



BVDW-Stellungnahme zu den EDSA-Leitlinien 02/2026 zur Anonymisie- rung

Für einen rechtssicheren und praxis-
tauglichen Maßstab der Anonymisie-
rung

EXECUTIVE SUMMARY

Der BVDW begrüßt, dass die Leitlinien die Anonymität grundsätzlich aus der Perspektive der jeweils betrachteten Entität beurteilen. Dieser relative Ansatz wird jedoch nicht konsequent durchgehalten: Die Leitlinien dehnen den Personenbezug durch weit verstandene Kriterien, theoretische Re-Identifizierungsszenarien und eine unzureichende Berücksichtigung wirksamer Schutzmaßnahmen so weit aus, dass Anonymität in der Praxis kaum erreichbar wäre. Erforderlich ist ein rechtssicherer, operationalisierbarer Maßstab, der tatsächliche Identifizierungsmöglichkeiten bewertet und wirksame Anonymisierung fördert.

Aus Sicht des BVDW sind fünf Anpassungen zentral:

- Identifizierbarkeit eigenständig prüfen. Unterscheidbarkeit, Aussondern, Wiedererkennung, Profilbildung und Einwirkbarkeit sind lediglich Indizien oder mögliche Vorstufen einer Identifizierung; sie sind ihr weder einzeln noch kumulativ gleichzusetzen.
- Den relativen Ansatz konsequent anwenden. Maßgeblich sind die rechtlichen, technischen und tatsächlichen Möglichkeiten der jeweils betrachteten Stelle im jeweiligen Zeitpunkt.
- Nur vernünftigerweise wahrscheinliche Identifizierungsmittel berücksichtigen. Theoretische Möglichkeiten, zufällige Identifizierungen und Szenarien, die einen Rechtsbruch voraussetzen, dürfen nicht zum Regelmaßstab werden. Entscheidend sind tatsächlicher Zugang zu Zusatzinformationen, rechtliche Zulässigkeit, Kosten und Zeitaufwand, technische Machbarkeit, Genauigkeit und Erfolgswahrscheinlichkeit. Die Leitlinien sollten diese Faktoren in einem dokumentierbaren Prüfraster zusammenführen, angemessene Anforderungen für KMU vorsehen und von Aufsichtsbehörden die Benennung eines konkreten Re-Identifizierungspfads verlangen.
- Technische, organisatorische und vertragliche Schutzmaßnahmen gemeinsam bewerten. Wirksame Zugangsbeschränkungen und rechtlich bindende, überprüfbare und durchsetzbare Re-Identifizierungsverbote können die praktische Wahrscheinlichkeit einer Identifizierung erheblich senken und müssen risikomindernd berücksichtigt werden.
- Anonymisierung rechtlich fördern. Anonymisierung ist ein Verarbeitungsvorgang innerhalb einer Verarbeitungstätigkeit und benötigt weder einen eigenständigen Zweck noch eine eigene Rechtsgrundlage. Wirksam anonymisierte Informationen fallen nicht unter die DSGVO und müssen für weitere Zwecke wie Statistik, Produktverbesserung oder Forschung nutzbar sein. Rechtssicherheit und regulatorischer Spielraum schaffen den notwendigen Anreiz, in belastbare Anonymisierungsverfahren zu investieren.

Mit diesen Anpassungen können die Leitlinien den relativen Personenbezug in einen rechtssicheren und praxistauglichen Prüfmaßstab überführen, der den Schutz betroffener Personen mit verantwortungsvoller Datennutzung und Innovation verbindet.

Inhaltsverzeichnis

EXECUTIVE SUMMARY	1
1. EINLEITUNG	2
2. RECHTLICHE WÜRDIGUNG (ABSCHNITT 2 DER LEITLINIEN)	2
2.1 DER ZWEISTUFIGE PRÜFUNGSaufbau: IDENTIFIZIERBARKEIT ALS EIGENTLICHER PRÜFUNGSMAßSTAB.....	2
2.2 MAßGEBLICHE PERSPEKTIVE UND IHRE DURCHBRECHUNGEN.....	2
2.3 ANONYMISIERUNG VOR DER ÜBERMITTLUNG: REICHWEITE DER INFORMATIONSPFLICHT	3
2.4 AUFTRAGSVERARBEITUNG	3
2.5 DAS MERKMAL „RELATES TO“: INHALT, ZWECK UND WIRKUNG.....	4
2.6 „IDENTIFIED OR IDENTIFIABLE“	4
2.7 ANONYMISIERUNG INNERHALB EINER ORGANISATION.....	5
3. DER MAßSTAB DER „MEANS REASONABLY LIKELY TO BE USED“	6
3.1 FEHLENDE OPERATIONALISIERUNG	6
3.2 ZUKUNFTSBEZUG UND VERHÄLTNIßMÄßIGKEIT	6
3.3 KREIS DER RELEVANTEN STELLEN	7
3.4 MOTIVATION	7
4. ANERKENNUNG VERTRAGLICHER STEUERUNG („REGULATION BY CONTRACT“)	7
5. ZUM TECHNISCHEN PRÜFPROGRAMM (ABSCHNITT 3 DER LEITLINIEN).....	8
5.1 DATENSATZ UND DATENSEGMENTE; FOLGEFRAGEN	8
5.2 NO LINKAGE.....	9
5.3 NO INFERENCE	9
6. ANONYMISIERUNG ALS VERARBEITUNGSVORGANG OHNE EIGENEN ZWECK UND OHNE EIGENE RECHTSGRUNDLAGE	9
7. SCHLUSSBEMERKUNG.....	10

1. Einleitung

Der Bundesverband Digitale Wirtschaft (BVDW) e.V. begrüßt die Gelegenheit, zu den Leitlinien des Europäischen Datenschutzausschusses (EDSA) Stellung zu nehmen. Für die Unternehmen der digitalen Wirtschaft hat die Abgrenzung zwischen personenbezogenen und anonymen Daten erhebliche praktische Bedeutung.

Die Leitlinien erscheinen zu einem Zeitpunkt, an dem der Gerichtshof die Grundlagen geklärt hat. Mit dem Urteil EDSB/SRB (EuGH, Urt. v. 4.9.2025 – C-413/23 P) hat er die Linie der Breyer-Rechtsprechung fortgeführt. Ob eine Information personenbezogen ist, bemisst sich nach der Perspektive der jeweiligen Stelle und den Mitteln, die diese nach allgemeinem Ermessen wahrscheinlich nutzt. Dass sich der EDSA zu diesem relativen Ansatz bekennt, begrüßt der BVDW.

In der Ausgestaltung bleiben die Leitlinien jedoch an mehreren Stellen hinter diesem Ausgangspunkt zurück. Weite Auslegungen des Merkmals „relates to“, eine Gleichsetzung von Individualisierbarkeit und Identifizierbarkeit, ein sehr weiter Kreis relevanter Stellen und der weitgehende Ausschluss vertraglicher Maßnahmen führen im Ergebnis dazu, dass Anonymisierung in der Praxis kaum implementierbar ist. Zugleich fehlt es an operationalisierbaren Kriterien, anhand derer Verantwortliche ihre Beurteilung belegen und Aufsichtsbehörden sie überprüfen können.

2. Rechtliche Würdigung (Abschnitt 2 der Leitlinien)

2.1 Der zweistufige Prüfungsaufbau: Identifizierbarkeit als eigentlicher Prüfungsmaßstab

Zutreffend gliedert der EDSA in den Leitlinien den Kerntest in zwei Stufen: Zu fragen ist zunächst, ob sich die Information auf eine natürliche Person bezieht (a), sodann, ob diese Person identifiziert oder identifizierbar ist (b). Auf der zweiten Stufe ist eine echte Risikobetrachtung anzustellen. Bei der Erläuterung des Tests beschränkt sich der EDSA indes im Wesentlichen auf die Eintrittswahrscheinlichkeit („likelihood“), ohne die Risikodimension methodisch auszuformen.

Die in den Leitlinien herausgearbeitete Prüfung, ob die betreffende Stelle Zugang zu den Daten oder Kontrolle über sie hat oder erlangen kann, ist sachgerecht, sollte allerdings konsequenter durchgehalten werden, namentlich dort, wo die Leitlinien später sehr weite Empfängerkreise in den Blick nehmen.

Die Leitlinien sollten um eine ausdrückliche Risikobetrachtung ergänzt werden, die Eintrittswahrscheinlichkeit und Schwere der Auswirkungen für die betroffene Person zueinander in Beziehung setzt.

2.2 Maßgebliche Perspektive und ihre Durchbrechungen

Ausgangspunkt der Prüfung, ob ein Datum anonym ist, ist nach den Leitlinien die jeweilige Stelle und deren Perspektive. Die Leitlinien sehen jedoch Durchbrechungen dieses Grundsatzes vor, ohne sie systematisch zu erfassen.

Die Perspektive des Empfängers zum Maßstab zu erheben ist nur dann folgerichtig, wenn tatsächlich allein auf den Empfänger abgestellt wird; maßgeblicher Bezugspunkt sind dessen Fähigkeiten. Die in den Leitlinien angenommene „Rückwirkung“ auf den Übermittelnden – wonach die Daten auch für die übermittelnde Stelle mittelbar personenbezogen werden – liefe darauf hinaus, den relativen Ansatz im Ergebnis abzuschwächen. Mit der Rechtsprechung lässt sie sich kaum in Einklang bringen.

Zudem stellt der Ausschuss die Behauptung auf, dass bestimmte Pflichten aus der DSGVO die Perspektive durchbrechen können. Offen bleibt jedoch, welche Pflichten dies im Einzelnen sind.

2.3 Anonymisierung vor der Übermittlung: Reichweite der Informationspflicht

Werden personenbezogene Daten erhoben und vor ihrer Übermittlung anonymisiert, sollen nach den Leitlinien gleichwohl die Empfänger zu benennen sein, weil die Daten im Zeitpunkt ihrer Erhebung personenbezogen waren. Daraus erwächst eine für die Praxis zentrale Folgefrage: Gilt dies auch dann, wenn der ursprüngliche Erhebungszweck die spätere Übermittlung nicht umfasste, diese im Zeitpunkt der Erhebung also weder geplant noch absehbar war? Und gilt dies auch dann, wenn der Verantwortliche gerade deshalb anonymisiert, um einer Löschpflicht nachzukommen, und sich der Nutzen des anonymen Datenbestands für Analysen erst nachträglich ergibt?

Hinzu kommt ein innerer Widerspruch: Werden die Daten vor der Übermittlung anonymisiert, betrifft der Übermittlungsvorgang selbst keine personenbezogenen Daten mehr. Er fällt nicht in den Anwendungsbereich der Verordnung. Eine Pflicht, Empfänger anonymer Informationen zu benennen, lässt sich daher allenfalls aus der Perspektive des Verantwortlichen im Zeitpunkt der Erhebung begründen. Sie kann sich – wenn überhaupt – nur auf Übermittlungen erstrecken, die zu diesem Zeitpunkt bereits geplant oder absehbar waren.

2.4 Auftragsverarbeitung

Entscheidend ist, dass die Zuordnung der Auftragsverarbeitung zur Sphäre des Verantwortlichen nur die Frage des Personenbezugs aus der Perspektive des Verantwortlichen beantwortet, nicht aus derjenigen des Auftragsverarbeiters. Ob die Daten für den Auftragsverarbeiter selbst personenbezogen sind, folgt daraus nicht; dies ist gesondert festzustellen. Rollen im Sinne der DSGVO sind funktional und auf den einzelnen Verarbeitungsvorgang bezogen. Die Aussage des EDSA zur Auftragsverarbeitung ist daher zu präzisieren und darf nicht über das hinausgehen, was dem Regelungszweck und dem Anwendungsbereich der DSGVO immanent ist. Verfügt der Auftragsverarbeiter über keine Mittel, die nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der betroffenen Personen genutzt werden, so beruht die Einordnung der Daten als personenbezogen nicht auf einer Anwendung von Art. 4 Nr. 1 DSGVO und ErwG 26, sondern auf einer Rechtsfiktion, die allein an das Auftragsverhältnis anknüpft.

Diese Fiktion lässt sich nicht auf die Rechtsprechung des Gerichtshofs stützen. Im Urteil EDSB/SRB hat der Gerichtshof festgehalten, dass Informationen nicht in jedem Fall und nicht für jede Stelle personenbezogen sein müssen und dass technische und organisatorische Maßnahmen dazu führen können, dass Informationen für einen Empfänger ohne Identifizierungsmöglichkeit keinen Personenbezug aufweisen. Ob die Informationen aus Sicht des Empfängers personenbezogen waren, hat der Gerichtshof offengelassen.

Zudem droht ein Zirkelschluss. Auftragsverarbeiter ist nach Art. 4 Nr. 8 DSGVO, wer personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Aus dieser Rolle zwingend abzuleiten, dass die Daten auch für den Auftragsverarbeiter personenbezogen sind, setzt voraus, was erst zu prüfen wäre.

Das Auftragsverhältnis mag ein gewichtiger tatsächlicher Umstand im Rahmen der Identifizierbarkeitsprüfung sein, nicht aber deren Ersatz. Dies entspricht der Aussage der Leitlinien, dass das Verhältnis der Beteiligten und die Verarbeitung im Auftrag einer anderen Stelle Umstände sind, die für die maßgebliche Perspektive von Bedeutung sind. Das macht die Prüfung der tatsächlichen rechtlichen, technischen und organisatorischen Umstände aber nicht entbehrlich.

Zudem sind die gezogene Konsequenz, die Anwendung der Pflichten des Auftragsverarbeiters, u. a. aus Art. 28, 29, 30 Abs. 2 und 32 DSGVO, für die weiteren Aussagen in den Leitlinien als das zu benennen werden, was sie der Sache nach sind: eine wirksame vertragliche Kontrolle über die Daten. Konsequenterweise muss dieselbe Wertung auch bei der Beurteilung vertraglicher Maßnahmen gelten. Der EDSA erkennt in den Leitlinien selbst an, dass vertragliche Vereinbarungen und Pflichten aus der DSGVO zusammenwirken, um einen sachgerechten Umgang des Auftragsverarbeiters mit den personenbezogenen Daten sicherzustellen (dazu später mehr).

2.5 Das Merkmal „relates to“: Inhalt, Zweck und Wirkung

Die zugrunde gelegte Trias aus Inhalt, Zweck und Wirkung ist in ihrer Reichweite und begrifflichen Fassung zu weit geraten. Unproblematisch ist zumindest noch das Inhaltselement.

Anders verhält es sich mit dem Zweckelement. Danach genügt es, dass die Information die Person oder etwas mit ihr in Verbindung Stehendes betrifft und dazu verwendet werden soll, die Person zu bewerten, in bestimmter Weise zu behandeln oder zu beeinflussen. Die Information erzeugt weder selbst einen Identifikator, noch steht sie zwingend in einem Zurechnungsverhältnis zu der Person. Käme es allein auf die mit der Verarbeitung verfolgte Absicht an, hinge die Einordnung von subjektiven, ex ante nicht bestimmbarsten Umständen ab; sie wäre kaum noch verlässlich vorhersehbar.

Das Wirkungselement erfasst Informationen über Gegenstände, deren Verarbeitung sich lediglich auf die Person auswirkt. Die in den Leitlinien verlangte „konkrete Möglichkeit“ einer Ungleichbehandlung bleibt jedoch ohne nähere Konturen. Ohne eine solche Eingrenzung droht das Kriterium nahezu jede Datenverarbeitung in den Anwendungsbereich der DSGVO zu ziehen.

Der EDSA schreibt in den Leitlinien außerdem, dass ein Bezug auch dann bestehen soll, wenn die Verbindung erst durch weitere Verarbeitungsschritte hergestellt werden muss; ausdrücklich auch bei aggregierten Informationen. Im Zusammenspiel mit dem Wirkungselement hätte dies zur Folge, dass aggregierte Informationen regelmäßig als potenziell personenbezogen zu behandeln wären. Das widerspricht der ebenfalls in den Leitlinien getroffenen Feststellung, wonach aggregierte Daten das Kriterium der „No Record Isolation“ regelmäßig erfüllen.

Das Wirkungselement muss restriktiv und in Orientierung an der Rechtsprechung des Gerichtshofs auszulegen; maßgeblich muss eine konkrete, nicht bloß theoretische Auswirkung auf eine bestimmte Person sein. Das Zweckelement sollte dahin präzisiert werden, dass es auf eine objektiv feststellbare, im Zeitpunkt der Verarbeitung angelegte Zuordnung zu einer konkreten Person ankommt – nicht auf eine hypothetische Verwendungsabsicht. Andernfalls wären auch rein sachbezogene Informationen, etwa über Gegenstände, Vorgänge oder technische Systeme, in einer Vielzahl von Fällen als personenbezogen einzustufen. Die Unterscheidung zwischen personenbezogenen und nicht personenbezogenen Daten, auf der die DSGVO aufbaut, verlöre damit an Bestimmbarkeit.

2.6 „identified or identifiable“

Die Leitlinien bestimmen die Identifizierung (direkt und indirekt) im Kern anhand zweier Elemente: Eine natürliche Person müsse in einem bestimmten Kontext von anderen unterscheidbar sein, und diese Unterscheidbarkeit müsse es ermöglichen, sie anders zu behandeln. Dieser Ansatz greift zu weit. Unterscheidbarkeit und die Möglichkeit einer Einwirkung können Anhaltspunkte für eine Identifizierbarkeit sein; sie sind mit ihr aber weder einzeln noch kumulativ gleichzusetzen. Art. 4 Nr. 1 DSGVO verlangt neben dem Bezug einer Information zu einer natürlichen Person eigenständig, dass diese Person identifiziert oder identifizierbar ist. Dieses Tatbestandsmerkmal darf nicht durch Indizien ersetzt werden.

Unterscheidbarkeit besagt zunächst nur, dass ein Datensatz, Profil, Gerät, Browser oder Anschluss von anderen abgegrenzt werden kann. Auch das in Erwägungsgrund 26 genannte Aussondern beschreibt lediglich ein mögliches Mittel auf dem Weg zu einer Identifizierung, nicht deren Ergebnis.

Auch die Möglichkeit einer unterschiedlichen Behandlung schließt diese Lücke nicht. Sie zeigt lediglich, dass auf ein unterscheidbares technisches Objekt oder Profil eingewirkt werden kann. Eine Werbeauspielung anhand einer Cookie-ID, Werbe-ID oder eines Fingerprints behandelt etwa einen Browser, ein Endgerät oder ein pseudonymes Profil anders als andere. Daraus folgt weder, dass die handelnde Stelle die dahinterstehende natürliche Person kennt, noch, dass sie diese mit Mitteln bestimmen kann, die nach allgemeinem Ermessen wahrscheinlich genutzt werden.

Die Leitlinien verwechseln damit die Unterscheidbarkeit mit einer möglichen Folge der Identifizierung. Ist eine natürliche Person identifiziert oder identifizierbar, kann dies der handelnden Stelle ermöglichen, gezielt auf sie einzuwirken. Daraus folgt jedoch nicht die Umkehrung, dass jede

Einwirkungsmöglichkeit oder Unterscheidbarkeit eine direkte oder indirekte Identifizierbarkeit voraussetzt oder belegt. Die Relation ist asymmetrisch. Identifizierbarkeit kann Einwirkbarkeit ermöglichen; Einwirkbarkeit begründet für sich genommen aber keine Identifizierbarkeit.

Das zeigt ein vereinfachtes Beispiel an Hand der Ausspielung von Werbung. Ein System kann anhand einer Kennung Inhalte auswählen und damit das Nutzungserlebnis einer natürlichen Person tatsächlich beeinflussen, ohne dass die handelnde Stelle bestimmen kann, um welche Person es sich handelt. Die Wirkung tritt dann vermittelt über ein Gerät, einen Browser oder ein pseudonymes Profil ein. Sie richtet sich faktisch an einen Nutzer, stellt aber noch keine belastbare Verbindung zwischen der verarbeiteten Information und einer bestimmten oder bestimmbaren natürlichen Person her.

Auch die kumulative Verbindung von Unterscheidbarkeit und Einwirkbarkeit beseitigt diesen Logikfehler nicht. Beide Merkmale können ohne Identifizierbarkeit zugleich vorliegen. Ein Profil kann von anderen Profilen abgegrenzt, wiedererkannt und individuell behandelt werden, obwohl die dahinterstehende natürliche Person nicht mit vernünftigerweise wahrscheinlich eingesetzten Mitteln bestimmt werden kann. Zwei Indizien ergeben zusammen keinen Ersatz für die gesetzlich geforderte Identifizierbarkeit.

Dies entspricht der Systematik der DSGVO. Pseudonymisierte Datensätze bleiben anhand eines Kennzeichens unterscheidbar, können einer natürlichen Person aber ohne gesondert aufbewahrte Zusatzinformationen nicht zugeordnet werden. Ebenso setzt Art. 11 DSGVO voraus, dass ein Verantwortlicher personenbezogene Daten verarbeiten kann, ohne die betroffene Person zu identifizieren. Wäre bereits jede Unterscheidbarkeit oder individuelle Behandlung eine Identifizierung, liefen diese Differenzierungen weitgehend leer.

Entsprechendes gilt für IP-Adressen, Cookie-IDs, Werbe-IDs, MAC-Adressen, Fingerprints, Sozialversicherungsnummern und vergleichbare Kennungen. Sie bezeichnen zunächst einen Anschluss, ein Gerät, einen Browser, ein Nutzerkonto oder einen Datensatz. Ob dadurch auch eine natürliche Person identifizierbar ist, hängt von zusätzlichen Zuordnungsmitteln ab. Erforderlich ist eine belastbare Verbindung zwischen der Kennung und einer natürlichen Person.

Entscheidend bleibt daher der Filter der Mittel, die nach allgemeinem Ermessen wahrscheinlich zur Identifizierung genutzt werden. Zu prüfen sind aus der Perspektive der jeweiligen Stelle insbesondere der tatsächliche Zugang zu Zusatzinformationen, die rechtliche Zulässigkeit ihrer Erlangung und Verknüpfung, Kosten und Zeitaufwand, technische Machbarkeit sowie Genauigkeit und Erfolgswahrscheinlichkeit.

Die Leitlinien sollten daher klarstellen, dass Unterscheidbarkeit und Einwirkbarkeit weder alternative noch kumulative Ersatzmerkmale der Identifizierung sind. Insbesondere darf aus einer möglichen Einwirkung nicht auf Identifizierbarkeit zurückgeschlossen werden: Die Einwirkung kann Folge einer Identifizierung sein, tritt aber ebenso gegenüber lediglich unterscheidbaren Geräten, Browsern oder pseudonymen Profilen auf.

2.7 Anonymisierung innerhalb einer Organisation

Die Leitlinien erkennen im Grundsatz an, dass eine Anonymisierung auch ohne Löschung der Ausgangsdaten möglich ist. Alle Beispiele, die diesen Grundsatz veranschaulichen, sind jedoch auf eine Offenlegung nach außen zugeschnitten, während jede Darstellung einer Anonymisierung innerhalb einer Organisation mit der Löschung der Ausgangsdaten verknüpft wird. Daraus entsteht – auch wenn dies nicht beabsichtigt sein dürfte – der Eindruck, ein Verantwortlicher könne Daten für eigene interne Zwecke nur anonymisieren, wenn er die Quelldaten löscht.

Dies liegt oberhalb des von den Leitlinien selbst formulierten Maßstabs und ist kontraproduktiv: Verantwortliche, die in interne Anonymisierung investieren, erhalten dafür keine regulatorische Anerkennung. Die kontextuelle, perspektivbezogene Methodik der Leitlinien ist ohne Weiteres in der Lage, eine abgeschirmte interne Umgebung als maßgeblichen Bezugspunkt zu erfassen; dies entspricht unmittelbar dem Grundsatz der Datenminimierung nach Art. 5 Abs. 1 lit. c DSGVO.

Der BVDW empfiehlt daher klarzustellen, dass die Anonymität auch innerhalb einer Organisation beurteilt werden kann und dass das Vorhalten der Ausgangsdaten an anderer Stelle der Organisation die Anonymität nicht bereits für sich genommen ausschließt, sofern eine Re-Identifizierung aus der maßgeblichen internen Perspektive nach allgemeinem Ermessen nicht wahrscheinlich ist. Die Begriffsbestimmung der relevanten Stelle und die Ausführungen zur maßgeblichen Perspektive sollten entsprechend erweitert und um mindestens ein Beispiel einer organisationsinternen Anonymisierung ohne Löschung der Ausgangsdaten ergänzt werden.

3. Der Maßstab der „means reasonably likely to be used“

3.1 Fehlende Operationalisierung

Positiv hervorzuheben ist, dass der EDSA in den Leitlinien objektive Faktoren benennt: die Eigenschaften des Datensatzes und seine Anfälligkeit für unterschiedliche Angriffsvektoren, den Kontext der Verarbeitung einschließlich wirksamer und dauerhafter Zugangsbeschränkungen, den Zugang zu weiteren Daten, Kosten und Zeitaufwand sowie die verfügbare Technologie. Diese Faktoren sollten zu einem nachvollziehbaren und dokumentierbaren Prüfraster fortentwickelt werden, anhand dessen Verantwortliche ihre Beurteilung belegen und Aufsichtsbehörden sie überprüfen können.

In verfahrensrechtlicher Hinsicht ist zudem klarzustellen, dass die Darlegungs- und Beweislast für das Vorliegen eines Personenbezugs im Ausgangspunkt die Aufsichtsbehörde trifft. Zwar erstreckt sich die Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) auf den Anonymisierungsvorgang als solchen. Die Leitlinien dürfen jedoch nicht auf eine Annahme einer sekundären Darlegungslast oder eine faktische Beweislastumkehr hinauslaufen, die Verantwortlichen den Nachweis abverlangt, dass kein denkbarer Re-Identifizierungspfad besteht. Besonders problematisch ist insoweit die Bezeichnung einer Anonymitätsfeststellung als „false positive“ in den Leitlinien. Damit wird der Schluss auf Anonymität als zu vermeidender Fehler eingeordnet und im Ergebnis eine Vermutung des Personenbezugs begründet. Eine Aufsichtsbehörde, die den Personenbezug behauptet, sollte vielmehr einen konkreten Re-Identifizierungspfad benennen müssen und sich nicht auf eine theoretische Möglichkeit beschränken können.

KMU und Start-ups fehlt häufig die rechtliche und technische Expertise, um alle relevanten Akteure, Zusatzdatensätze, möglichen Re-Identifizierungsketten und die technische Entwicklung zu erfassen. Der vereinfachte Ansatz wirkt für sie handhabbarer, führt bei systematischer Anwendung aber dazu, dass tatsächlich anonyme Daten als personenbezogen behandelt werden. Der kontextuelle Ansatz verlangt dagegen Ressourcen und eine Dokumentationstiefe, die kleinere Unternehmen überfordern kann. Das vorgeschlagene Prüfraster sollte deshalb an etablierte internationale Normen anknüpfen, namentlich an ISO/IEC 27559:2022 (Rahmenwerk für die Deidentifizierung) und ISO/IEC 20889:2018 (Terminologie und Klassifikation von Deidentifizierungstechniken).

In einen Annex sollte ein strukturiertes, dokumentierbares Prüfraster („Anonymisierungs-Assessment“) aufgenommen werden, einschließlich einer angemessenen Dokumentationstiefe für KMU. Ein solches Raster würde zugleich die in den Leitlinien geforderte Dokumentation des Anonymisierungsprozesses handhabbar machen.

3.2 Zukunftsbezug und Verhältnismäßigkeit

Zu begrüßen ist die Klarstellung des EDSA in den Leitlinien, dass sich der Test allein auf eine mögliche künftige Identifizierung bezieht. Ebenso begrüßenswert ist die Klarstellung, dass Mittel außer Betracht bleiben, deren Einsatz einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft erfordern würde. Dieser Maßstab wird im weiteren Verlauf jedoch abgeschwächt. So halten die Leitlinien daran fest, dass Zeit und Kosten in der Regel nicht prohibitiv seien. Damit widersprechen sich die Leitlinien selbst, denn Zeit, Kosten und Arbeitsaufwand werden zuvor ausdrücklich als relevante Faktoren benannt. Auch der Hinweis auf KI-gestützte Re-Identifizierung führt in Verbindung mit der Anknüpfung an die Ressourcen der jeweiligen Stelle zu dem widersinnigen Ergebnis, dass gerade besonders leistungsfähige Organisationen Anonymität nie erreichen könnten. Es sollte klargestellt werden, dass überlegene Ressourcen allein die Anonymität nicht ausschließen.

Die Leitlinien sollten konkretisieren, ab wann ein Aufwand an Zeit, Kosten und Arbeitskraft als unverhältnismäßig anzusehen ist, und hierfür quantitative Orientierungswerte oder anerkannte Metriken benennen, anhand derer Verantwortliche ihre Verfahren validieren können. Darüber hinaus sollten die Leitlinien datenschutzfreundliche Technologien (Privacy-Enhancing Technologies, PETs) substantiell behandeln. Anhand praktischer Beispiele sollte erläutert werden, wie Differential Privacy, sichere Mehrparteienberechnung, homomorphe Verschlüsselung und synthetische Daten unter geeigneten Umständen zur Anonymisierung beitragen können. Dass ihre Wirksamkeit stets im jeweiligen Kontext zu beurteilen ist, bleibt davon unberührt. Solche Hinweise würden den Stand der Technik besser abbilden und Investitionen in Verfahren fördern, die wirksame Anonymisierung gerade für KMU erreichbar machen. Das vorgeschlagene Prüfraster im Annex sollte durch KMU-spezifische Beispiele ergänzt werden, die zeigen, wie eine belastbare kontextuelle Beurteilung mit begrenzten Ressourcen gelingt. Zu PETs sollten Praxisbeispiele aufgenommen werden.

3.3 Kreis der relevanten Stellen

Der EDSA bezieht in den Leitlinien unmittelbare wie mittelbare Empfänger in sehr weitem Umfang ein. Diese Stellen können gegebenenfalls bei der Bewertung der Informationssicherheit eine Rolle spielen. Für die Abgrenzung zwischen anonymen und personenbezogenen Daten hat eine derart weite Betrachtung jedoch zur Folge, dass Anonymität praktisch nicht erreichbar ist, weil sich das Verhalten rechtswidrig handelnder Dritter niemals ausschließen lässt. Die Aufzählung in den Leitlinien darf kein obligatorisches Prüfprogramm begründen. Einzubeziehen sind nur solche Stellen, für deren Zugang zu den Daten im konkreten Verarbeitungskontext tatsächliche Anhaltspunkte bestehen.

Maßgeblich ist nicht, ob eine Identifizierung theoretisch möglich ist, sondern ob sie unter den konkreten Umständen vernünftigerweise vorhersehbar ist. Die Vorhersehbarkeit ist dem Maßstab der „means reasonably likely to be used“ nach ErwG 26 S. 3 DSGVO immanent. Eine bloß theoretische Möglichkeit genügt nicht, und in den Blick zu nehmen sind nur Personen und Mittel, die über einen Zugang zu den erforderlichen Zusatzinformationen verfügen oder ihn vernünftigerweise erlangen können.

3.4 Motivation

Der EDSA warnt in den Leitlinien davor, eine fehlende Motivation zur Re-Identifizierung als Faktor heranzuziehen, insbesondere mit Blick auf Stellen, bei denen konkrete Anhaltspunkte für einen rechtswidrigen Zugriff bestehen. Es sollte klargestellt werden, dass Re-Identifizierungsszenarien, die einen Rechtsbruch voraussetzen, grundsätzlich außer Betracht bleiben und nur bei konkreten, belegbaren Anhaltspunkten zu berücksichtigen sind. Konsequenterweise sollten unbefugt und rechtswidrig handelnde Akteure aus dem Kreis der relevanten Stellen gestrichen werden. Entsprechendes gilt für die versehentliche Identifizierung. Zufall und Fahrlässigkeit sind im Rahmen der Sicherheitsbewertung zu berücksichtigen, nicht aber bei der Frage nach dem Personenbezug im Sinne von Art. 4 Nr. 1 DSGVO.

4. Anerkennung vertraglicher Steuerung („Regulation by Contract“)

Die DSGVO selbst setzt in erheblichem Umfang auf vertragliche Steuerung. Art. 28 DSGVO macht den Auftragsverarbeitungsvertrag zum Instrument der Kontrolle über die Daten; Art. 46 Abs. 2 lit. c DSGVO erhebt Standardvertragsklauseln zu geeigneten Garantien für Übermittlungen in Drittländer; Art. 40 DSGVO erkennt Verhaltensregeln mit verbindlicher Wirkung an. An anderer Stelle werden vertragliche Bindungen mithin als hinreichend wirksam angesehen, um Grundrechtsschutz herzustellen; bei der Beurteilung der Anonymität sollen sie hingegen im Wesentlichen unbeachtlich sein. Dieser Wertungswiderspruch sollte aufgelöst werden.

Auch wenn eine vertragliche Verpflichtung weder die grundlegende Beschaffenheit von Daten ändern noch eine wirksame technische De-Identifizierung ersetzen kann, stellen durchsetzbare Vertragsbedingungen eine wesentliche, ergänzende Schutzmaßnahme dar. Die Leitlinien sollten anerkennen, dass in kontrollierten Umgebungen rechtsverbindliche und überwachte vertragliche

Verpflichtungen (gestützt durch Rechtsbehelfe wie Audit-Rechte, Schadensersatz, Vertragsstrafen und einstweiligen Rechtsschutz) die praktische Wahrscheinlichkeit einer Re-Identifizierung messbar senken.

Schließlich erkennt der Ausschuss „wirksame und dauerhafte Zugangsbeschränkungen“ und Sicherheitskontrollen als Faktoren an, die den Kreis der relevanten Akteure auf autorisierte Nutzer begrenzen. In der Praxis wirken vertragliche und technische Maßnahmen gerade im Verbund.

Der Ausschluss vertraglicher Maßnahmen sollte daher durch einen Nachweismaßstab ersetzt werden. Ist ein Re-Identifizierungsverbot rechtlich bindend, durch Audits oder technische Nachweise überprüfbar und mit durchsetzbaren Folgen versehen und flankiert es wirksame technische Maßnahmen, ist es bei der Beurteilung der nach allgemeinem Ermessen wahrscheinlich genutzten Mittel risikomindernd zu berücksichtigen. Selbst eine Maßnahme, die diese Voraussetzungen nicht erfüllt, kann zwar geringeres Gewicht haben; das Gewicht ist jedoch zu bewerten und nicht pauschal zu verneinen.

5. Zum technischen Prüfprogramm (Abschnitt 3 der Leitlinien)

5.1 Datensatz und Datensegmente; Folgefragen

Die Unterscheidung zwischen der Anonymität des Datensatzes als solchen und derjenigen einzelner Teile in den Leitlinien ist sachgerecht. Die daran geknüpfte Rechtsfolge, ein Datensatz ist nur dann anonym, wenn er es für alle darin erfassten Personen ist; anderenfalls gilt der gesamte Datensatz als personenbezogen, ist jedoch sehr weitreichend. Sie sollte um praxistaugliche Möglichkeiten der Trennung ergänzt werden. Zu differenzieren ist danach, ob die Daten trennbar sind oder nicht. Die in den Leitlinien herangezogene Parallele zum Urteil Meta Platforms/Bundeskartellamt trägt nicht. Die dortigen Ausführungen betreffen besondere Kategorien und sonstige personenbezogene Daten, die bei der Erhebung nicht getrennt werden können, nicht aber den rechtlichen Status anonymer Informationen. ErwG 26 S. 5 DSGVO nimmt anonyme Informationen ausdrücklich vom Anwendungsreich der Verordnung aus. Dabei ist zu prüfen, ob sich die Bestandteile trennen lassen und ob identifizierbare Datensätze die Anonymität der übrigen beeinträchtigen. Die Re-Identifizierung einer einzelnen Person kann diese Prüfung auslösen, nicht aber ohne Weiteres über den Status nicht betroffener Datensätze entscheiden. Maßgeblich ist, ob die Umstände, die die Identifizierung eines Datensatzes ermöglicht haben, die Identifizierbarkeit der übrigen wesentlich erhöhen. Hinzu kommt, dass die Leitlinien die Formulierung des Gerichtshofs verändern. Dort war maßgeblich, ob eine Trennung der Daten möglich war, während die Leitlinien darauf abstellen, ob die Daten getrennt behandelt werden – also auf eine Handhabungsentscheidung. Richtigerweise sollte die Prüfung zwei Fragen stellen: ob das Re-Identifizierungsrisiko über den Datensatz hinweg unerheblich ist und ob identifizierbare Datensätze trennbar sind.

Dass sich die Anonymität von Daten mit dem technischen Fortschritt, dem Stand der Technik und den Fähigkeiten der beteiligten Stellen verändern kann, ist mag richtig sein. Tatsächlich anonyme Informationen liegen jedoch außerhalb des Anwendungsbereichs der DSGVO. Die als „good practice“ bezeichnete Überprüfung darf deshalb nicht in eine fortdauernde, anlasslose Überwachungspflicht nach der DSGVO für Daten umschlagen, die ursprünglich zu Recht als nicht personenbezogen eingestuft wurden. Offen lassen die Leitlinien zudem, wen die Überprüfung trifft: den anonymisierenden Verantwortlichen, die Stelle, die den Datensatz aktuell nutzt, oder auch Auftragsverarbeiter und Unterauftragsverarbeiter. Statt einer unbestimmten, fortlaufenden Überprüfungspflicht sollten definierte Auslöser benannt werden: eine wesentliche Sicherheitsverletzung, die eine tatsächlich herangezogene Schutzmaßnahme betrifft, oder ein belegter Re-Identifizierungspfad.

Die ursprüngliche Beurteilung ist an den Informationen und der Technik zu messen, die im Zeitpunkt ihrer Vornahme verfügbar waren. Neue Daten, Technologien oder Verfahren machen eine frühere, auf dem damaligen Erkenntnisstand beruhende Beurteilung nicht nachträglich fehlerhaft. Wird das Identifizierungsrisiko später erheblich, hat die betroffene Stelle die Daten ab dem Zeitpunkt als personenbezogen zu behandeln, zu dem sie von der Änderung Kenntnis erlangt oder hätte erlangen müssen. Eine nachträgliche Änderung der Umstände macht eine frühere Verarbeitung nicht

rechtswidrig, wenn die ursprüngliche Beurteilung vertretbar war.

5.2 No Linkage

Zwar stellt der EDSA in den Leitlinien klar, dass im kontextuellen Ansatz zu fragen ist, ob die Verknüpfung aus der jeweiligen Perspektive mit „means reasonably likely to be used“ möglich ist. Die dortige Definition der Verknüpfbarkeit und die dazugehörigen Beispiele folgen jedoch dem vereinfachten Ansatz. Die Leitlinien sollten deutlicher hervorheben, dass die Verknüpfbarkeit am Maßstab der „means reasonably likely to be used“ zu beurteilen ist – also unter Berücksichtigung des tatsächlichen Zugangs zu den Zusatzdaten sowie der rechtlichen und vertraglichen Zulässigkeit der Verknüpfung.

5.3 No Inference

Das Kriterium ist erfüllt, wenn sich aus den Daten keine spezifische und bedeutsame Schlussfolgerung ziehen lässt. Die Abgrenzung ist in der Anwendung jedoch kaum praktikabel. Der in den Leitlinien vorgeschlagene Vergleichstest (Auswertung mit und ohne den Datensatz der betroffenen Person) lässt sich für aggregierte Daten und KI-Modelle in der Praxis nur mit erheblichem Aufwand umsetzen. Die dort vorgesehene widerlegliche Vermutung ist als Auffanglösung zu begrüßen; sie steht jedoch nur zur Verfügung, wenn weder die Nachverfolgung noch der Vergleichstest möglich ist, etwa nach Aggregation und Löschung der Ausgangsdaten.

Im Ganzen gilt: Ein Rückschluss ist unbeachtlich, wenn die gewonnene Information ihrerseits keinen Personenbezug aufweist. Dieser Grundsatz sollte in den Leitlinien deutlicher vorangestellt werden.

Für den Inference-Test sollten praktikable Nachweiswege aufgenommen werden, insbesondere die Anerkennung etablierter und dokumentierter Verfahren als Grundlage einer Regelvermutung für die Erfüllung des Kriteriums. Zugleich sollte klargestellt werden, dass die in den Leitlinien beschriebenen Angriffstechniken – insbesondere Membership Inference und Modellextraktion – am Maßstab der „means reasonably likely to be used“ zu bewerten sind und nicht automatisch zum Scheitern des Kriteriums „No Inference“ führen. Der in den Leitlinien vorgesehene Vergleich von Ergebnissen mit und ohne den Datensatz einer Person ist eine der wenigen praktikablen Konkretisierungen und ausdrücklich zu begrüßen.

6. Anonymisierung als Verarbeitungsvorgang ohne eigenen Zweck und ohne eigene Rechtsgrundlage

Nach den Leitlinien soll die Anonymisierung einer eigenen Rechtsgrundlage nach Art. 6 DSGVO und, bei besonderen Kategorien personenbezogener Daten, eines eigenen Ausnahmetatbestands nach Art. 9 Abs. 2 DSGVO bedürfen; Grundlage und Ausnahme sollen mit denen der vorangehenden Verarbeitung übereinstimmen, sofern die Anonymisierung Teil derselben Verarbeitungstätigkeit ist und der Verantwortliche mit ihr dieselben Zwecke verfolgt.

Dieser Ansatz überzeugt nicht. Anonymisierung wird in der Praxis nicht auf Daten angewandt, die zu einem einzigen Zweck auf einer einzigen Rechtsgrundlage erhoben wurden, sondern auf konsolidierte Datenbestände, die aus vielen Erhebungen stammen und mehreren Zwecken auf unterschiedlichen Grundlagen dienen. Beide Bedingungen der Leitlinien laufen damit regelmäßig leer, und die Leitlinien lassen offen, welche Folge dies haben soll.

Zweck und Rechtsgrundlage knüpfen an die Verarbeitungstätigkeit an, nicht an den einzelnen Verarbeitungsvorgang. Art. 4 Nr. 2 DSGVO definiert die Verarbeitung als jeden Vorgang oder jede Vorgangsreihe; die Prüfung der Erforderlichkeit nach Art. 6 Abs. 1 DSGVO lässt sich erst durchführen, wenn der verfolgte Zweck bestimmt ist. Bedürfte die Anonymisierung einer eigenen Rechtsgrundlage, so müsste dies gleichermaßen für Speicherung, Abruf, Übermittlung und Löschung gelten. Löschung und Verschlüsselung belegen dies: Beide sind Verarbeitung im Sinne von Art. 4 Nr. 2 DSGVO, beide werden an personenbezogenen Daten vorgenommen, und keine bedarf einer eigenen

Rechtsgrundlage; die Verschlüsselung ist in Art. 32 Abs. 1 lit. a DSGVO ausdrücklich als Sicherheitsmaßnahme vorgesehen. Art. 6 Abs. 4 lit. e DSGVO führt die Pseudonymisierung unter den Garantien und nicht unter den rechtfertigungsbedürftigen Vorgängen; der EDSA selbst bezeichnet die Pseudonymisierung als Sicherheits- und Datenschutzmaßnahme. Die Anonymisierung ist die stärkste Maßnahme dieser Familie und kann nicht die einzige sein, die einer Erlaubnis bedarf.

Andernfalls entsteht ein Wertungswiderspruch. Der Vorgang, der die Risiken für betroffene Personen am stärksten verringert, wäre am schwersten zu rechtfertigen, während die unveränderte Weiterverarbeitung identifizierbarer Daten keiner zusätzlichen Grundlage bedarf. Das widerspricht Art. 25 DSGVO. Die Leitlinien sind insoweit auch in sich widersprüchlich, da sie einerseits die Angabe verlangen, die Daten würden zur Erzeugung anonymer Informationen verarbeitet, und damit den Vorgang als Zweck behandeln, andererseits die Anonymisierung in die Interessenabwägung der vorangehenden Verarbeitung einstellen, was gerade voraussetzt, dass sie kein eigener Zweck ist.

Es sollte daher klargestellt werden, dass die Anonymisierung ein Verarbeitungsvorgang ist, der weder einen eigenen Zweck noch eine eigene Rechtsgrundlage trägt, sondern von der Verarbeitungstätigkeit erfasst wird, deren Teil er ist. Die Bedingung, dass der Verantwortliche „dieselben Zwecke“ verfolgen muss, sollte gestrichen werden. Ebenso ist klarzustellen, dass die Anonymisierung nicht als eigenständiger Verarbeitungszweck nach Art. 13 und 14 DSGVO auszuweisen ist.

Darüber hinaus sollten die Leitlinien ausdrücklich anerkennen, dass die Anonymisierung Verantwortlichen die Möglichkeit eröffnet, Daten für weitere Zwecke zu nutzen, etwa für statistische Auswertungen, Produktverbesserung oder Forschung. Da anonyme Informationen nach ErwG 26 S. 5 DSGVO nicht in den Anwendungsbereich der Verordnung fallen, unterliegt ihre weitere Nutzung weder dem Grundsatz der Zweckbindung nach Art. 5 Abs. 1 lit. b DSGVO noch der Vereinbarkeitsprüfung nach Art. 6 Abs. 4 DSGVO. Gerade darin liegt ein wesentlicher Anreiz, in wirksame Anonymisierungsverfahren zu investieren. Die Leitlinien sollten diesen Zusammenhang ausdrücklich benennen, statt die Anonymisierung vorrangig unter dem Gesichtspunkt von Pflichten und Risiken zu behandeln.

7. Schlussbemerkung

Mit dem Bekenntnis zum relativen Personenbezug haben die Leitlinien den richtigen Ausgangspunkt gewählt. Der EDSA sollte diesen Ansatz nun konsequent in operationalisierbare und überprüfbare Kriterien überführen. So können Verantwortliche und Aufsichtsbehörden die Identifizierbarkeit verlässlich beurteilen, während wirksamer Datenschutz und verantwortungsvolle Datennutzung zusammenwirken. Zugleich sollte der EDSA die Chance nutzen, Unternehmen bei datenschutzfreundlicher Anonymisierung mehr regulatorische Flexibilität einzuräumen. Wer in wirksame Anonymisierung investiert, sollte dafür Rechtssicherheit und Spielraum für die weitere Nutzung der Daten erhalten. Für den weiteren Austausch steht der BVDW gern zur Verfügung.



Bundesverband Digitale Wirtschaft (BVDW) e.V.

Der Bundesverband Digitale Wirtschaft (BVDW) e. V. ist die Interessenvertretung für Unternehmen, die digitale Geschäftsmodelle betreiben oder deren Wertschöpfung auf dem Einsatz digitaler Technologien beruht. Mit seinen Mitgliedern aus der gesamten Digitalen Wirtschaft gestaltet der BVDW bereits heute die Zukunft – durch kreative Lösungen und modernste Technologien. Als Impulsgeber, Wegweiser und Beschleuniger digitaler Geschäftsmodelle setzt der Verband auf faire und klare Regeln und tritt für innovationsfreundliche Rahmenbedingungen ein. Dabei hat der BVDW immer Wirtschaft, Gesellschaft und Umwelt im Blick. Neben der DMEXCO, der führenden Fachmesse für Digitales Marketing und Technologien, und dem Deutschen Digital Award richtet der BVDW auch den CDR-Award, die erste Preisverleihung im DACH-Raum für Digitale Nachhaltigkeit und Verantwortung sowie eine Vielzahl von Fachveranstaltungen aus.

Autor*in: Philipp Hagen, Director Legal Affairs & Data Privacy, hagen@bvdw.org

www.bvdw.org

Impressum

Erscheinungsort und -datum	Berlin, 29. Oktober 2026
Herausgeber	Bundesverband Digitale Wirtschaft (BVDW) e.V. Obentrautstraße 55, 10963 Berlin +49 30 2062186 – 0 info@bvdw.org www.bvdw.org
Vorstand gem. § 26 BGB	Carsten Rasner
Präsident	Dirk Freytag
Vizepräsident*innen	Thomas Duhr, Anke Herbener, Corinna Hohenleitner, Dr. Moritz Holzgraeffe, Björn Kaspring, Julian Simons
Kontakt	politik@bvdw.org
Vereinsregisternummer	Amtsgericht Charlottenburg VR 42449 B
Rechtshinweise	Alle in dieser Veröffentlichung enthaltenen Angaben und Informationen wurden vom Bundesverband Digitale Wirtschaft (BVDW) e.V. sorgfältig recherchiert und geprüft. Diese Informationen sind ein Service des Verbandes. Für Richtigkeit, Vollständigkeit und Aktualität können weder der Bundesverband Digitale Wirtschaft (BVDW) e.V. noch die an der Erstellung und Veröffentlichung dieses Werkes beteiligten Unternehmen die Haftung übernehmen. Die Inhalte dieser Veröffentlichung und / oder Verweise auf Inhalte Dritter sind urheberrechtlich geschützt. Jegliche Vervielfältigung von Informationen oder Daten, insbesondere die Verwendung von Texten, Textteilen, Bildmaterial oder sonstigen Inhalten, bedarf der vorherigen Zustimmung durch den Bundesverband Digitale Wirtschaft (BVDW) e.V. bzw. die Rechteinhaber (Dritte).