Der Bayerische Landesbeauftragte
für den Datenschutz

Wann ist eine natürliche Person identifizierbar?

Aktuelle Kurz-Information 53

Stichwörter: Datum, Personenbezug – Identifizierbarkeit, personenbezogenes Datum – Personenbezogenes Datum, Identifizierbarkeit – Personenbezug, Datum | **Stand:** 19. Januar 2024

Was sind die Kernaussagen dieser Aktuellen Kurz-Information?

- Personenbezogene Daten liegen nicht erst dann vor, wenn sie sich auf eine identifizierte Person beziehen. Ausreichend ist, wenn natürliche Personen direkt oder indirekt „identifizierbar" sind.
- Bei der Frage, ob eine Person identifizierbar ist, kommt es sowohl nach der Datenschutz-Grundverordnung als auch nach dem Europäischen Gerichtshof nicht nur auf Mittel des Verantwortlichen, sondern auch auf Mittel Dritter an.
- Mittel, die eine Identifizierung ermöglichen, werden aber nur so weit berücksichtigt, wie deren Nutzung hinreichend wahrscheinlich oder vernünftigerweise zu erwarten ist.
- Auch nach einer jüngeren Entscheidung des Europäischen Gerichtshofs sind noch nicht alle Fragen zur „Identifizierbarkeit" einer natürlichen Person geklärt.

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 Sinn „identifizierbar" ist. 1

Wann eine „Identifizierbarkeit" natürlicher Personen und in der Folge eine Verarbeitung personenbezogener Daten anzunehmen ist, hat jüngst auch den Europäischen Gerichtshof (abermals) beschäftigt.[1] Aus diesem Anlass möchte die vorliegende Aktuelle Kurz-Information den bayerischen öffentlichen Stellen die rechtlichen Hintergründe auf Basis der bisherigen unionsgerichtlichen Rechtsprechung zusammenfassend erläutern und einige Empfehlungen mit auf den Weg zu 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 3

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

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]

4 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?

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

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 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] 8

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 Entscheidungen der Unionsgerichte vorgestellt, die sich (auch) mit der Frage der Identifizierbarkeit einer natürlichen Person und so mit den Anforderungen an den Personenbezug von Daten befasst haben. Zwei dieser Entscheidungen stammen vom Europäischen Gerichtshof, eine vom Gericht der Europäischen Union.[7] 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 11

Blick zu behalten, dass der Europäische Gerichtshof dem Begriff der „personenbezogenen Daten“ generell eine weite Bedeutung beimisst.[8]

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

12 Als durchaus wegweisend kann das sogenannte „Breyer-Urteil“ des Europäischen Gerichtshofs bezeichnet werden.[9] Diese Entscheidung ist zwar noch zur „alten“ Datenschutzrichtlinie[10] ergangen; die insoweit maßgeblichen rechtlichen Vorgaben finden sich jedoch im Wesentlichen – mit geringfügigen sprachlichen Abweichungen[11] – auch in der Datenschutz-Grundverordnung. Die Erwägungen des Gerichtshofs im Breyer-Urteil können daher auch unter Geltung der Datenschutz-Grundverordnung nutzbar gemacht werden (siehe hierzu näher Rn. 24).

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.[12]

14 Der Gerichtshof hat diese Frage anhand der ihm vorliegenden Informationen im Ergebnis bejaht:[13] 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.“[14] 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 Sinn 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 wäre, sodass „das Risiko einer Identifizierung de facto vernachlässigbar“ erscheine.[15] 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 akzeptiert ein gegebenenfalls verbleibendes Identifizierungs(rest-)risiko, sofern dieses „de facto vernachlässigbar“ ist.

16 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.[16]

b) Das Europäische Gericht und die Übermittlung pseudonymisierter Daten

17 Regelmäßig steht die Rechtsprechung des Europäischen Gerichtshofs im Fokus der datenschutzfachlichen Aufmerksamkeit. In jüngerer Zeit hat jedoch auch eine Entscheidung des Gerichts der Europäischen Union, die sich mit Fragen der Identifizierbarkeit natürlicher Personen und dem Personenbezug von Daten befasste, in Fachkreisen für Aufsehen gesorgt.[17] Im konkreten Fall war zwar nicht die Datenschutz-Grundverordnung maßgebend, sondern die Verordnung (EU) 2018/1725. Dieses Gesetz enthält datenschutzrechtliche Vorgaben für Verarbeitungen durch Stellen der Europäischen Union.[18] Was den Begriff der „personenbezogenen Daten" angeht, sind die einschlägigen Bestimmungen in diesen Verordnungen jedoch inhaltlich deckungsgleich;[19] das Urteil des Gerichts ist daher auch in der Welt der Datenschutz-Grundverordnung von Bedeutung.

18 Der im Einzelnen durchaus komplexe Sachverhalt lässt sich vereinfacht wie folgt zusammenfassen: Eine Stelle, hier der „Einheitliche Abwicklungsausschuss", erhob im Rahmen eines Anhörungsverfahrens Stellungnahmen natürlicher Personen. Die eingegangenen Stellungnahmen wurden mit einem alphanumerischen Code versehen, sodass die Inhalte der Stellungnahmen von den persönlichen Daten der einreichenden Personen getrennt waren. Die Identitätsdaten der Beteiligten hielt der Einheitliche Abwicklungsausschuss 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 Einheitliche Abwicklungsausschuss 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.[20]

19 Nach Auffassung des Europäischen Datenschutzbeauftragten – des Beklagten in diesem Verfahren – hat der Einheitliche Abwicklungsausschuss pseudonymisierte 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.[21] Der Einheitliche Abwicklungsausschuss war demgegenüber der Ansicht, die übermittelten Daten seien für das Beratungsunternehmen anonymisiert worden; er habe weder die für eine Reidentifizierung notwendigen Zusatzinformationen mit dem Beratungsunternehmen geteilt, noch habe dieses ein entsprechendes Zugangsrecht.[22]

20 Das Gericht nimmt in seiner Entscheidung zunächst ausführlich Bezug auf das oben dargestellte Breyer-Urteil des Europäischen Gerichtshofs.[23] Auf dieser Grundlage vergleicht es sodann die Situation des Beratungsunternehmens mit derjenigen des Anbieters von Online-Mediendiensten im Breyer-Urteil: Für die Bewertung, ob es sich bei den übermittelten Informationen um personenbezogene Daten handle, sei darauf abzustellen, ob sich diese Informationen nach dem Verständnis des Beratungsunternehmens auf „identifizierbare Personen" bezogen hätten.[24] Demgegenüber habe sich die Prüfung des Europäischen Datenschutzbeauftragten auf die Perspektive des Einheitlichen Abwicklungsausschusses und damit (nur) des Datenübermittlers beschränkt.[25]

21 Bemerkenswert ist dieses Urteil unter anderem[26] deshalb, weil es bei der Frage, ob die Übermittlung pseudonymisierter Daten datenschutzrechtlich relevant ist, dem „Empfängerhorizont" entscheidende Bedeutung beimisst. Damit eröffnet das Gericht Raum für eine im Einzelfall mögliche „anonymisierende Wirkung" einer Pseudonymisierung: Eine solche Pseudonymisierung ändert zwar für den Verantwortlichen, der die für eine (Re-)Identifizierung der betroffenen Personen erforderlichen Zusatzinformationen vorhält, grundsätzlich nichts am Personenbezug (vgl. Art. 4 Nr. 15 DSGVO). Folgt man der Auffassung des Gerichts, kann eine Übermittlung von pseudonymisierten Daten unter Umständen gleichwohl zu einer auf die konkrete Übermittlung beschränkten Aufhebung des Personenbezugs dieser Daten führen, nämlich dann, wenn der Empfänger über keine vernünftigerweise einsetzbaren Identifizierungsmöglichkeiten verfügt. Ob Letzteres im konkreten Fall tatsächlich zutraf, hat das Gericht nicht entschieden, sondern die insoweit unterbliebene Prüfung der Aufsichtsbehörde moniert.[27]

22 Das Urteil des Gerichts ist noch nicht rechtskräftig;[28] eine Entscheidung des Europäischen Gerichtshofs in dieser Sache bleibt abzuwarten.

c) Der Europäische Gerichtshof und die Fahrzeug-Identifizierungsnummer

23 Etwas mehr als ein halbes Jahr nach der Entscheidung des Gerichts hatte nun der Europäische Gerichtshof in einem anderen Verfahren Anlass, sich zum Personenbezug von Daten und der Identifizierbarkeit natürlicher Personen zu äußern. Seine neueste Entscheidung[29] 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.

24 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.[30] Damit wiederholt der Gerichtshof Kernaussagen des Breyer-Urteils – erstaunlicherweise 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.

25 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.[31] 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.

26 Als „Zuordnungsmittel“ kam im vorliegenden Fall insbesondere die Zulassungsbescheinigung in Betracht, die neben der FIN auch Namen und Anschrift des Inhabers enthält.[32] Ob die FIN danach ein personenbezogenes Datum darstellt, hat der Gerichtshof nicht abschließend entschieden, sondern der Prüfung durch das vorlegende Gericht 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.[33] Ähnlich wie das Gericht der Europäischen Union in dem unter Rn. 17 ff. behandelten Urteil stellt der Gerichtshof bei der Beurteilung des Personenbezugs von (in diesem Fall durch Bereitstellung) offengelegten Daten auf den „Empfängerhorizont“ ab – dies freilich unter „geänderten Vorzeichen“: Während das Gericht den Personenbezug der übermittelten Daten mit der unter Rn. 21 dargelegten Argumentation hinterfragte, zieht der Gerichtshof diese gerade heran, um einen Personenbezug einzelfallabhängig begründen zu können.

4. Was folgt daraus für bayerische öffentliche Stellen?

27 Die Entscheidungen zeigen, dass die Frage der Identifizierbarkeit natürlicher Personen und damit des Personenzugs von Daten zwar in ihren Grundzügen, nicht jedoch in allen Einzelheiten geklärt ist. Dies betrifft insbesondere den Umfang, in welchem Wissen und Möglichkeiten Dritter bei der Beurteilung des Personenbezugs zu berücksichtigen sind, sowie die Bedeutung, die dem „Empfängerhorizont“ bei der Offenlegung von Daten insoweit zukommt. Weitere Konkretisierungen durch die unionsgerichtliche Rechtsprechung sind zu erwarten.

28 Bayerische öffentliche Stellen sind daher 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.[34]

29 Deutlich geworden ist aus den bisherigen Entscheidungen bereits: Ob und inwieweit sich Daten auf eine identifizierbare Person beziehen, erfordert in der Regel eine Einzelfallbetrachtung. 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.

30 In Zweifelsfällen sollten bayerische öffentliche Stellen einen Personenbezug annehmen und – gegebenenfalls „überobligatorisch“ – datenschutzrechtliche Vorgaben beachten.

5. Fazit

31 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 den Mitteln des Datenempfängers maßgebende Bedeutung beizumessen.

32 Klar ist aber auch: Das letzte Wort ist zu diesen Fragen noch nicht gesprochen.

1 Europäischer Gerichtshof, Urteil vom 9. November 2023, C-319/22.
2 Vgl. Karg, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 4 Nr. 1 DSGVO Rn. 57.
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, 2019, Art. 4 Nr. 1 DSGVO Rn. 58 ff.
4 Karg, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 4 Nr. 1 DSGVO Rn. 62.
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, 2019, Art. 4 Nr. 1 DSGVO Rn. 63.
7 Art. 19 Abs. 1 Satz 1 Vertrag über die Europäische Union (EUV) fasst unter der Dachbezeichnung „Gerichtshof der Europäischen Union“ den Europäischen Gerichtshof, das Gericht der Europäischen Union sowie Fachgerichte zusammen. Das Gericht der Europäischen Union entscheidet in erster Instanz über bestimmte Klagen gegen Maßnahmen der Union, vgl. Art. 256 EUV.
8 Vgl. nur Europäischer Gerichtshof, Urteil vom 4. Mai 2023, C-478/21, Rn. 23.
9 Europäischer Gerichtshof, Urteil vom 19. Oktober 2016, C-582/14, BeckRS 2016, 82520.
10 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.
11 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.
12 Europäischer Gerichtshof, Urteil vom 19. Oktober 2016, C-582/14, BeckRS 2016, 82520, Rn. 37.
13 Europäischer Gerichtshof, Urteil vom 19. Oktober 2016, C-582/14, BeckRS 2016, 82520, Rn. 49.
14 Europäischer Gerichtshof, Urteil vom 19. Oktober 2016, C-582/14, BeckRS 2016, 82520, Rn. 43.
15 Europäischer Gerichtshof, Urteil vom 19. Oktober 2016, C-582/14, BeckRS 2016, 82520, Rn. 45 f.
16 Europäischer Gerichtshof, Urteil vom 19. Oktober 2016, C-582/14, BeckRS 2016, 82520, Rn. 47 ff.
17 Gericht der Europäischen Union, Urteil vom 26. April 2023, T-557/20 = ZD 2023, 399 mit Anmerkung Baumgartner.
18 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.

[19] Vgl. nur die mit Art. 4 Nr. 1 DSGVO identische Begriffsbestimmung in Art. 3 Nr. 1 Verordnung (EU) 2018/1725.
[20] Vgl. im Einzelnen Gericht der Europäischen Union, Urteil vom 26. April 2023, T-557/20, Rn. 2 ff., insbesondere Rn. 14 ff. und Rn. 24.
[21] Vgl. Gericht der Europäischen Union, Urteil vom 26. April 2023, T-557/20, Rn. 32, 79 ff.
[22] Gericht der Europäischen Union, Urteil vom 26. April 2023, T-557/20, Rn. 76 ff.
[23] Gericht der Europäischen Union, Urteil vom 26. April 2023, T-557/20, Rn. 88 ff.
[24] Gericht der Europäischen Union, Urteil vom 26. April 2023, T-557/20, Rn. 97.
[25] Gericht der Europäischen Union, Urteil vom 26. April 2023, T-557/20, Rn. 103.
[26] Die weiteren Ausführungen des Gerichts beschäftigen sich im Schwerpunkt mit der Frage, ob die Stellungnahmen überhaupt Informationen enthielten, die sich inhaltlich auf natürliche Personen beziehen, vgl. Gericht der Europäischen Union, Urteil vom 26. April 2023, T-557/20, Rn. 64 ff.
[27] Gericht der Europäischen Union, Urteil vom 26. April 2023, T-557/20, Rn. 104 f.
[28] Vgl. Rechtsmittel des Europäischen Datenschutzbeauftragten, ABl. C Nr. 296 vom 21. August 2023, S. 26.
[29] Europäischer Gerichtshof, Urteil vom 9. November 2023, C-319/22.
[30] Europäischer Gerichtshof, Urteil vom 9. November 2023, C-319/22, Rn. 45.
[31] Europäischer Gerichtshof, Urteil vom 9. November 2023, C-319/22, Rn. 46.
[32] Europäischer Gerichtshof, Urteil vom 9. November 2023, C-319/22, Rn. 47 f.
[33] Europäischer Gerichtshof, Urteil vom 9. November 2023, C-319/22, Rn. 49.
[34] Internet: https://www.datenschutz-bayern.de/static/rss-main.html und https://www.datenschutz-bayern.de/mastodon.