerung zu seiner Person lediglich auf statistischen Informationen über eine entsprechende Vergleichsgruppe.

Diese Abgrenzung ist für die Versicherungswirtschaft zentral. Versicherer verwenden anonyme Schadenstatistiken, Trainings- und Referenzdaten sowie versicherungsmathematische Modelle, um Prämien, Reserven oder Risiken für vergleichbare Versicherungsrisiken oder Versicherungsnehmer zu bewerten. Der konkrete Risikoscore oder die Entscheidung über einen Versicherungsnehmer kann personenbezogen sein. Der zugrunde liegende anonyme Statistik-, Trainings- oder Referenzdatensatz wird dadurch jedoch nicht personenbezogen. Etwas anderes würde nur gelten, wenn das Modell oder der Datensatz spezifische Informationen über eine bestimmte Person aus dem Ausgangsdatenbestand offenbart.

Anregung an den EDSA: Es muss ganz deutlich werden, dass die Anwendung generalisierter Erkenntnisse auf eine identifizierte Person den anonymen Ausgangsdatenbestand nicht allein aufgrund des Verwendungszwecks wieder zu personenbezogenen Daten macht. Wir regen an, die in Beispiel 14 angelegte Abgrenzung im Haupttext deutlicher hervorzuheben und diese Überlegungen über den Kreditkontext hinaus auf statistische, versicherungsmathematische und KI-gestützte Risikomodelle zu übertragen.

Berlin, den 8. Oktober 2026