Der Bayerische Landesbeauftragte
für den Datenschutz

Identifizierbarkeit natürlicher Personen

Arbeitspapier

Der Bayerische Landesbeauftragte für den Datenschutz
80538 München | Wagmüllerstraße 18 | Telefon: +49 89 21 26 72-0
poststelle@datenschutz-bayern.de | https://www.datenschutz-bayern.de

Inhalt

Bearbeiter: Dr. Matthias Stief

Version 1.0 | Stand: 1. April 2026
überarbeitete und erweiterte Fassung der Aktuellen Kurz-Information 53
„Wann ist eine natürliche Person identifizierbar?“

Dieses Arbeitspapier wird ausschließlich in elektronischer Form bereitgestellt.
Es kann im Internet auf https://www.datenschutz-bayern.de in der Rubrik
„Infothek“ abgerufen werden.

Die PDF-Datei ist für den doppelseitigen Ausdruck optimiert.

Ohne die Verarbeitung personenbezogener Daten gibt es weder funktionsfähige öffentliche Verwaltungen noch erfolgreiche private Unternehmen. Soweit und solange verarbeitete Daten personenbezogen sind, müssen Datenverarbeiter allerdings datenschutzrechtliche Vorgaben beachten. Die Antwort auf die Frage, ob Daten einen Personenbezug aufweisen, ist daher von grundlegender Bedeutung. Vielfach wird das einfach zu beurteilen sein; in anderen Fällen jedoch bereitet die Weichenstellung in das Datenschutzrecht erhebliches Kopfzerbrechen. Schwierigkeiten ergeben sich insbesondere bei der Feststellung, ob eine Person im datenschutzrechtlichen Sinne „identifizierbar" ist. 1

Wann eine „Identifizierbarkeit" natürlicher Personen und in der Folge eine Verarbeitung personenbezogener Daten anzunehmen ist, hat auch den Europäischen Gerichtshof wiederholt beschäftigt. Anlässlich einer jüngeren Entscheidung des Gerichtshofs, des „SRB-Urteils",[1] möchte das vorliegende Papier den bayerischen öffentlichen Stellen die rechtlichen Hintergründe auf Basis der bisherigen unionsgerichtlichen Rechtsprechung zusammenfassend erläutern und einige Empfehlungen mit auf den Weg geben. 2

1. Rechtlicher Hintergrund

Nach Art. 4 Nr. 1 Halbsatz 1 Datenschutz-Grundverordnung (DSGVO) sind personenbezogene Daten „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person" (die sogenannte „betroffene Person") beziehen. Ein Personenbezug liegt also nicht erst dann vor, wenn sich die Identität einer betroffenen Person unmittelbar aus den verarbeiteten Daten ergibt, die Person mithin bereits identifiziert ist. Ausreichend ist vielmehr, dass die Daten die Identifizierung einer natürlichen Person „direkt oder indirekt" (vgl. Art. 4 Nr. 1 Halbsatz 2 DSGVO) ermöglichen. Eine solche Identifizierbarkeit setzt (mindestens) einen „Zwischenschritt" voraus, nämlich den Einsatz von (Identifizierungs-)Mitteln (insbesondere in Form von „Zusatzwissen"), mit deren Hilfe eine Beziehung zwischen dem Informationsgehalt der verarbeiteten Daten und einer Person – und damit ein Personenbezug – hergestellt werden kann.[2] 3

Damit stellt sich die Frage, auf wessen Mittel es ankommen soll, um die Identifizierbarkeit einer Person und damit einen Personenbezug im Sinne von Art. 4 Nr. 1 DSGVO annehmen zu können. Sind hier nur die Mittel des Verantwortlichen selbst oder auch – und gegebenenfalls in welchem Umfang – Erkenntnisse oder Erkenntnismöglichkeiten Dritter zu berücksichtigen? 4

Die praktische Bedeutung dieser Frage ist nicht zu unterschätzen: Relevant wird sie etwa in Fällen der Übermittlung pseudonymisierter Daten. Bei einer Pseudonymisierung werden 5

[1] Europäischer Gerichtshof, Urteil vom 4. September 2025, C-413/23 P.

[2] Vgl. Karg, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2. Auflage 2025, Art. 4 Nr. 1 DSGVO Rn. 57.

personenbezogene Daten so verarbeitet, dass eine Zuordnung dieser Daten zu einer natürlichen Person nur mittels gesondert aufbewahrter und gesicherter „zusätzlicher Informationen“ erfolgen kann. Für die übermittelnde Stelle, welche über diese Zusatzinformationen verfügt, bleiben diese Daten jedenfalls personenbezogen, vgl. Art. 4 Nr. 5 DSGVO. Doch wie ist der Personenbezug zu bewerten, wenn der Empfänger von pseudonymisierten Daten über diese Zusatzinformationen nicht verfügt und auch keine (legale) Möglichkeit hat, auf diese Informationen zuzugreifen?

2. „Relatives“ und „absolutes“ Verständnis des Personenbezugs

6 Die Diskussion zur Identifizierbarkeit natürlicher Personen und zum Personenbezug von Daten reicht in der (deutschen) Datenschutz-Fachwelt noch bis deutlich vor den Geltungsbeginn der Datenschutz-Grundverordnung zurück. Die Ergebnisse dieser Diskussion lassen sich wie folgt zusammenfassen: Nach einem sogenannten „relativen“ oder „subjektiven“ Verständnis des Personenbezugs sind allein die Mittel – insbesondere das „Zusatzwissen“ – des Verantwortlichen maßgebend. Für das „absolute“ oder „objektive“ Verständnis genügt demgegenüber, dass eine beliebige Stelle, nicht zwingend der Verantwortliche selbst, einen Personenbezug herstellen kann. Überspitzt gesagt, nimmt das absolute Verständnis das „Weltwissen“ in den Blick. Zwischen diesen Extrempositionen gruppieren sich zahlreiche vermittelnde, differenzierende oder anderweit kompromissorientierte Meinungen.[3]

3. Wie verhält sich die Datenschutz-Grundverordnung hierzu?

7 Die Legaldefinition in Art. 4 Nr. 1 DSGVO erhellt nicht, auf wessen Mittel es zur Identifizierbarkeit einer Person ankommen soll. Aussagen dazu bringt allerdings Erwägungsgrund (EG) 26 Satz 3 DSGVO: Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten danach „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 […]“. Offenbar sollen also nicht allein die Mittel des Verantwortlichen, die dieser zur Identifizierung einer Person nutzen kann, sondern auch entsprechende Mittel anderer Stellen in den Blick genommen werden. Dabei kommt es dem Wortlaut nach allein auf das „Nutzungspotential“ an; ob bestehende Identifizierungsmöglichkeiten vom Verantwortlichen oder von Dritten dann tatsächlich auch ausgeschöpft werden, soll wohl nicht entscheidend sein.[4]

8 Dieser im Ausgangspunkt weitreichende Ansatz wird zugleich dahin eingeschränkt, dass nur Mittel berücksichtigt werden sollen, die Verantwortliche oder andere Stellen nach allgemeinem Ermessen wahrscheinlich zu Identifizierungszwecken nutzen. Wann das der Fall ist, bestimmt sich nach EG 26 Satz 4 DSGVO anhand „objektiver Faktoren“. Daraus folgt, dass subjektive Absichtserklärungen von Verantwortlichen oder anderen Stellen, auf bestimmte

[3] Ausführlich hierzu Klar/Kühling, in: Kühling/Buchner, DS-GVO/BDSG, 4. Auflage 2024, Art. 4 Nr. 1 DSGVO Rn. 25 ff.; Karg, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2. Auflage 2025, Art. 4 Nr. 1 DSGVO Rn. 58 ff.

[4] Karg, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2. Auflage 2025, Art. 4 Nr. 1 DSGVO Rn. 62 f.

Identifizierungsmittel verzichten zu wollen, im Rahmen dieser Wahrscheinlichkeitsbeurteilung für sich genommen unerheblich sind.[5] Zu berücksichtigen sind hingegen stets „die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen" (EG 26 Satz 4 DSGVO am Ende). Dies trägt dem Umstand Rechnung, dass die fortschreitende technologische Entwicklung zunehmend mehr Möglichkeiten der (Re-)Identifizierung von Personen bietet. Demnach können sich auch vormals anonyme oder als anonymisiert angesehene Daten – Daten also, die vermeintlich keinen Personenbezug (mehr) aufweisen –, allein aufgrund technologischer Entwicklungen als noch oder wieder personenbezogen herausstellen.[6]

Zusammenfassend verdeutlicht EG 26 DSGVO, dass es bei der Frage der Identifizierbarkeit einer Person sowohl auf die Mittel des Verantwortlichen als auch anderer Stellen ankommen kann. Umgekehrt wird jedoch nicht auf ein gegebenenfalls nur rein theoretisch abrufbares „Weltwissen" abgestellt – verfügbare Mittel müssen vielmehr „nach allgemeinem Ermessen wahrscheinlich" eingesetzt werden. Dabei spielen auch zunehmend technologische Möglichkeiten zur (Re-)Identifizierung betroffener Personen eine Rolle; sie können dazu führen, dass eine vormalige Einstufung von Daten als „nicht personenbezogen" im Nachgang revidiert werden muss. 9

Übertragen auf deutsche Begrifflichkeiten vereint EG 26 DSGVO damit Elemente sowohl des absoluten als auch des relativen Personenbezugs. Auf diesem Weg bietet die Datenschutz-Grundverordnung bereits wertvolle Orientierung bei der Beurteilung, ob personenbezogene Daten vorliegen oder nicht. Die Ausführungen bleiben soweit noch abstrakt – insbesondere bedarf die Anforderung, dass lediglich hinreichend „wahrscheinlich" eingesetzte Mittel zu berücksichtigen sind, einer Konkretisierung. Abgesehen von gesetzlichen Ergänzungen oder Klarstellungen ist dies Aufgabe der Rechtsprechung – insbesondere des Europäischen Gerichtshofs –, jedoch auch der Datenschutz-Aufsichtsbehörden in den Mitgliedstaaten. 10

4. Die unionsgerichtliche Rechtsprechung zur Identifizierbarkeit einer natürlichen Person

Im Folgenden werden drei ausgewählte Entscheidungen des Europäischen Gerichtshofs vorgestellt, die sich (auch) mit der Frage der Identifizierbarkeit einer natürlichen Person und so mit den Anforderungen an den Personenbezug von Daten befasst haben. Ziel der Darstellung ist keine vertiefte wissenschaftliche Auseinandersetzung mit den einzelnen Urteilen, sondern das Herausarbeiten und eine Kurzbewertung ihrer wesentlichen Aussagen. Dabei ist stets im Blick zu behalten, dass der Europäische Gerichtshof dem Begriff der „personenbezogenen Daten" generell eine weite Bedeutung beimisst.[7] 11

[5] Für eine Berücksichtigung subjektiver Faktoren im Rahmen des objektiven Maßstabs nach EG 26 Satz 4 DSGVO Klar/Kühling, in: Kühling/Buchner, DS-GVO/BDSG, 4. Auflage 2024, Art. 4 Nr. 1 DSGVO Rn. 23.

[6] Vgl. Karg, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2. Auflage 2025, Art. 4 Nr. 1 DSGVO Rn. 64 f.

[7] Vgl. nur Europäischer Gerichtshof, Urteil vom 4. Mai 2023, C-478/21, Rn. 23.

a) Das Urteil des Europäischen Gerichtshofs zu dynamischen IP-Adressen

12 Als durchaus wegweisend kann das sogenannte „Breyer-Urteil" des Europäischen Gerichtshofs bezeichnet werden.[8] Diese Entscheidung ist zwar noch zur „alten" Datenschutzrichtlinie[9] ergangen; die insoweit maßgeblichen rechtlichen Vorgaben finden sich jedoch im Wesentlichen – mit geringfügigen sprachlichen Abweichungen[10] – auch in der Datenschutz-Grundverordnung wieder. Die Erwägungen des Gerichtshofs im „Breyer-Urteil" können daher auch unter Geltung der Datenschutz-Grundverordnung nutzbar gemacht werden (siehe hierzu näher Rn. 18 und Rn. 26).

13 Dem „Breyer-Urteil" lag unter anderem die Vorlagefrage zugrunde, ob – verkürzt gesagt – dynamische IP-Adressen, die ein Anbieter von Online-Mediendiensten von Besucherinnen und Besuchern der Internetpräsenz gespeichert hat, für diesen Anbieter personenbezogene Daten darstellen. Prämisse war dabei, dass zwar nicht der Anbieter selbst, aber ein Dritter (hier: der Internetzugangsanbieter) über das zur Identifizierung der betroffenen Person erforderliche Zusatzwissen verfügt.[11]

14 Der Gerichtshof hat diese Frage anhand der ihm vorliegenden Informationen im Ergebnis bejaht:[12] Für die Einstufung eines Datums als „personenbezogenes Datum" sei es nicht erforderlich, „dass sich alle zur Identifizierung der betreffenden Person erforderlichen Informationen in den Händen einer einzigen Person befinden."[13] Damit erteilte der Gerichtshof unter Bezugnahme auf EG 26 Satz 2 Richtlinie 95/46/EG jedenfalls dem streng relativen Verständnis des Personenbezugs im oben dargestellten Sinne eine Absage.

15 Zu berücksichtigen seien allerdings nur Mittel, die „vernünftigerweise zur Bestimmung der betroffenen Person eingesetzt werden" können. Letzteres sei nicht der Fall, wenn die Identifizierung der betroffenen Person gesetzlich verboten oder praktisch – etwa wegen eines unverhältnismäßigen Aufwands an Zeit und Kosten – nicht durchführbar sei, sodass „das Risiko einer Identifizierung de facto vernachlässigbar" erscheine.[14] Der Gerichtshof konkretisiert die „vernünftigerweise" oder – in der Formulierung der Datenschutz-Grundverordnung – „nach allgemeinem Ermessen wahrscheinlich" genutzten Mittel somit durch eine „Negativabgrenzung" – wobei im Einzelnen allerdings offen bleibt, wann die Schwelle zum „unverhältnismäßigen Aufwand" überschritten ist. Der Gerichtshof verlangt jedenfalls nicht, dass die Identifizierung einer Person in jedem Falle mit Sicherheit ausgeschlossen sein muss, sondern

8 Europäischer Gerichtshof, Urteil vom 19. Oktober 2016, C-582/14, BeckRS 2016, 82520.

9 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

10 So stellt etwa EG 26 Satz 2 der Richtlinie 95/46/EG im vorliegenden Zusammenhang auf Mittel ab, die „vernünftigerweise" eingesetzt werden können, während EG 26 Satz 3 DSGVO von Mitteln spricht, die „nach allgemeinem Ermessen wahrscheinlich genutzt werden." Die englischen Sprachfassungen sind an diesen Stellen „näher beieinander" und nennen einmal „all the means likely reasonably to be used" beziehungsweise „all the means reasonably likely to be used". Es ist daher davon auszugehen, dass der europäische Gesetzgeber sowohl in der Datenschutz-Richtlinie als auch in der Datenschutz-Grundverordnung insoweit das Gleiche gemeint hat.

11 Europäischer Gerichtshof, Urteil vom 19. Oktober 2016, C-582/14, BeckRS 2016, 82520, Rn. 37.

12 Europäischer Gerichtshof, Urteil vom 19. Oktober 2016, C-582/14, BeckRS 2016, 82520, Rn. 49.

13 Europäischer Gerichtshof, Urteil vom 19. Oktober 2016, C-582/14, BeckRS 2016, 82520, Rn. 43.

14 Europäischer Gerichtshof, Urteil vom 19. Oktober 2016, C-582/14, BeckRS 2016, 82520, Rn. 45 f.

akzeptiert ein gegebenenfalls verbleibendes Identifizierungs(rest-)risiko, sofern dieses „de facto vernachlässigbar" ist.

Mit Blick auf die Vorlagefrage stellt der Gerichtshof im Weiteren auf Mittel ab, die dem Anbieter von Online-Mediendiensten zur Verfügung stehen. Vernünftigerweise einsetzbar seien dabei „rechtliche Mittel", die es diesem erlauben, gegebenenfalls mittels eines „Umwegs" über die zuständige Behörde die betroffene Person bestimmen zu lassen.[15] 16

b) Der Europäische Gerichtshof und die Fahrzeug-Identifizierungsnummer

Eine deutlich jüngere Entscheidung des Europäischen Gerichtshofs (das „FIN-Urteil")[16] betrifft zwar im Schwerpunkt keine ausgesprochen datenschutzrechtliche Streitsache, behandelt gleichwohl aber die Frage, ob Fahrzeughersteller im Sinne von Art. 6 Abs. 1 UAbs. 1 Buchst. c DSGVO verpflichtet sind, sogenannten „unabhängigen Wirtschaftsakteuren" (wie etwa unabhängigen Werkstätten oder Ersatzteilhändlerinnen und Ersatzteilhändlern) die Fahrzeugidentifizierungsnummern (FIN) der produzierten Fahrzeuge bereitzustellen. Die Anwendbarkeit von Art. 6 Abs. 1 UAbs. 1 Buchst. c DSGVO – und der Datenschutz-Grundverordnung insgesamt – hängt hier davon ab, ob es sich bei der FIN um eine Information über eine identifizierbare natürliche Person und damit um ein personenbezogenes Datum im Sinne von Art. 4 Nr. 1 DSGVO handelt. 17

Unter Bezugnahme auf sein „Breyer-Urteil" macht der Gerichtshof eingangs darauf aufmerksam, dass zur Beantwortung dieser Frage alle Mittel berücksichtigt werden sollten, die vernünftigerweise entweder von dem Verantwortlichen oder von einem Dritten eingesetzt werden könnten, um die betroffene Person zu bestimmen. Dabei sei es nicht erforderlich, dass sich alle zur Identifizierung dieser Person notwendigen Informationen in den Händen einer einzigen Einrichtung befinden.[17] Damit wiederholt der Gerichtshof Kernaussagen des „Breyer-Urteils" – erstaunlicherweise aber, ohne EG 26 Satz 3 und 4 DSGVO zu erwähnen. Der Gerichtshof sieht die Grundsätze aus dem „Breyer-Urteil" also auch unter der Datenschutz-Grundverordnung weiter als maßgebend an. 18

Da die FIN unmittelbar nur die Identifizierung eines Fahrzeugs ermöglicht, stellt sie nach Ansicht des Gerichtshofs „als solche" zwar kein personenbezogenes Datum dar. Verfügt eine Stelle allerdings „bei vernünftiger Betrachtung" über Mittel, die es ihr ermöglichen, „Daten wie die FIN" einer bestimmten Person zuzuordnen, werden diese Daten zu personenbezogenen Daten.[18] Noch deutlicher als im „Breyer-Urteil" lässt der Gerichthof damit ein relatives Grundverständnis des Personenbezugs erkennen: Ein „eigentlich" nicht personenbezogenes Datum kann in bestimmten Verwendungszusammenhängen zu einem personenbezogenen Datum werden. 19

15 Europäischer Gerichtshof, Urteil vom 19. Oktober 2016, C-582/14, BeckRS 2016, 82520, Rn. 47 ff.
16 Europäischer Gerichtshof, Urteil vom 9. November 2023, C-319/22.
17 Europäischer Gerichtshof, Urteil vom 9. November 2023, C-319/22, Rn. 45.
18 Europäischer Gerichtshof, Urteil vom 9. November 2023, C-319/22, Rn. 46.

20 Als „Zuordnungsmittel“ kam im vorliegenden Fall insbesondere die Zulassungsbescheinigung in Betracht, die neben der FIN auch Namen und Anschrift des Inhabers enthält.[19] Ob die FIN danach ein personenbezogenes Datum darstellt, hat der Gerichtshof nicht abschließend entschieden, sondern dem vorlegenden Gericht zur Prüfung überlassen. Sollte die FIN für die unabhängigen Wirtschaftsakteure nach den oben genannten Kriterien ein personenbezogenes Datum sein, gilt dies nach Auffassung des Gerichtshofs allerdings „mittelbar“ auch für die Fahrzeughersteller, welche die FIN bereitstellen.[20] Der Gerichtshof stellt bei der Beurteilung des Personenbezugs von (in diesem Fall durch Bereitstellung) offengelegten Daten damit maßgeblich auf den „Empfängerhorizont“ ab.

c) Das „SRB-Urteil“ des Europäischen Gerichtshofs

21 Vertiefend führt der Europäische Gerichtshof zum Begriff der personenbezogenen Daten schließlich in seinem „SRB-Urteil“ aus.[21] Dieses Urteil erging anlässlich eines Rechtsmittels des Europäischen Datenschutzbeauftragten (EDSB), der mit Unterstützung des Europäischen Datenschutzausschusses (EDSA) die Aufhebung einer Entscheidung des Gerichts der Europäischen Union beantragt hatte. Diese Entscheidung hatte bereits in Fachkreisen für Aufsehen gesorgt:[22] Vordergründig ging es bei ihr zwar „nur“ um die Frage, ob der Verantwortliche seine datenschutzrechtlichen Informationspflichten hinreichend erfüllt hatte. Inhaltlich befasste sich der Gerichtshof im Schwerpunkt allerdings mit der Identifizierbarkeit natürlicher Personen und dem Personenbezug im Zusammenhang mit pseudonymisierten Daten. Maßgebend war im konkreten Fall zwar nicht die Datenschutz-Grundverordnung, sondern die Verordnung (EU) 2018/1725. Dieses Gesetz enthält datenschutzrechtliche Vorgaben für Verarbeitungen durch Stellen der Europäischen Union.[23] Was den Begriff der „personenbezogenen Daten“ angeht, sind die einschlägigen Bestimmungen in beiden Verordnungen jedoch inhaltlich deckungsgleich.[24]

22 Der im Einzelnen durchaus komplexe Sachverhalt lässt sich vereinfacht wie folgt zusammenfassen: Eine Stelle, hier der „Einheitliche Abwicklungsausschuss“ (Single Resolution Board, SRB)[25], erhob im Rahmen eines Anhörungsverfahrens Stellungnahmen natürlicher Personen. Die eingegangenen Stellungnahmen wurden mit einem alphanumerischen Code versehen, sodass die personenbezogenen Inhalte der Stellungnahmen[26] von den Identitätsdaten

19 Europäischer Gerichtshof, Urteil vom 9. November 2023, C-319/22, Rn. 47 f.

20 Europäischer Gerichtshof, Urteil vom 9. November 2023, C-319/22, Rn. 49.

21 Europäischer Gerichtshof, Urteil vom 4. September 2025, C-413/23 P.

22 Gericht der Europäischen Union, Urteil vom 26. April 2023, T-557/20 = ZD 2023, 399 mit Anmerkung Baumgartner.

23 Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG.

24 Vgl. nur die mit Art. 4 Nr. 1 DSGVO identische Begriffsbestimmung in Art. 3 Nr. 1 Verordnung (EU) 2018/1725; nach dem Europäischen Gerichtshof, Urteil vom 4. September 2025, C-413/23 P, Rn. 52, ist damit sicherzustellen, dass diese Vorschriften „gleich ausgelegt werden“.

25 Zu dieser Stelle näher https://www.srb.europa.eu/en/about.

26 Der Europäische Gerichtshof hat in diesem Zusammenhang klargestellt, dass persönliche Meinungen oder Sichtweisen „als Ausdruck der Gedanken einer Person zwangsläufig eng mit dieser Person verknüpft“ und

der einreichenden Personen getrennt waren. Die Identitätsdaten der Beteiligten hielt der SRB in einer eigenen Datenbank vor, zu der nur einige seiner Beschäftigten Zugang hatten. Ein Teil der so „codierten" Stellungnahmen wurde im Anschluss an ein externes Beratungsunternehmen zur Bewertung übermittelt. Der SRB konnte anhand des verwendeten Codes und der vorgehaltenen Identitätsdaten die einzelnen Stellungnahmen bestimmten Personen zuordnen. Das Beratungsunternehmen hatte dagegen keinen Zugang zu der Datenbank mit den Identitätsdaten der Beteiligten.[27] Im Nachgang hierzu wandten sich mehrere betroffene Personen mit dem Vorbringen an den EDSB, sie seien vom SRB nicht ordnungsgemäß darüber informiert worden, dass die von ihnen abgegebenen Stellungnahmen an das Beratungsunternehmen übermittelt würden. Diese Beschwerden rügten damit einen Verstoß gegen die datenschutzrechtliche Pflicht des Verantwortlichen, betroffene Personen bei Datenerhebungen über die Empfänger ihrer personenbezogenen Daten zu informieren.[28]

23 Nach Auffassung des EDSB – des Beklagten im Ausgangsverfahren vor dem Gericht der Europäischen Union – hatte der SRB pseudonymisierte (vgl. bereits Rn. 5) und damit personenbezogene Daten an das Beratungsunternehmen übermittelt; schließlich sei aufgrund der noch vorhandenen Identitätsdaten eine (Re-)Identifizierung der betroffenen Personen „hinter" den codierten Stellungnahmen weiterhin möglich.[29] Der SRB war demgegenüber der Ansicht, die übermittelten Daten seien für das Beratungsunternehmen anonymisiert worden; er habe weder die für eine (Re-)Identifizierung notwendigen Zusatzinformationen mit dem Beratungsunternehmen geteilt noch habe dieses ein entsprechendes Zugangsrecht.[30] Das Gericht der Europäischen Union gab der Klage des SRB im Ergebnis statt und erklärte die angefochtene Entscheidung des EDSB für nichtig.

24 Der Auffassung, wonach pseudonymisierte Daten in jedem Fall personenbezogen sind, ohne dass es einer konkreten Prüfung bedarf, ob die Person „hinter" diesen Daten identifizierbar ist, tritt der Europäische Gerichtshof in seiner Rechtsmittelentscheidung entgegen:[31] Insoweit führt er zunächst aus, dass sich die Legaldefinition der „personenbezogenen Daten" nach Art. 3 Nr. 1 Verordnung (EU) 2018/1725 (entspricht Art. 4 Nr. 1 DSGVO, vgl. bereits Rn. 3 ff.) nicht zu pseudonymisierten Daten verhalte; für letztere sei vielmehr die Begriffsbestimmung nach Art. 3 Nr. 6 Verordnung (EU) 2018/1725 (entspricht Art. 4 Nr. 5 DSGVO) maßgebend. Die Pseudonymisierung sei demnach (nur, aber immerhin) eine technische und organisatorische Maßnahme, die das (Re-)Identifizierungsrisiko für betroffene Personen verringern solle.[32] Da eine Pseudonymisierung von Daten schon ihrer Definition nach aber das Vorhandensein von (gesondert aufzubewahrenden und zu sichernden) Identifizierungsinformationen voraussetze, könnten pseudonymisierte Daten zwar nicht in jedem Fall als anonymisierte

damit personenbezogen sind, vgl. Europäischer Gerichtshof, Urteil vom 4. September 2025, C-413/23 P, Rn. 58 ff.

27 Vgl. im Einzelnen Europäischer Gerichtshof, Urteil vom 4. September 2025, C-413/23 P, Rn. 9 ff., insbesondere Rn. 16 ff. und Rn. 22ff.

28 Vgl. Art. 15 Abs. 1 Buchst. d Verordnung (EU) 2018/1725, der inhaltlich Art. 13 Abs. 1 Buchst. e DSGVO entspricht.

29 Vgl. Gericht der Europäischen Union, Urteil vom 26. April 2023, T-557/20, Rn. 32, 79 ff.

30 Gericht der Europäischen Union, Urteil vom 26. April 2023, T-557/20, Rn. 76 ff.

31 Vgl. zum Folgenden Europäischer Gerichtshof, Urteil vom 4. September 2025, C-413/23 P, Rn. 68 ff.

32 Europäischer Gerichtshof, Urteil vom 4. September 2025, C-413/23 P, Rn. 70 ff.

Daten betrachtet werden; eine Pseudonymisierung könne sich aber gleichwohl im Einzelfall auf die Personenbezogenheit von Daten auswirken.[33]

25 Diese abstrakten Feststellungen veranschaulicht der Gerichtshof sodann am konkreten Fall, indem er die unterschiedlichen Perspektiven der beteiligten Datenverarbeiter einnimmt: Da der SRB die Pseudonymisierung der Stellungnahmen selbst durchgeführt hat und weiterhin über Zusatzinformationen verfügt, die eine Re-Identifizierung der betroffenen Personen ermöglichen, sind die Stellungnahmen auch in ihrer „codierten" Form für den SRB selbst weiterhin personenbezogen.[34] Ob die pseudonymisierten Stellungnahmen auch für den Empfänger personenbezogen sind, hängt wiederum davon ab, ob dieser die zuvor durchgeführte Pseudonymisierung – untechnisch gesagt – „auflösen", die betroffenen Personen mithin (re)identifizieren kann.

26 Damit ist der Gerichtshof erneut bei der Frage angelangt, welche (Re-)Identifizierungsmittel insoweit zu berücksichtigen sind. Unter Bezugnahme auf EG 16 Verordnung (EU) 2018/1725 (der im Wesentlichen EG 26 DSGVO entspricht, vgl. bereits Rn. 7 ff.) und seine bisherige Rechtsprechung – einschließlich des „Breyer-Urteils" (vgl. bereits Rn. 12 ff.) und des „FIN-Urteils" (vgl. bereits Rn. 17 ff.) – führt der Gerichtshof dabei die etablierten Maßstäbe fort:[35] Einzubeziehen sind demnach Mittel des Empfängers sowie anderer Personen mit der Maßgabe, dass die Mittel „nach allgemeinem Ermessen wahrscheinlich" genutzt werden, um die natürlichen Personen hinter den Stellungnahmen zu identifizieren. Ein „Restrisiko" für eine Identifizierung hindert die Annahme fehlenden Personenbezugs nicht, sofern dieses Risiko „de facto" unbedeutend erscheint, weil die Identifizierung gesetzlich verboten oder (etwa wegen unverhältnismäßigen Aufwands) praktisch nicht durchführbar ist (vgl. zu Einzelheiten hierzu die bisherigen Ausführungen). Für die Übermittlung pseudonymisierter Daten bedeutet dies in den Worten des Gerichtshofs:

> „Folglich müssen […] pseudonymisierte Daten […] nicht in jedem Fall und für jede Person als personenbezogene Daten betrachtet werden. Denn die Pseudonymisierung kann – je nach den Umständen des Einzelfalls – andere Personen als den Verantwortlichen tatsächlich an einer Identifizierung der betroffenen Person hindern, so dass letztere für sie nicht oder nicht mehr identifizierbar ist."[36]

27 Stärker noch als seine vorhergehenden Entscheidungen verdeutlicht das „SRB-Urteil" damit das „personen- und kontextrelative"[37] Verständnis des Gerichtshofs vom Personenbezug: Je nach Verarbeitungssituation und datenverarbeitender Stelle kann ein Personenbezug im Hinblick auf bestimmte Daten gegebenenfalls das eine Mal vorliegen, das andere Mal fehlen. Der Gerichtshof unterstreicht dieses relative Verständnis an späterer Stelle des „SRB-Urteils" mit der Bemerkung, dass sich „die maßgebliche Sicht für die Beurteilung der Identifizierbarkeit

[33] Europäischer Gerichtshof, Urteil vom 4. September 2025, C-413/23 P, Rn. 73 ff.
[34] Europäischer Gerichtshof, Urteil vom 4. September 2025, C-413/23 P, Rn. 76.
[35] Vgl. zum Folgenden ausführlich Europäischer Gerichtshof, Urteil vom 4. September 2025, C-413/23 P, Rn. 77 ff.
[36] Europäischer Gerichtshof, Urteil vom 4. September 2025, C-413/23 P, Rn. 86.
[37] So Baumgartner, ZD 2025, 638 (639).

der betroffenen Person wesentlich nach den Umständen der Datenverarbeitung im Einzelfall“ richtet.[38]

28 Gegen ein dergestalt relatives Verständnis hatten sowohl der EDSB als auch der EDSA im Vorfeld Bedenken vorgebracht: Schließlich ermögliche dieses einem Verantwortlichen, eigentlich personenbezogene Daten dem Anwendungsbereich des Unionsrechts zu entziehen.[39] Konkret am Fall veranschaulicht: Nähme man an, dass die an das Beratungsunternehmen übermittelten Stellungnahmen für dieses nicht (mehr) personenbezogenen sind, so könnte das Beratungsunternehmen die pseudonymisierten Stellungnahmen – ohne an das unionale Datenschutzrecht „gebunden“ zu sein – beliebig an weitere Dritte (die sich gegebenenfalls sogar in einem Drittland befinden) übermitteln. Diese Dritten hätten dann aber unter Umständen hinreichende Mittel, um die betroffenen Personen doch noch (re-)identifizieren zu können.

29 Der Gerichtshof selbst sieht auf Grundlage seines relativen Verständnisses eine solche Schutzlücke gleichwohl nicht: Übermittelt nämlich eine Stelle Daten, die aus ihrer Sicht nicht personenbezogen sind, an einen Dritten, bei dem nicht ausgeschlossen werden kann, dass er über Identifizierungsmittel nach den dargestellten Maßgaben verfügt, dann gelten diese Daten „sowohl in Bezug auf die Übermittlung […] als auch in Bezug auf die spätere Verarbeitung […] durch Dritte“ als personenbezogen.[40] Der Personenbezug von Daten kann dergestalt also wieder „aufleben“, und zwar nicht nur für den Dritten, der die Daten empfängt, sondern mittelbar bzw. indirekt auch für den Übermittler;[41] Letzterer müsste die Datenweitergabe in einem solchen Fall dann auf eine hinreichende datenschutzrechtliche Rechtsgrundlage stützen können. Die vom Übermittler hiernach vorzunehmende Beurteilung, ob ein Datenempfänger über Identifizierungsmöglichkeiten im obigen Sinne verfügt oder nicht, dürfte sich in der Praxis im Einzelfall allerdings als durchaus herausfordernd gestalten.

30 Der SRB konnte sich damit in seiner Auffassung zum Personenbezug pseudonymisierter Daten durch den Europäischen Gerichtshof zwar im Wesentlichen bestätigt sehen. Zugleich hielt dessen spezifisch relatives Verständnis des Personenbezugs für den SRB aber noch eine „bittere Pille“ bereit:[42] Denn in dem zugrunde liegenden Rechtsstreit ging es ja, wie eingangs erwähnt (Rn. 21), im Wesentlichen um die Frage, ob der SRB die betroffenen Personen über die Weitergabe der (pseudonymisierten) Stellungnahmen an das Beratungsunternehmen als „Empfänger“ hätte informieren müssen (Art. 15 Abs. 1 Buchst. d Verordnung [EU] 2018/1725, der Art. 13 Abs. 1 Buchst. e DSGVO entspricht). Diese Informationspflicht knüpft zeitlich jedoch nicht an die (spätere) Weitergabe von Daten an, sondern entsteht bereits zu dem Zeitpunkt, in welchem ein Verantwortlicher personenbezogene Daten bei der betroffenen Person erhebt. Sie betrifft mit anderen Worten (allein) das „Rechtsverhältnis zwischen der betroffenen Person und dem Verantwortlichen“.[43] Da die erhobenen Daten aus Sicht des SRB zum Erhebungszeitpunkt (und auch noch später, vgl. bereits Rn. 25) personenbezogen

38 Europäischer Gerichtshof, Urteil vom 4. September 2025, C-413/23 P, Rn. 100.

39 Vgl. Europäischer Gerichtshof, Urteil vom 4. September 2025, C-413/23 P, Rn. 64.

40 Europäischer Gerichtshof, Urteil vom 4. September 2025, C-413/23 P, Rn. 85.

41 Europäischer Gerichtshof, Urteil vom 4. September 2025, C-413/23 P, Rn. 84 unter Bezugnahme auf das FIN-Urteil.

42 Vgl. zum Folgenden Europäischer Gerichtshof, Urteil vom 4. September 2025, C-413/23 P, Rn. 110 ff.

43 Europäischer Gerichtshof, Urteil vom 4. September 2025, C-413/23 P, Rn. 110.

sind, hätte der SRB betroffene Personen bereits zu diesem Zeitpunkt auch über mögliche Empfänger der erhobenen personenbezogenen Daten informieren müssen – und zwar unabhängig davon, ob die späteren Empfänger tatsächlich in der Lage sind, die betroffenen Personen zu identifizieren.[44]

4. Was folgt daraus für bayerische öffentliche Stellen?

31 Die dargestellten Entscheidungen zeigen, dass die Frage, ob und inwieweit sich Daten auf eine identifizierbare Person beziehen, vielfach eine Einzelfallbetrachtung erfordert. Deutlich zu kurz gegriffen wäre es dabei, wenn eine öffentliche Stelle nur ihre eigenen Identifizierungsmöglichkeiten in den Blick nehmen würde. Nicht nur, aber gerade bei der Offenlegung von Daten können die Mittel Dritter dazu führen, dass ein Personenbezug von Daten erst hergestellt wird. Aus EG 26 Satz 4 DSGVO ergibt sich ferner, dass der Begriff der „personenbezogenen Daten" nicht statisch ist. Technologische Entwicklungen können dazu führen, dass Daten, bei denen ein Personenbezug zunächst verneint worden ist, einen solchen mit fortschreitender Entwicklung dann doch erhalten.

32 Umgekehrt hat der Europäische Gerichtshof aufgezeigt, dass Daten für eine datenverarbeitende Stelle personenbezogen, für eine andere hingegen nicht (mehr) personenbezogen sein können. Eine Pseudonymisierung personenbezogener Daten kann damit im Hinblick auf bestimmte Verarbeitungssituationen gegebenenfalls auch „anonymisierende Wirkung" entfalten. Sich hieran anschließende Fragestellungen, etwa zur Auswirkung einer solchen Konstellation auf Auftragsverarbeitungsverhältnisse nach Art. 28 DSGVO, hat der Gerichtshof bislang noch nicht entschieden.[45] Nicht gänzlich geklärt erscheint ferner, welche Bedeutung dem „Empfängerhorizont" bei der Offenlegung von Daten im Einzelnen zukommt.

33 Bayerische öffentliche Stellen sind daher unverändert gut beraten, die Rechtsprechung aufmerksam zu verfolgen; es empfiehlt sich, zu diesem Zweck den Newsletter „Privacy in Bavaria" per RSS-Feed oder Mastodon-Account zu beziehen.[46]

34 Die bisherige Darstellung zeigt (hoffentlich) auch: Ob Daten einen Personenbezug aufweisen, ist nicht immer einfach zu beantworten und bedarf gegebenenfalls einer durchaus komplexen Einzelfallbetrachtung. In Zweifelsfällen sollten bayerische öffentliche Stellen einen Personenbezug annehmen und – gegebenenfalls „überobligatorisch" – datenschutzrechtliche Vorgaben beachten.

[44] Europäischer Gerichtshof, Urteil vom 4. September 2025, C-413/23 P, Rn. 112 f.

[45] Vgl. zu dem SRB-Urteil des Europäischen Gerichtshofs nur die Anmerkungen von Golland, NJW 2025, 3423, Roßnagel, ZD 2025, 637 und Baumgartner, ZD 2025, 638.

[46] Internet: https://www.datenschutz-bayern.de/static/rss-main.html und https://www.datenschutz-bayern.de/mastodon.

5. Fazit

Die Frage, welche Mittel für die Identifizierbarkeit natürlicher Personen zu berücksichtigen sind, ist für den Begriff der „personenbezogenen Daten“ und damit für die Anwendbarkeit des Datenschutzrechts von erheblicher Bedeutung. Sowohl die Datenschutz-Grundverordnung als auch die Rechtsprechung des Europäischen Gerichtshofs verweisen darauf, dass es hier nicht nur auf die Mittel des Verantwortlichen, sondern auch auf Mittel Dritter ankommen kann. Solche Mittel werden dem Verantwortlichen nicht schrankenlos zugerechnet; begrenzend wirkt insbesondere die Prüfung, ob der Einsatz eines Mittels zur Identifizierung natürlicher Personen hinreichend wahrscheinlich oder vernünftigerweise zu erwarten ist. In Fällen der Datenoffenlegung scheint die jüngere unionsgerichtliche Rechtsprechung dabei auch den Mitteln des Datenempfängers maßgebende Bedeutung beizumessen. Aus dem kontext- und stellenrelativen Verständnis des Europäischen Gerichtshofs folgt ferner, dass ein und dieselben Daten unter bestimmten Umständen für eine Stelle personenbezogen, für andere Stellen hingegen nicht mehr personenbezogen sein können. 35

Klar ist aber: Der Gerichtshof wird auch künftig (mehr als eine) Gelegenheit haben, sich zum Begriff der „personenbezogenen Daten“ und zur Identifizierbarkeit einer natürlichen Person zu äußern. 36