Alexander Roßnagel

Anonymisierung personenbezogener Daten und Nutzung anonymer Daten

Eine Schlüsselfrage der künftigen Digitalisierung

Je weiter Wirtschaft und Verwaltung digitalisiert werden, desto mehr Daten benötigen sie. Insbesondere soweit sie lernfähige Systeme einsetzen, erfordert dies sehr viele Daten, mit denen diese trainiert, getestet und evaluiert werden. Sind die Daten personenbezogen, erzeugt ihre Verwendung für diese Zwecke datenschutzrechtliche Probleme. Diese Probleme könnten durch Anonymisierung dieser Daten und die Nutzung anonymer Daten vermieden werden. Der Beitrag untersucht, unter welchen Voraussetzungen und mit welchen Rechtsfolgen die Zuschreibung von Anonymität rechtlich möglich ist.

1 Schlüsselelement der Digitalisierung

Datennutzung ist die Grundlage der künftigen Digitalisierung aller Gesellschaftsbereiche. Zu einem großen Teil sind die Daten, die genutzt werden sollen, jedoch personenbezogen. Sie fallen dann unter das Datenschutzrecht. Soweit sie für andere Zwecke erstellt oder erhoben worden sind, dürfte ihre weitere Verwendung im Regelfall dem Gebot der Zweckbindung nach Art. 5 Abs. 1 Buchst. b DSGVO und oft auch dem Grundsatz der Datenminimierung nach Art. 5 Abs. 1 Buchst. c DSGVO widersprechen. Daten können jedoch ohne Begrenzung und für neue Zwecke genutzt werden, wenn sie keinen Personenbezug haben – wenn sie also anonym sind.

Anonymisieren bedeutet, personenbezogene Daten so zu verändern, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.[1] Anonyme Daten können von Anfang an ohne Personenbezug sein, sie können aber auch das Ergebnis der Anonymisierung sein. Sie sind das Gegenteil von personenbezogenen Daten.[2] Sie grenzen sich definitorisch von diesen dadurch ab, dass ihnen der Personenbezug fehlt.[3] Anonymisierung und Personenbezug korrelieren insofern negativ.[4] Entscheidend ist, dass die Daten zwar Angaben enthalten, die für eine bestimmte Person zutreffen können, dass mit ihnen aber kein Bezug zu einer identifizierten oder identifizierbaren natürlichen Person hergestellt werden kann. Anonymisiert sind Daten also nur dann, wenn ihre Verarbeitung das Ergebnis hat, dass zu ihnen kein Personenbezug mehr hergestellt werden kann.

Hinsichtlich der Rechtsfolge anonymisierter Daten verweisen ErwG 26 Satz 5 und 6 DSGVO darauf, dass „personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann", nicht von der DSGVO erfasst werden. Daher kann jeder Verantwortliche anonymisierte oder von Anfang an anonyme Daten für seine Zwecke – auch zum Training von KI – weiterverarbeiten.

Die Anonymisierung von personenbezogenen Daten ist eine Verarbeitung nach Art. 4 Nr. 2 DSGVO.[5] Sie dürfte überwiegend nach Art. 6 Abs. 1 UAbs. 1 Buchst. f DSGVO zulässig sein, weil durch die Anonymisierung schutzwürdige Rechte der betroffenen Person selten oder in geringem Maß berührt sein dürften.[6] Sieht ein nationales Gesetz im öffentlichen Interesse eine Ano-

1 Ebenso z. B. die Definitionen in § 3 BbgDSG, § 2 Abs. 4 BremDSG, § 11 Abs. 2 HmbDSG, § 2 Abs. 4 HDSIG, § 4 DSG NRW; § 24 Nr. 18 NDSG, § 3 Abs. 2 Satz 2 Nr. 4 Sächs. DSG, § 2 Abs. 7 DSG LSA; § 13 Abs. 2 DSG SH, § 28 Abs. 3 ThürDSG. Die DSGVO kennt keine Definition von Anonymität oder Anonymisierung. Im Unionsrecht gibt es nur eine Definition des Begriffs „Anonymisieren" in Art. 2 Nr. 7 RL über offene Daten 2019/1024 vom 20.6.2019, s. auch ErwG 52 dieser RL. Der Begriff ist in dieser Richtlinie nur für die Kostenregelung für das Anonymisieren von elektronischen Dokumenten relevant.

2 S. z. B. *Klar/Kühling*, in: Kühling/Buchner, DSGVO/BDSG, 4. Aufl. 2024, Art. 4 Rn. 32; *Roßnagel*, ZD 2021, 188 (189).

3 S. ErwG 52 RL über offene Daten 2019/1024 vom 20.6.2019; *Hofmann/Johannes*, ZD 2017, 221 (223).

4 *Roßnagel/Scholz*, MMR 2000, 721 (723).

5 S. *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 4 Nr. 2 Rn. 12, 14, 32; *Hornung/Wagner*, ZD 2020, 223; *Roßnagel*, ZD 2021, 188 (189).

6 S. z. B. *Hornung/Wagner*, ZD 2020, 223; *Roßnagel*, ZD 2021, 188 (189).

Prof. Dr. Alexander Roßnagel

ist Hessischer Beauftragter für Datenschutz und Informationsfreiheit (HBDI).

E-Mail: a.rossnagel@uni-kassel.de

nymisierung vor, ist sie nach diesem gemäß Art. 6 Abs. 3 i.V.m. Art. 6 Abs. 1 Buchst. c oder e DSGVO zulässig.[7]

Anonymisierung könnte daher ein Schlüsselinstrument für die rechtlich zulässige umfassende Nutzung von ehemals personenbezogenen Daten und daher für eine Lösung des Konflikts zwischen Datennutzung und Datenschutz sein.[8]

Ist aber eine Verarbeitung personenbezogener Daten in der Weise möglich, dass die Wiederherstellung des Personenbezugs ausgeschlossen ist? Gegenüber dieser Möglichkeit werden zunehmend Zweifel geäußert. Wegen der enormen Zunahme personenbezogener Daten und des technischen Fortschritts in der Verknüpfung von Daten und der Zuordnung zu einzelnen Personen erscheint es immer schwieriger zu werden, Verfahren der Anonymisierung zu finden, die eine Wiederherstellung des Personenbezugs ausschließen. Aus technikwissenschaftlicher Sicht muss man wohl zu dem Ergebnis kommen, dass ein vollständiger Ausschluss der (Re-)Identifizierung nicht möglich ist.

Entspricht dieses Ergebnis aber einer rechtlichen Sichtweise, bei der es nicht um absolute Feststellungen geht, sondern um die Regelung des menschlichen Zusammenlebens auf Grundlage von Risikoabwägungen? Ihr entspricht es eher zu fragen, wie stark die Möglichkeit der Wiederherstellung des Personenbezugs ausgeschlossen sein muss, um von einer Anonymität der durch Anonymisierungsverfahren veränderten Daten ausgehen zu können. Die Sätze 5 und 6 des ErwG 26 DSGVO gehen jedenfalls davon aus, dass es anonyme und anonymisierte Daten gibt, die nicht mehr der DSGVO unterfallen.

2 Rechtliches Verständnis von Anonymität

Ausgangspunkt für das rechtliche Verständnis von Anonymität müssen die Sätze 3 und 4 des ErwG 26 DSGVO sein. Diese beschreiben die rechtlichen Anforderungen an die Identifizierbarkeit einer natürlichen Person.

2.1 Wahrscheinlichkeitsbewertung

Satz 3 bestimmt: „Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten 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, wie beispielsweise das Aussondern." Aus dieser Beschreibung geht als erstes hervor, dass die Identifizierbarkeit einer Person als Handlungsmöglichkeit des Verantwortlichen oder einer anderen Person keine Eigenschaft des jeweiligen Datums ist, sondern eine Frage des möglichen Mitteleinsatzes. Es geht also um das mobilisierbare Wissen des Verantwortlichen oder einer anderen Person, um eine Verbindung zwischen Datum und betroffener Person herzustellen. Bezogen auf diese Wissensbeziehung geht es zweitens um die Wahrscheinlichkeit der Identifizierung, nicht um ihren völligen Ausschluss. Es geht also um die Feststellung der Grundrechtsrisiken für die betroffene Person. Dabei soll das Risiko konkret und nicht nur abstrakt bestimmt werden. Denn es geht um die Mittel, die „genutzt werden" – nicht um die, die „genutzt werden können". Für die Bestimmung dieses Risikos sollen zwar „alle" Mittel berücksichtigt werden, aber nur dann, wenn sie nach „allgemeinem Ermessen" wahrscheinlich genutzt werden. Bei der Wahrscheinlichkeitsbewertung geht es also nicht nur um die Sicht spezialisierter Technik, sondern um eine auf die konkrete Situation bezogene allgemeine Lebenserfahrung. Gefordert ist daher eine pragmatische Bewertung. Für diese Wahrscheinlichkeitsbewertung nennt die DSGVO kein Wahrscheinlichkeitsmaß, sie geht aber von einem Risikorest aus, der für einen Ausschluss des Datenschutzrechts akzeptabel ist.[9] Wie hoch dieser sein darf, überlässt sie der Praxis. Die Inanspruchnahme eines „Ermessens" deutet auf eine notwendige Abwägung hin – zwischen der Bewertung des Schadenspotentials bei der betroffenen Person und dem Grundrechtseingriff beim Verantwortlichen.

2.2 Risikofaktoren

Was bei der Feststellung des Risikos zu berücksichtigen ist, erläutert Satz 4: „Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind." Nach Satz 4 verstärkt sich der Schluss, dass eine pragmatische, objektive Bestimmung der Wahrscheinlichkeit der (Re-)Identifizierung getroffen werden muss. Zu berücksichtigen sind alle objektiven Faktoren. Diese hängen von der jeweils konkreten Situation und den in ihr bestehenden Umständen ab. Wer welchen Zeitaufwand erbringen muss, hängt von der Person des Verantwortlichen oder der anderen Person ab, die zu berücksichtigen ist, sowie vom Zusatzwissen, den Fähigkeiten und den mobilisierbaren Hilfsmitteln. Zu berücksichtigen sind auch die für sie verfügbaren Technologien. Dies gilt nicht nur für den Zeitpunkt der Datenverarbeitung, sondern auch für die nach allgemeinem Ermessen absehbar verfügbaren technologischen Entwicklungen. Allerdings muss die jeweilige Technologie für die praktische Anwendung durch den Verantwortlichen verfügbar sein.[10] Die Berücksichtigung des Zeitaspekts muss auch für sonstige objektive Faktoren gelten, die für die Einschätzung der Wahrscheinlichkeit einer Identifizierung relevant sind. Die Wahrscheinlichkeitsbewertung soll alle objektiven Faktoren berücksichtigen, nicht aber subjektive Faktoren, wie die (fehlende) Motivation des Verantwortlichen oder der anderen Person. Als ein objektives Kriterium müsste aber die festgelegte Aufgabe eines Verantwortlichen angesehen werden, wie die von Nachrichtendiensten oder Strafverfolgungsbehörden.

2.3 Identifizierungsmöglichkeiten Dritter

Nach ErwG 26 Satz 3 DSGVO sind für die Risikoprognose alle Mittel zu berücksichtigen, die „*von dem Verantwortlichen oder einer anderen Person*" genutzt werden, um die natürliche Person zu identifizieren. Umstritten ist, wer diese „andere Person" sein

7 S. z. B. Art. 89 Abs. 1 Satz 4 DSGVO, §§ 6 und 8 GDNG, §§ 25a, 64e, 287 SGB V, § 12a eGovG.

8 *Roßnagel/Geminn*, ZD 2021, 487.

9 S. hierzu z. B. auch EuGH vom 19.10.2016, C-582/14, Rn. 46 – Breyer; DSK, Risiko für die Rechte und Freiheiten natürlicher Personen, Kurzpapier 18, S. 2; *Kühling/Klar*, ZD 2017, 27 (28); *Roßnagel/Geminn*, ZD 2021, 487 (488); *Lukas*, ZD 2023, 321 (324); *Burghoff*, ZD 2023, 658 (660); *Baumgartner*, ZD 2023, 402 (403); *Stummer*, DuD 2024, 368 (371); *Schulz*, in: Gola/Heckmann, Art. 6 DSGVO, Rn. 153.

10 S. z. B. *Hofmann/Johannes*, ZD 2017, 2021 (225).

kann, ob sie in einer Beziehung zum Verantwortlichen stehen muss oder ob es jede andere beliebige Person sein kann.[11] Wann es auf die eine und wann auf die andere Sichtweise ankommt, wird weiter unten erörtert.[12]

2.4 Anonymität als rechtliche Bewertung

Als Schlussfolgerung aus der Auswertung des ErwG 26 DSGVO ist festzuhalten, dass Anonymität keine feststehende Eigenschaft des Datums ist, sondern eine Zuschreibung aufgrund der Bewertung des Risikos der (Re-)Identifizierung der betroffenen natürlichen Person als vernachlässigbar. Dieses Risiko kann sich je nach Verantwortlichem, je nach Zeitpunkt und ja nach Umständen verändern. Für die Bestimmung der Anonymität sind daher die konkreten Umstände der Beteiligten, also ihr sozialer Kontext entscheidend. Für die Risikobewertung sind *alle* objektiven Faktoren zu berücksichtigen – sowohl die risikoverstärkenden als auch die risikomindernden.

3 Rechtsprechung des EuGH

Für das rechtliche Verständnis von Anonymität sind auch die inzwischen ergangenen Entscheidungen des EuGH auszuwerten, aus denen eine Linie des Gerichtshof abgeleitet werden kann, wie er Anonymisierung und die Nutzung anonymer Daten versteht.

3.1 Breyer

In seinem Breyer-Urteil aus dem Jahr 2016 prüft der EuGH, ob das Wissen Dritter einzubeziehen ist, aus Sicht des Verantwortlichen. Als Anbieter von Internetdiensten verarbeitet er IP-Adressen von Nutzern. Er kann eine IP-Adresse nicht selbst der Identität eines Nutzers zuordnen, wohl aber der Internetzugangsanbieter. Für die Frage, ob die IP-Adressen für den verantwortlichen Dienstanbieter personenbezogen sind, ist nach EuGH „*zu prüfen …, ob die Möglichkeit, eine dynamische IP-Adresse mit den Zusatzinformationen zu verknüpfen, über die der Internetzugangsanbieter verfügt, ein Mittel darstellt, das vernünftigerweise[13] zur Bestimmung der betreffenden Person eingesetzt werden kann*".[14] Dieses Wissen des Dritten könnte jedoch nicht einbezogen werden, „*wenn die Identifizierung der betreffenden Person gesetzlich verboten oder praktisch nicht durchführbar wäre, z. B. weil sie einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften erfordern würde, so dass das Risiko einer Identifizierung de facto vernachlässigbar erschiene*".[15] Die IP-Adresse ist für den EuGH also nur dann kein anonymes, sondern ein personenbezogenes Datum, „*wenn er* (der Verantwortliche) über rechtliche Mittel verfügt, die es ihm erlauben, die betreffende Person anhand der Zusatzinformationen, über die der Internetzugangsanbieter dieser Person (also der Dritte) *verfügt, bestimmen zu lassen*".[16] Der EuGH prüft die Frage der Personenbeziehbarkeit konsequent nur aus dem Blickwinkel des Verantwortlichen.[17] Nur wenn er auf das Zusatzwissen des Dritten rechtmäßig zugreifen kann, ist dessen Wissen ein Mittel, das er zur Identifizierung nutzen kann. Die (Re-)Identifizierungsmöglichkeiten weiterer Stellen – hier der Internetzugangsanbieter – bleiben für die Frage der Anonymität der Daten unberücksichtigt.[18]

3.2 Gesamtverband Autoteile-Handel

In seinem Urteil zum Gesamtverband Autoteile-Handel aus dem Jahr 2023 ging es um den Personenbezug der Fahrzeugidentifikationsnummer (FIN), über die unabhängige Wirtschaftsakteure wie z. B. Reparaturwerkstätten auf der Website eines Kraftfahrzeugherstellers nach Daten zu einem bestimmten Kraftfahrzeug suchen konnten. Auch in diesem Urteil stellte der EuGH für die Feststellung des Personenbezugs auf den Verantwortlichen ab. Die FIN wird nur „*für denjenigen, der bei vernünftiger Betrachtung über Mittel verfügt, die es ermöglichen, sie einer bestimmten Person zuzuordnen, zu personenbezogenen Daten*".[19] Entscheidend ist, ob „*derjenige, der Zugang zur FIN hat, über Mittel verfügen könnte, die es ihm ermöglichen, die FIN zur Identifizierung des Halters … zu nutzen*".[20] Wenn ein Fahrzeughersteller Kraftfahrzeugdaten zur FIN eines bestimmten Kraftfahrzeugs etwa Reparaturbetrieben zur Verfügung stellt, ist zu prüfen, ob die Empfänger „*bei vernünftiger Betrachtung über Mittel verfügen können, die es ermöglichen, die FIN einer identifizierten oder identifizierbaren natürlichen Person zuzuordnen*" – etwa über die Zulassungsbescheinigung. In diesem Fall stelle sie für die Empfänger „*ein personenbezogenes Datum dar, selbst wenn die FIN für sich genommen für die Fahrzeughersteller kein persönliches Datum darstellt, insbesondere dann nicht, wenn das Fahrzeug, dem sie zugewiesen wurde, nicht einer natürlichen Person gehört*".[21] Nach diesem Urteil kann also ein Datum je nach Verantwortlichem seinen Charakter als anonymes oder als personenbeziehbares Datum verändern. Entscheidend sind die Mittel des jeweils Verantwortlichen, nicht die irgendwelcher Dritter. Überträgt ein Verantwortlicher Daten an einen Empfänger, überträgt er personenbezogene Daten, wenn der Empfänger sie der betroffenen Person zuordnen kann, selbst wenn ihm dies nicht möglich wäre.[22] Für die Feststellung der Anonymität oder Personenbeziehbarkeit ist nicht das Datum, vielmehr sind die Umstände des Einzelfalls entscheidend. Zu berücksichtigen ist, wer Zugriff auf die Daten hat, wer über welche Mittel (hier Zulassungsbescheinigung) verfügen kann und wie schwer eine Identifizierung einer natürlichen Person ist (hier abhängig von der Haltereigenschaft).

11 S. ausführlich hierzu Karg, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 4 Nr. 1 Rn. 57 ff.; *Roßnagel/Geminn*, in Dierks/Roßnagel, Sekundärnutzung von Sozial- und Gesundheitsdaten, 2019, S. 143 ff.

12 S. Kap. 3 und 5.

13 ErwG 26 Satz 2 DSRL, um den es hier geht, und ErwG 26 Satz 3 DSGVO sind weitgehend identisch. „Vernünftigerweise" in ErwG 26 Satz 2 DSRL wurde in ErwG 26 Satz 3 DSGVO durch „nach allgemeinem Ermessen" ersetzt.

14 EuGH vom 19.10.2016, C-582/14, Rn. 45 – Breyer mAnm *Kühling/Klar*, ZD 2017, 27; *Moos/Rothkegel*, MMR 2016, 845 und *Mantz/Spittka*, NJW 2016, 3582; ebenso EuG vom 26.4.2023, T-557/20, Rn. 104f. mAnm *Baumgartner*, ZD 2023, 402; *Hofmann/Johannes*, ZD 2017, 2021 (223).

15 EuGH vom 19.10.2016, C-582/14, Rn. 46 – Breyer; bestätigt durch EuGH vom 7.3.2024, C-479/22 P, Rn. 51 – OLAF.

16 EuGH vom 19.10.2016, C-582/14, Rn. 49 – Breyer; bestätigt durch EUGH vom 7.3.2024, C-604/22, Rn. 48, 51 – IAB Europe.

17 S. auch ebenso EuG vom 26.4.2023, T-557/20, Rn. 97; *Mantz/Spittka*, NJW 2016, 3582; *Baumgartner*, ZD 2023, 402 (403).

18 Ebenso *Kühling/Klar*, ZD 2017, 27 (28); *Hanloser*, ZD 2024, 175f.

19 EuGH vom 9.11.2023, C-319/22, Rn. 46, 48 – Gesamtverband Autoteile-Handel; s. auch Anm. von *Hanloser*, ZD 2024, 175.

20 EuGH vom 9.11.2023, C-319/22, Rn. 48 – Gesamtverband Autoteile-Handel.

21 EuGH vom 9.11.2023, C-319/22, Rn. 49 – Gesamtverband Autoteile-Handel; s. kritisch *Hanloser*, ZD 2024, 175 (176).

22 S. auch *Hanloser*, ZD 2024, 175 (175f.)

3.3 OLAF

In seinem Urteil vom 7. März 2024 zu einer Pressemitteilung des Europäischen Amtes für Betrugsbekämpfung (OLAF) hatte der EuGH festzustellen, wann der Öffentlichkeit bekanntgegebene Daten personenbeziehbar sind. „*Dass ein Investigativjournalist die Identität einer von einer Pressemitteilung betroffenen Person verbreitet hat, … lässt für sich genommen noch nicht den Schluss zu, dass die in dieser Mitteilung enthaltenen Informationen zwingend als personenbezogene Daten … zu qualifizieren sind*“.[23] Ob die Verantwortlichen für die Pressemitteilung mit diesem Risiko rechnen mussten, wäre näher zu prüfen. Eine Pressemitteilung über die Untersuchung eines Forschungsprojekts, die an die Öffentlichkeit gerichtet ist, ist aber auch an Personen gerichtet, die auf demselben wissenschaftlichen Gebiet arbeiten wie die betroffene Person und ihren beruflichen Werdegang kennen. Sie sind Empfänger der Presseerklärung und können aus Daten wie die Informationen über das Projekt, die fördernde und die durchführende Institution und weitere Details die betroffene Person „ohne einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft“ identifizieren.[24] Daher war das „*Risiko der Identifizierung … nicht als unbedeutend*“ anzusehen.[25] Auch bei einer Offenlegung von Daten gegenüber der Öffentlichkeit ist das Risiko der Identifizierung zu prüfen und auf seine Beachtlichkeit hin zu bewerten. Aufgrund der breiten Öffentlichkeit, an die die Mitteilung gerichtet war, sind die Mittel zur Identifizierung durch alle potenziellen Empfänger (eine Vielzahl von Empfängern) zu berücksichtigen.

3.4 IAB-Europe

Schließlich ist noch das Urteil der EuGH im Fall von IAB-Europe, ebenfalls vom 7. März 2024, zu berücksichtigen. In diesem Fall ging es um die massenhafte automatisierte Versteigerung von Nutzerprofilen für den Verkauf von Werbeplätzen auf Websites oder in Apps (Real Time Bidding). Ob der Nutzer in diese Datenverarbeitung eingewilligt hat, wird in einem individuellen „TC-String“, einer Kombination aus Buchstaben und Zeichen, gespeichert. Dieser TC-String lässt nicht von sich aus auf den jeweiligen Internetnutzer schließen. Er ermöglicht aber den Anbietern von Webseiten oder Apps sowie Datenbrokern und Werbeplattformen durch Kombination mit anderen Daten wie der IP-Adresse des verwendeten Endgeräts auf die betroffene Person zu schließen. Der EuGH entschied, dass dieser TC-String für den Verband IAB-Europe ein personenbezogenes Datum darstellt, auch wenn er weder Zugang zu den Daten hat, die von seinen Mitgliedern verarbeitet werden, noch diesen String mit anderen Elementen kombinieren kann, wenn er einen Rechtsanspruch gegenüber seinen Mitgliedern hat, ihm „*auf Anfrage alle Informationen zu übermitteln, die es ihm ermöglichen, die Nutzer zu identifizieren, deren Daten Gegenstand eines TC Strings sind*“.[26] Als Schlussfolgerung aus diesem Urteil kann festgehalten werden, dass auch hier die Feststellung des Personenbezugs auf den Verantwortlichen bezogen ist. Das Gericht nimmt einen Personenbezug der umstrittenen Daten nicht deshalb an, weil andere Personen, hier die Anbieter von Webseiten oder Apps sowie Datenbroker und Werbeplattformen, die Identität der betroffenen Personen feststellen können. Vielmehr ist für den Personenbezug entscheidend, dass der Verantwortliche das Wissen der anderen Personen mobilisieren kann. Entscheidend ist, dass er einen Rechtsanspruch gegenüber der anderen Person hat, ihm ihr Wissen zugänglich zu machen.[27]

3.5 Erkenntnisse der EuGH-Rechtsprechung

Der EuGH geht immer vom Verantwortlichen aus und fragt, ob die von ihm verarbeiteten Daten für ihn personenbezogen sind. Andere Personen, deren Wissen der Verantwortliche nicht nutzen kann, spielen für diese Bewertung keine Rolle, auch wenn sie die betroffenen Personen identifizieren können. Dass der EuGH an der Datenverarbeitung und an dem für sie Verantwortlichen ansetzt, entspricht seiner Entscheidungssituation. Aber auch Datenschutzaufsichtsbehörden müssen für eine konkrete Datenverarbeitung eines bestimmten Verantwortlichen entscheiden, ob die relevanten Daten personenbezogen oder anonym sind. Dies entspricht auch ErwG 26 DSGVO. Hätte der Verordnungsgeber alle Personen berücksichtigen wollen, hätte er nicht den „Verantwortlichen oder eine andere Person“ anführen müssen, sondern formuliert: Mittel, die von „jeder Person genutzt“ werden, oder schlicht: „Mittel, die genutzt werden können“. Auch Satz 6 des ErwG 26 DSGVO bezieht sich auf den Verantwortlichen, indem er die Rechtsfolge der Anonymisierung anspricht. Denn die DSGVO betrifft danach „*nicht die Verarbeitung solcher anonymer Daten*“. Die Verarbeitung führt nur der Verantwortliche durch.

Andere Personen spielen nur dann eine Rolle, wenn sie in irgendeiner Beziehung zum Verantwortlichen stehen. Dies kann in zweifacher Weise der Fall sein. Zum einen kann es sein, dass der Verantwortliche ihr Wissen, ihre Fähigkeiten oder ihre Mittel für sich nutzen kann – entweder de facto oder de jure. Zum anderen können andere Personen eine Rolle spielen, wenn der Verantwortliche ihnen Daten offenlegt. Dann stellt sich die Frage, ob es sich um die Offenlegung personenbezogener Daten handelt. Dies ist der Fall, wenn der Empfänger nach allgemeinem Ermessen die Personen, auf die sich die Daten beziehen, identifizieren kann. Der Verantwortliche legt somit personenbezogene Daten offen, wenn sie für den Empfänger personenbezogen sind, auch wenn sie für ihn anonym sind.

In jedem Fall bestimmt der EuGH den Personenbezug oder die Anonymität nicht abstrakt am Maßstab einer Theorie,[28] sondern, wie ErwG 26 DSGVO dies erfordert, nach den jeweils spezifischen Umständen des Einzelfalls, die das jeweilige Risiko einer (Re-) Identifizierung der betroffenen Person bestimmen.

4 Konkretes Risiko des Einzelfalls

Um feststellen zu können, ob ein ausreichender Schutz der betroffenen Person vor einer Zuordnung der Daten zu ihr besteht, ist es notwendig, alle objektiven Faktoren für das Risiko der (Re-)Identifizierung im jeweils zu beurteilenden Fall zu berücksichtigen.

23 EuGH vom 7.3.2024, C-479/22 P, Rn. 58 – OLAF.
24 EuGH vom 7.3.2024, C-479/22 P, Rn. 60f. – OLAF.
25 EuGH vom 7.3.2024, C-479/22 P, Rn. 63 – OLAF.
26 EUGH vom 7.3.2024, C-604/22, Rn. 48, 51 – IAB Europe; s. Anm. *Halim/Marosi*, ZD 2024, 333.
27 Hierfür scheint die abstrakte Möglichkeit zu genügen – s. *Halim/Marosi*, ZD 2024, 333.
28 S. Fn. 11.

Das wichtigste Kriterium dürfte die technisch zu bestimmende Qualität des konkret verwendeten Anonymisierungsverfahrens oder des konkret einsetzbaren Identifizierungsverfahrens sein. Diese Qualität ist nicht nur für die jeweilige Gegenwart sondern auch für den Zeitraum zu bestimmen, für den die Entwicklung zu einer für den Verantwortlichen verfügbaren Technik absehbar ist. Daneben sind aber auch weitere objektive Faktoren des Einzelfalls zu berücksichtigen, die das Risiko der (Re-)Identifizierung verstärken oder vermindern.[29] Beispiele solcher Faktoren können sein:

- Aufwand und Kosten der (Re-)Identifizierung. Diese sind in Beziehung zu dem objektiven Interesse der zu berücksichtigenden Personen an einer (Re-)Identifizierung zu setzen. Von einem Risiko ist nach ErwG 26 Satz 4 DSGVO nur auszugehen, wenn nach allgemeinem Ermessen eine relevante Wahrscheinlichkeit der Herstellung des Personenbezugs besteht.
- Missbrauchs- und Schadenspotential für die betroffenen Personen. Ob die Wahrscheinlichkeit der (Re-)Identifizierung relevant ist, hängt auch von den möglichen Nachteilen für die betroffene Person ab.[30] Hier kann der Unterschied bedeutsam sein, ob es um besondere Kategorien personenbezogener Daten, um Daten schützenswerter Personengruppen, um Daten zur Bewertung persönlicher Aspekte oder um Daten geht, mit denen voraussichtlich kein Potential sozialer Diskriminierung, wirtschaftlicher Verluste oder anderer Nachteile verbunden ist.[31] Bedeutsam ist auch der Grad der Reversibilität von Schäden.
- Verfügbarkeit der Daten. Für die Bestimmung des konkreten Risikos ist wichtig, wer Zugriff auf die Daten haben kann.[32] Daher sind z. B. Maßnahmen des Zugriffsschutzes und geschützte Umgebungen wie Use & Access-Mechanismen, Treuhandmodelle oder Federated Learning risikomindernd und freier Zugriff auf die Daten weltweit risikoverstärkend zu berücksichtigen.[33]
- Umfang und Verfügbarkeit notwendiger Hilfsinformationen. Entscheidend ist auch, welches Wissen, welche Fähigkeiten und welche Mittel anderer Personen der Verantwortliche im konkreten Fall rechtmäßig nutzen kann.[34]
- Kontext der weiteren Verarbeitung. Für die Bestimmung des konkreten Risikos ist auch relevant, ob begrenzte Zwecke wie z. B. ein einmaliges Forschungsprojekt oder weite Zwecke wie z. B. Veröffentlichung als Open Data mit den Daten verfolgt werden können.[35]
- Verwendung der Daten. Entscheidend sind auch persönliche oder zeitliche Beschränkungen der Datenverarbeitung wie eine zeitnahe Löschung der Daten nach der Verwendung durch eine vertrauenswürdige Stelle.
- Rechtlicher Schutz vor einer Re-Identifizierung. Risikobegründend ist ein Rechtsanspruch gegenüber dem Inhaber des entscheidenden Zusatzwissens.[36] Risikomindernd kann auch ein rechtliches Verbot der Re-Identifizierung sein,[37] das mit einer abschreckenden Haftung oder Strafbewehrung sowie einer realistischen Chance der Entdeckung verbunden ist.

Ob durch diese risikoverstärkenden oder -mindernden Faktoren im konkreten Fall eine ausreichende Risikoreduktion erfolgt, kann nicht der „Natur" der Daten entnommen werden, sondern muss die unterschiedlichen Rollen der Akteure berücksichtigen, deren Datenverarbeitung beurteilt wird.

5 Verantwortliche in unterschiedlichen Rollen

Die Analyse der EuGH-Rechtsprechung hat gezeigt, dass im konkreten Fall die Handlungsmöglichkeiten des jeweils Verantwortlichen entscheidend sind. Nach Art. 2 Abs. 1 DSGVO treffen den Verantwortlichen die Pflichten nach der DSGVO[38] dann, wenn er personenbezogene Daten verarbeitet. Die mit dieser Feststellung verbundenen Eingriffe in die Grundrechte des Verantwortlichen sind lediglich dann gerechtfertigt, wenn von seiner Datenverarbeitung für die betroffene Person ein Risiko für ihre Grundrechte ausgeht.[39] Dies ist nur der Fall, wenn er für eine mögliche (Re-)Identifizierung das Wissen, die Fähigkeiten und die Mittel einer anderen Person rechtmäßig nutzen kann. Daher ist es auch primärrechtlich richtig, an der Risikoverursachung des Verantwortlichen anzusetzen.

Für die Frage, ob eine Datenverarbeitung mit personenbezogenen oder nicht personenbezogenen Daten stattfindet, sind zumindest zwei verschiedene Rollen zu unterscheiden, die mit unterschiedlichen Anforderungen an den Ausschluss des Personenbezugs verbunden sind.

5.1 Anonymisierung personenbezogener Daten

Wenn der Verantwortliche personenbezogene Daten anonymisieren will, ist für die Frage, ob er durch sein Verfahren das Risiko eines Personenbezugs ausreichend reduziert, entscheidend, wer die Daten danach zu welchen Zwecken verarbeiten kann und welche risikoreduzierenden Maßnahmen er gegen eine (Re-)Identifizierung getroffen hat.

Legt der Verantwortliche die Daten anderen Stellen offen, muss er sich deren Wissen, Fähigkeiten und Mittel zurechnen lassen.[40] Für eine ausreichende Anonymisierung müssen die Daten für alle potentiellen Verarbeiter weder personenbezogen noch personenbeziehbar sein. Daher ist das mobilisierbare Zusatzwissen aller Internetnutzer zu berücksichtigen, wenn die Daten – etwa im Rahmen von Open Data – frei im Internet zur Verfügung gestellt werden sollen.

Dagegen ist nur das mögliche Zusatzwissen etwa eines bestimmten Forschers zu berücksichtigen, wenn durch ausreichende Schutzmaßnahmen sichergestellt ist, dass nur er die anonymisierten Daten verwenden kann und sie danach gelöscht werden. Will der Verantwortliche die Daten anonymisieren, um sie selbst – geschützt gegen Zugriffe Dritter – ohne Datenschutzbeschrän-

29 DSK (Fn. 10), S. 3 ff.; s. z. B. auch *Burghoff*, ZD 2023, 658 (661).

30 DSK (Fn. 10), S. 1f.

31 DSK (Fn. 10), S. 2, 5; *Bieker/Bremert/Hansen*, DuD 2018, 492 (494).

32 EuGH vom 9.11.2023, C-319/22, Rn. 48 – Gesamtverband Autoteile-Handel; s. auch *Stummer*, DuD 2024, 373 (375).

33 S. z. B. *Stummer*, DuD 2024, 373 (375).

34 EuGH vom 19.10.2016, C-582/14, Rn. 45 – Breyer; ebenso EuG vom 26.4.2023, T-557/20, Rn. 104f.; *Hofmann/Johannes*, ZD 2017, 223.

35 S. für eine Presserklärung EuGH vom 7.3.2024, C-479/22 P, Rn. 58 ff. – OLAF.

36 EuGH vom 19.10.2016, C-582/14, Rn. 49 – Breyer; EUGH vom 7.3.2024, C-604/22, Rn. 48, 51 – IAB Europ.

37 S. hierzu *Roßnagel/Geminn*, ZD 2021, 487 (488, 500); insofern könnte Japan ein Vorbild sein – s. hierzu *Fujiwara/Geminn/Roßnagel*, ZD 2019, 204 ff.

38 Erfüllungsverantwortung nach Art. 5 Abs. 2 Satz 1 DSGVO und Handlungspflichten nach Art. 24 ff. DSGVO.

39 S. z. B. auch *Hofmann/Johannes*, ZD 2017, 2021 (223, 225).

40 EUGH vom 7.3.2024, C-604/22, Rn. 48, 51 – IAB Europe; EuGH vom 7.3.2024, C-479/22 P, Rn. 58 ff. – OLAF.

kungen weiterzuverarbeiten, ist zu prüfen, ob er selbst in der Lage ist, die betroffenen Personen zu (re-)identifizieren.

5.2 Nutzung anonymer Daten

Nutzt ein Verantwortlicher anonyme Daten, weiß er oft nicht, ob sie nachträglich anonymisiert oder ursprünglich anonym sind. Zu prüfen ist, ob sie jeweils für ihn personenbeziehbar sind.[41] Dabei ist das potentielle Zusatzwissen anderer Personen dann zu berücksichtigen, wenn der Verantwortliche dieses auf rechtmäßige Weise nutzen kann.[42] Sind die anonymen Daten – egal ob ursprünglich anonym oder nachträglich anonymisiert – für ihn unter keinen Umständen personenbeziehbar, geht von ihm also in keiner Weise ein Risiko der (Re-)Identifizierung aus, gibt es keinen Grund, warum er in seinen Grundrechten (z. B. Forschungsfreiheit, Berufsfreiheit) beeinträchtigt werden könnte. Insofern unterscheiden sich z. B. Forschende, die in einem geschützten Raum mit eigenen Programmen anonymisierte Daten auswerten lassen, ohne dass die Daten diesen Raum jemals verlassen, von kommerziellen Verarbeitern, die anonymisierte Daten ins Ausland transferieren, um sie dort mit personenbezogenen Daten, die sie durch Tracking und Scraping im Internet gewinnen und von Dritten aufkaufen, zusammen für die Erstellung von Werbeprofilen auszuwerten, auch wenn es um die gleichen Daten geht.

5.3 Berücksichtigung der konkreten Risikosituation

Um die Anforderungen an eine ausreichend risikominimierende Anonymisierung oder anonyme Nutzung zu beurteilen sind die unterschiedlichen Rollen der Verantwortlichen und die jeweils für sie bestehenden risikoverstärkenden oder -mindernden Faktoren zu berücksichtigen. Um Anonymität zu gewährleisten ist meist ein Strauß von Schutzmaßnahmen erforderlich. Die jeweils realisierten Schutzmaßnahmen können für die abschließende Risikobeurteilung entscheidend sein.

6 Risikofaktoren unterschiedlicher Anwendungsbereiche

Um die Anforderungen an eine ausreichende Anonymisierung oder an eine anonyme Nutzung der Daten zu bestimmen, empfiehlt es sich, typische Anwendungsbereiche zu unterscheiden. Im Folgenden werden exemplarisch fünf typische Szenarien und einige mit ihnen verbundene Herausforderungen skizziert sowie zusätzliche Schutzmechanismen angedeutet. Für die vom EuGH geforderte konkrete Risikobewertung ist die jeweils spezifische Risikosituation entscheidend.

6.1 Medizinische Forschung

Die medizinische Forschung verarbeitet Gesundheitsdaten. Das Schadenspotential einer (Re-)Identifizierung ist daher sehr groß und die Anforderungen an die Risikoreduktion durch Anonymisierung oder bei der Nutzung anonymer Daten sind sehr hoch. Anonymität kann die Nutzung von Patientendaten zu Forschungszwecken vereinfachen oder überhaupt erst ermöglichen. Gleichzeitig muss bei der Anwendung anonymer Daten sichergestellt werden, dass sie für den Forschungszweck noch aussagekräftig sind.

Medizinische Forschung kann das Risiko reduzieren, wenn die Weitergabe und Verwendung anonymisierter Patientendaten in kontrollierter Form erfolgt. So könnte die Nutzung anonymisierter Daten auf einzelne Forschungsgruppen oder -projekte begrenzt sein oder zeitlich befristet erfolgen. Der Zugriff auf die anonymisierten Daten könnte ausgeschlossen sein und die Datenauswertungen in einem geschützten Datenraum erfolgen. Organisatorisch könnten die Weitergabe und Nutzung der anonymisierten Forschungsdaten von einem Treuhänder kontrolliert werden, der rechtlich in besonderer Weise verpflichtet ist. Eine weitere rechtliche Risikoreduktion könnte die Anerkennung eines spezifischen Forschungsgeheimnisses bewirken.[43]

6.2 Staatliche Statistiken und Planungen

Aussagekräftige Statistiken können helfen, insbesondere gesellschaftliche und wirtschaftliche Entwicklungsprognosen und strategische Planungen in unterschiedlichen Politikbereichen zu verbessern. Ihnen können personenbezogene Daten aus allen Gesellschaftsbereichen zugrunde liegen. Das Schadenspotential kann daher sehr unterschiedlich sein. Um personenbezogene Daten für Statistiken zu verwenden, müssen sie – vor allem durch Aggregation – anonymisiert werden. Je umfangreicher der gesamte Datenschatz ist, je detaillierter die einzelnen Datensätze sind und je mehr Bezüge sie untereinander aufweisen, umso aussagekräftiger ist die aus ihnen erstellte Statistik.

Für die anonymisierten statistischen Daten ist zu beachten, dass die verbleibende Anonymitätsmenge jeweils groß genug bleibt, um auch durch die Verwendung mehrerer Merkmale keine (Re-)Identifizierung zu ermöglichen. Risikosteigernd ist der öffentliche Zugang zu Statistikdaten, risikomindernd die beschränkte Weitergabe an wenige bekannte Empfänger (z. B. staatliche Stellen für strategische Planung).[44] Dabei ist jeweils der Detaillierungsgrad der anonymisierten Daten zu berücksichtigen. Dies ist aber eine Aufgabe, zu deren Bewältigung die Statistikämter ausreichende Erfahrung haben. Weiter ist entscheidend, ob den Empfängern untersagt ist, die anonymisierten Daten auch für konkrete Verwaltungsverfahren und für andere Zwecke zu verwenden.[45] Ein rechtlicher Schutz bietet das Statistikgeheimnis.[46]

6.3 Training lernender Systeme

Das Schadenspotential beim Training lernender Systeme ist abhängig vom Anwendungsbereich. Ist dieser nicht eingrenzbar, ist ein hohes Schadenspotential anzunehmen.[47] Risikosteigernd wäre, wenn das trainierte KI-System in der Lage wäre, bei einer (Re-) Identifizierung hilfreich zu sein. Gleiches gilt für den Fall, dass es Nutzenden möglich wäre, zusätzliche Informationen über be-

41 EuGH vom 19.10.2016, C-582/14, Rn. 49 – Breyer; EUGH vom 7.3.2024, C-604/22, Rn. 48 ff. – IAB Europe; EuGH vom 7.3.2024, C-479/22 P, Rn. 58 ff. – OLAF; EuGH vom 9.11.2023, C-319/22, Rn. 46 ff. – Gesamtverband Autoteile-Handel.

42 EuGH vom 19.10.2016, C-582/14, Rn. 49 – Breyer; EUGH vom 7.3.2024, C-604/22, Rn. 48, 51 – IAB Europe.

43 S. hierzu § 7 GDNG. S. zu den risikoreduzierenden Maßnahmen auch DSK, Petersberger Erklärung zur datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung vom 24.11.2022.

44 S. z. B. *Stummer*, DuD 2024, 373 (376).

45 S. BVerfGE 65, 1 (51, 61 ff.).

46 *Ziegler*, Statistikgeheimnis und Datenschutz, 1990.

47 S. *Kugelmann*, Scharniere zwischen DS-GVO und KI (in diesem Heft).

troffene Personen zu erlangen, deren anonymisierte Daten für das Training eines KI-Systems verwendet wurden. Ein besonders hohes Risiko ist anzunehmen, wenn die anonymisierten Daten auf einem Markt für KI-Training angeboten und für viele KI-Systeme mit unterschiedlichen Einsatzwecken verwendet werden können.

Risikomindernd könnte sein, wenn die anonymisierten Daten nur für einen einzigen Zweck – Training von einem oder mehreren spezifischen KI-Systemen – verwendet und danach gelöscht werden. Gleiches gilt, wenn die anonymisierten Daten nicht an die Hersteller von KI-Systemen übermittelt, sondern von Treuhändern verwaltet werden, die das Training von KI-Systemen in geschützten Räumen ermöglichen.

6.4 Datenübermittlung in Drittländer

Das Risiko der (Re-)Identifizierung könnte beträchtlich steigen, wenn der Verantwortliche die Daten in ein Drittland übermittelt oder eine Stelle des Drittlands über ihn auf die Daten zugreifen kann. In diesem Fall sind auch die Möglichkeiten der Behörden in dem Drittland zu berücksichtigen, Identitäten aufzudecken. Da sie die Daten aufbewahren und die betroffenen Personen zu einem späteren Zeitpunkt (re-)identifizieren können, ist auch die zeitlich begrenzte Gültigkeit der Feststellung, dass die Daten nicht personenbeziehbar sind, zu berücksichtigen. Dies gilt insbesondere in „unsicheren" Drittländern mit unzureichenden Datenschutzregelungen.

Umgekehrt können auch hier als risikomindernd der jeweilige Verwendungsbereich und -zweck sowie die zusätzlichen Schutzmaßnahmen und deren Zuverlässigkeit zu berücksichtigen sein. So könnte von Bedeutung sein, dass die Daten im Rahmen eines internationalen Forschungsprojekts von einem zuverlässigen Forschungsinstitut in einem Drittland mit anerkanntem angemessenen Datenschutzniveau verwendet werden und Schutzvorkehrungen bestehen, die Daten nicht weiterzugeben und nach Projektende zuverlässig zu löschen.

6.5 Open Data

Besondere Anforderungen an die Anonymisierung von Verwaltungsdaten entstehen, wenn die Daten auf einem Open Data-Portal im Internet frei und unbeschränkt zugänglich sein sollen.[48] In diesem Fall können beliebige Akteure weltweit die Daten beziehen und verarbeiten. Hinsichtlich ihrer Möglichkeit, einen Personenbezug herzustellen, wäre von einem Worst-Case-Szenario auszugehen. Hinsichtlich der Entwicklung von Technologien zur Identifizierung wäre ein langer Zeitraum zu betrachten. Zwar kann die Bereitstellung der anonymisierten Daten auf dem Portal beendet werden. Jedoch dürfte die Löschung der bereits abgerufenen Daten sowie der durch eine etwaige Weitergabe entstandenen weiteren Kopien nicht durchsetzbar sein.

Soweit der Zugriff auf bestimmte Berechtigte und bestimmte Zwecke begrenzt und kontrolliert wird, können risikoreduzierende Maßnahmen ergriffen werden, etwa durch Modifikation des Open Access, wie z. B. eine Identifikation der Verarbeiter oder Maßnahmen zur Löschung der Daten.

48 März/Guggumos/Wilhelm, DuD 2024, 378 ff.

7 Rechtsfolgen der Anonymität

Nach ErwG 26 Satz 6 DSGVO „betrifft" die Verordnung „nicht die Verarbeitung (…) anonymer Daten". Ohne Personenbezug findet die DSGVO nach ihrem Art. 2 Abs. 1 DSGVO keine Anwendung.

7.1 Befürchtungen

Diese Rechtsfolge verbinden viele mit weitreichenden Befürchtungen: Die Feststellung, dass bestimmte Daten anonym sind, ermögliche einen beliebigen Umgang mit diesen Daten. Für sie gelte kein Datenschutzrecht mehr, sie seien außerhalb der Kontrolle der Datenschutzaufsichtsbehörden. Daher wäre es bezogen auf diese Daten zulässig, alle denkbaren Risiken ohne Einschränkung einzugehen. Die Daten könnten ohne Schutzmaßnahmen für beliebige Zwecke verwendet, an beliebige Empfänger über die ganze Welt verbreitet und mit allen denkbaren anderen Daten zusammengeführt werden. Um diese Risiken zu vermeiden, bestünde die einzige mögliche Maßnahme darin, einen extrem strengen Maßstab für die Anerkennung von Anonymität anzuwenden.

7.2 Datenschutzrechtliche Relevanz

Diese Befürchtungen verkennen, dass Anonymität keine feststehende Eigenschaft von Daten ist, sondern eine Zuschreibung aufgrund einer Risikobewertung. Bewertet wird die Wissensbeziehung zwischen dem Verantwortlichen und der betroffenen Person bezogen auf die Daten zu einem bestimmten Zeitpunkt. Diese Bewertung beruht auf den festgestellten risikosteigernden und risikomindernden Faktoren des jeweiligen Einzelfalls. Die für die Bewertung entscheidenden Faktoren bleiben Voraussetzungen für die Feststellung der Anonymität. Solange sie unverändert sind, gelten die Daten als anonym und das Datenschutzrecht findet auf sie keine Anwendung. Aber die zuvor anonymen Daten können zu personenbeziehbaren Daten werden, wenn eine wesentliche Voraussetzung für die positive Risikobewertung entfällt.

Erlangt der Verantwortliche eine neue Wissensbasis, kann er auf anderes Zusatzwissen Dritter zurückgreifen, kann er neue Technologien nutzen, lässt er Schutzmaßnahmen entfallen, verwendet er die Daten zu anderen Zwecken, führt er sie mit anderen Daten zusammen, gibt er sie an andere Verantwortliche weiter oder eröffnet er den Zugang zu ihnen, dann kann jede dieser Veränderungen dazu führen, dass die Grundlage für die Bewertung als anonym entfällt und die Daten als personenbeziehbar angesehen werden müssen. Dann erstreckt sich der Anwendungsbereich des Datenschutzrechts (wieder) auf die vormals anonymen Daten.[49]

7.3 Handlungsmöglichkeiten der Aufsichtsbehörden

Aus diesen Gründen fallen anonyme Daten auch nicht vollständig aus dem Aufsichtsbereich der Aufsichtsbehörden heraus. Der Umgang mit anonymen Daten unterliegt Regeln, die sich aus den Bedingungen für die Feststellung der Anonymität ergeben. Der potentiell Verantwortliche ist zu einer periodischen Prüfung der

49 S. hierzu auch Roßnagel/Scholz, MMR 2000, 721 (725 ff.); *Roßnagel/Geminn*, ZD 2021, 487 (488); *Stummer*, DuD 2024, 368.

Anonymität und zu deren Dokumentation verpflichtet.[50] Nur dann kann er sicher sein, dass seine Datenverarbeitung nicht dem Datenschutzrecht unterliegt und dies auch nachweisen. Verlieren seine Daten die Bewertung als anonym, muss er nach Art. 5 Abs. 2 DSGVO als Verantwortlicher alle Datenschutzvorgaben einhalten.[51]

Ob bestimmte Daten unter die DSGVO fallen oder als anonyme Daten davon ausgenommen sind, kann und muss die zuständige Aufsichtsbehörde immer wieder überprüfen. Sie kann dafür auf ihre Handlungsbefugnisse nach Art. 58 Abs. 1 DSGVO zurückgreifen. Stellt sie fest, dass entscheidende Faktoren für die Bewertung der Daten als anonym entfallen und die Daten dadurch personenbeziehbar geworden sind, stehen ihr alle Handlungsbefugnisse nach Art. 58 Abs. 2 DSGVO zu.

50 Hier geht es nicht nur um die Beobachtungspflicht des Anonymisierers aus Art. 25 Abs. 1 DSGVO, die z. B. Art. 29 Datenschutzgruppe, WP 216, S. 29; *Marnau*, DuD 2016, 428 (429); *Gierschmann*, ZD 2021, 482 (484); *Lukas*, ZD 2023, 321 (324); *Stummer*, DuD 2024, 373 (375) annehmen, sondern auch um die Pflicht des Verantwortlichen, der anonyme Daten nutzt – s. z. B. auch *Lukas*, ZD 2023, 321 (324).

51 S. hierzu näher *Stummer*, DuD 2024.

8 Zusammenfassung

Zusammenfassend lässt sich festhalten: Anonymität ist keine feststehende Eigenschaft von Daten. Anonymität ist eine Bewertung des ausreichend geringen Risikos, dass der Verantwortliche eine betroffene Person aufgrund bestimmter Daten identifizieren kann.

Für die Bewertung dieses Risikos ist die Rolle des Verantwortlichen als Anonymisierer oder als anonyme Daten Nutzender zu differenzieren. Für die Anonymisierung sind die Risiken der Identifizierung bei allen potentiellen Nutzern zu berücksichtigen, für die Nutzung anonymer Daten sind die Möglichkeiten des Nutzers – unter Berücksichtigung des mobilisierbaren Zusatzwissens Dritter – zur (Re-)Identifizierung zu prüfen.

Zu bewerten sind die Umstände des Einzelfalls. Dabei sind alle risikoerhöhenden und -mindernden Faktoren relevant. Diese sind je nach Anwendungsbereich unterschiedlich.

Entfallen die Grundlagen für die Bewertung von Daten als anonym, werden sie (wieder) zu personenbeziehbaren Daten. Die Verantwortlichen unterliegen allen Anforderungen des Datenschutzrechts und die Aufsichtsbehörden können all ihre Befugnisse anwenden.

So verstanden kann Anonymisierung und anonyme Nutzung von Daten zu einer Lösung des Konflikts zwischen umfangreicher Datennutzung – vor allem für lernende Systeme – und Datenschutz beitragen.