GERRIT HORNUNG / BERND WAGNER

Anonymisierung als datenschutzrelevante Verarbeitung?

Rechtliche Anforderungen und Grenzen für die Anonymisierung personenbezogener Daten

TOM
Datenminimierung
De-Anonymisierung
Identifizierung

■ Die Anonymisierung personenbezogener Daten ist nicht nur im informationstechnischen, sondern auch im datenschutzrechtlichen Sinne als Verarbeitung einzuordnen und bedarf deshalb einer Rechtsgrundlage. Da es sich zugleich um eine datenschutzfreundliche technische und organisatorische Maßnahmen (TOM) handelt, bestehen zwar Besonderheiten, die das geltende Recht aber für den Bereich „normaler" personenbezogener Daten bewältigen kann. Demgegenüber identifiziert der Beitrag die Anonymisierung von Daten nach Art. 9 Abs. 1 DS-GVO als zentrales Problem und plädiert nach Diskussion von Alternativen für eine teleologische Reduktion dieser Norm.
Lesedauer: 24 Minuten

■ The anonymization of personal data is not only to be categorized as processing in the sense of information technology, but also in the sense of data protection law and, therefore, requires a legal basis. As it is simultaneously a data protection friendly TOM, there are particularities which, however, applicable law is able to overcome for the area of „normal" personal data. In contrast, the article will identify the anonymization of data pursuant to Art. 9 Sec. 1 General Data Protection Regulation (GDPR/DS-GVO) as a central problem and – following the discussion – argues the case for a teleological reduction of this provision.

I. Einleitung und Fragestellung

Anonymität wird oftmals als „Königsweg" des Datenschutzes durch Technikgestaltung bezeichnet.[1] Der europäische Gesetzgeber hat Verantwortliche in vielen Vorschriften der DS-GVO verpflichtet, technische oder organisatorische Maßnahmen zu ergreifen, zu denen auch Anonymisierungen gehören können.[2]

Als Ausprägung des Datenminimierungs- und Speicherbegrenzungsgrundsatzes[3] können durch echte und dauerhafte Anonymisierung sowohl die Interessen der betroffenen Personen als auch die der Verantwortlichen verfolgt werden: Erstere werden vor unzulässigen Eingriffen in ihr Datenschutzgrundrecht geschützt, Letztere von den oftmals als starr empfundenen Vorgaben des Datenschutzrechts befreit.

Eine Anonymisierung kann allerdings auch nur den Interessen des Verantwortlichen dienen, wenn eine anonymisierte Kopie der im Bestand vorhandenen Daten erstellt wird und damit neue Verarbeitungsprozesse angestoßen werden, ohne an die Vorgaben des Datenschutzrechts gebunden zu sein. Dann wird aus Perspektive der betroffenen Personen durch den zusätzlichen anonymen Datensatz bestenfalls kein, je nach Wahrscheinlichkeit der De-Anonymisierung aber ein weiteres Risiko geschaffen.

Die DS-GVO strebt also Anonymisierung an. Zugleich verlangt das sog. Verbotsprinzip für jeden Vorgang, der unter den Begriff der Verarbeitung in Art. 4 Nr. 2 DS-GVO fällt, das Vorliegen einer der in Art. 6 Abs. 1 DS-GVO normierten Rechtsgrundlagen; dies wird für besondere Kategorien personenbezogener Daten in Art. 9 Abs. 1 DS-GVO weiter verschärft. In einem informationstechnischen Sinn ist auch die Anonymisierung von Daten eine Verarbeitung und fällt deshalb prima facie in den Anwendungsbereich des Datenschutzrechts. Dieses soll allerdings gem. Art. 1 Abs. 2 DS-GVO Grundrechte und Grundfreiheiten schützen. Ein Schutz jedenfalls des Datenschutzgrundrechts[4] ist jedoch bei anonymen Daten gerade nicht erforderlich.

II. Das Problem der Rechtfertigungsbedürftigkeit

Insofern stellt sich die Frage, ob der Vorgang der Anonymisierung tatsächlich unter das Verbotsprinzip fällt. Wenn dies zutrifft, ist zu klären, welche Erlaubnistatbestände ihn legitimieren können. Im Kern behandelt der folgende Text mithin die Frage, ob eine Anonymisierung personenbezogener Daten auch ohne Einwilligung der betroffenen Person rechtlich zulässig ist.[5] Nicht Gegenstand des Beitrags ist dagegen der Vorgang der Anonymisierung selbst und das Problem, wann Daten (im rechtlichen Sinn) tatsächlich anonym und nicht re-individualisierbar sind.[6] Dies wird vielmehr vorausgesetzt, wohl wissend, dass es in Zeiten von Big Data und KI sehr problematisch geworden ist.

Anders als § 3 Abs. 6 BDSG a.F. enthält die DS-GVO keine Definition der Anonymisierung.[7] Erwägungsgrund 26 DS-GVO umschreibt sie aber mit ihren Rechtsfolgen. Für ihre Wirksamkeit

1 So z.B. *Martini*, DVBl. 2014, 1481 (1487).
2 *Lang*, in: Taeger/Gabel, DSGVO/BDSG, 3. Aufl. 2019, Art. 25 Rn. 38; *Hartung*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 25 Rn. 16; *Martini*, in: Paal/Pauly, DS-GVO/BDSG, 2. Aufl. 2018, Art. 25 Rn. 2.
3 *Herbst*, in: Kühling/Buchner (o. Fußn. 2), Art. 5 Rn. 58; *Weichert*, in: Däubler/Wedde/Weichert/Sommer, DSGVO/BDSG, 2018, Art. 5 Rn. 61.
4 Auch anonyme Daten können rechtliche Probleme verursachen, z.B. mit Blick auf Nutzungsbefugnisse bzw. „Dateneigentum" oder Diskriminierungseffekte ohne Personenbezug; diese Fragen bleiben hier außen vor.
5 Der *BfDI* führt hierzu aktuell ein Konsultationsverfahren durch, s. *BfDI*, Öffentliches Konsultationsverfahren zum Thema Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche, 2020.
6 S. dazu z.B. *Art. 29-Datenschutzgruppe*, Stellungnahme 5/2014 zu Anonymisierungstechniken; *Ohm*, UCLA Law Review 57 (2010), 1701; zum Problem eines „schleichenden" Personenbezugs *Hornung/Wagner*, CR 2019, 565.
7 Anonymisierungstechniken können grob in zwei Gruppen unterteilt werden: „Generalisierung" (Ersetzung der Merkmale durch einen weniger spezifischen Wert mittels Veränderung der entsprechenden Größenskala oder -ordnung) und „Randomisierung" (Verfälschung, durch die die direkte Verbindung zwischen Daten und Person entfernt wird); s. näher *Art. 29-Datenschutzgruppe* (o. Fußn. 6).

sollen 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. Dies erfolgt unter Heranziehung aller „objektiven Faktoren". Insofern können zwei Anonymisierungsformen unterschieden werden. Während im Fall der absoluten Anonymisierung eine Re-Identifizierung gänzlich ausgeschlossen ist, scheitert eine solche bei der faktischen Anonymisierung allein an dem unverhältnismäßig hohen Aufwand (Zeit, Kosten, Arbeitskraft) einer Wiederherstellung des Personenbezugs. Auf Rechtsfolgenseite besteht kein Unterschied: Die DS-GVO ist – zumindest im Nachhinein – nicht anwendbar.[8] Dies gilt jedenfalls so lange, wie sich die Bewertung der Verhältnismäßigkeit nicht verändert.[9]

Versteht man Anonymisierung im rechtlichen Sinne als Verarbeitung, wird sie vom Verbotsprinzip erfasst und somit rechtfertigungsbedürftig.[10] Dies kann für den Verantwortlichen problematisch sein. So kann es dazu kommen, dass personenbezogene Daten zulässig erhoben wurden und nunmehr erkannt wird, dass sie in anonymer Form auch für sinnvolle andere Zwecke verwendet werden können. Eine echte und dauerhafte Anonymisierung bietet die Möglichkeit, mittels weitergehender Analysen neue Erkenntnisse zu finden, die für Forschungs-, Wirtschafts- und Verwaltungsprozesse von erheblichem Nutzen sein können. Auch Weitergabe und Austausch von Daten mit Vertrags- und Kooperationspartnern werden ermöglicht.

Diese Weiterverwendungen könnten unzulässig sein, wenn die Anonymisierung eine entsprechende Rechtsgrundlage erfordern würde und diese nicht gegeben sein sollte. Legitime Interessen und Ziele der Verantwortlichen, die teilweise auch grundrechtlich verankert sind (z.B. Berufs- und Forschungsfreiheit), würden so unmöglich gemacht oder jedenfalls eingeschränkt, obwohl für die Zielerreichung der Personenbezug der Daten nicht relevant ist. Dies erscheint insbesondere deshalb widersinnig, weil die Anonymisierung der Daten typischerweise auch im Interesse der betroffenen Person ist oder diesen Interessen zumindest nicht zuwiderläuft.

III. Anwendung der DS-GVO

Nur weil eine Anonymisierung im informationstechnischen Sinn einen Verarbeitungsvorgang darstellt, muss es sich nicht zwingend auch im Rechtssinn um eine Verarbeitung i.S.v. Art. 4 Nr. 2 DS-GVO handeln, die nach Art. 2 DS-GVO dem Anwendungsbereich der Verordnung unterfällt.

1. Anonymisierung als datenschutzrechtlich relevante Verarbeitung

Art. 4 Nr. 2 DS-GVO nennt – wie Art. 2 lit. a DS-RL, aber anders als § 3 BDSG a.F. – die einzelnen Verarbeitungsschritte nur beispielhaft und versteht Verarbeitung als umfassenden Begriff.

a) Verarbeitungsbegriff in Art. 4 Nr. 2 DS-GVO

Anonymisierung verändert gespeicherte Daten und könnte deshalb eine „Veränderung" i.S.v. Art. 4 Nr. 2 DS-GVO sein.[11] Allerdings sollte eine solche im Rechtssinn nur angenommen werden, wenn durch die inhaltliche Umgestaltung den Daten ein neuer Informationsgehalt über eine Person zukommt.[12] Auf einen solchen Gehalt zielt das Anonymisieren aber gerade nicht ab. Vielmehr soll der Personenbezug der Daten (im Wege der Kürzung oder Vernichtung von Informationen) aufgehoben werden.[13]

In Betracht kommt, Anonymisierung als Löschen oder Vernichten einzuordnen.[14] Unter Löschen wird jede Handlungsform verstanden, die dazu dient, dass Daten nicht mehr verwendet werden können;[15] Vernichtung meint das endgültige Zerstören eines physischen Datenträgers.[16] Auch bei der Anonymisierung ist das Ziel, die Zuordnung der Daten aufzuheben oder jedenfalls so zu erschweren, dass eine Re-Identifizierung nur mit unverhältnismäßig hohen Mitteln zu erreichen ist. Vor diesem Hintergrund sind sowohl das Ziel als auch die Wirkungen einer Anonymisierung (s.o.) jedenfalls vergleichbar mit denen einer Löschung. Von der h.M. wird eine solche allerdings nur angenommen, wenn die Daten irreversibel unkenntlich gemacht wurden.[17] Dies ist hier nicht zwingend gegeben; bei einer faktischen Anonymisierung bleibt die Re-Identifizierung der betroffenen Person zumindest möglich – wenn auch nur mit unverhältnismäßigen Mitteln. Folgt man der h.M., kann zumindest nicht für alle Fälle der Anonymisierung eine Löschung angenommen werden.

Mit der „Verwendung" hat Art. 4 Nr. 2 DS-GVO bereits innerhalb der benannten Beispiele einen sehr weiten Auffangtatbestand. Wenn man darunter jedes gezielte Umgehen mit personenbezogenen Daten versteht,[18] wird auch das Anonymisieren erfasst. Selbst wenn man dies ablehnt, wird man i.E. ein unbenanntes Beispiel der Verarbeitung annehmen müssen, da Art. 4 Nr. 2 DS-GVO erkennbar jeden Umgang mit personenbezogenen Daten erfassen will.[19]

b) Teleologische Reduktion des Anwendungsbereichs?

Der Anwendungsbereich ist damit gem. Art. 2 Abs. 1 DS-GVO grundsätzlich eröffnet. Dieses Ergebnis lässt sich allerdings mit Blick auf die damit verbundenen Probleme und die oftmals betroffenenfreundliche Zielrichtung der Anonymisierung (s.o.) hinterfragen. Beides ließe sich für eine teleologische Reduktion fruchtbar machen.

Das Telos der Regelungen deutet zunächst in die andere Richtung: Die Funktion der weiten Definition in Art. 4 Nr. 2 DS-GVO ist gerade der Einschluss aller Formen des Datenumgangs; das Verbotsprinzip soll ohne Bagatell- oder sonstigen Vorbehalt[20] jede Verarbeitung personenbezogener Daten erfassen. Überdies ist die Anonymisierung wertungsmäßig mit dem Löschen und

---

8 *Arning/Rothkegel*, in: Taeger/Gabel (o. Fußn. 2), Art. 4 Rn. 47; *Eßer*, in: Auernhammer, DSGVO/BDSG, 6. Aufl. 2018, Art. 4 Rn. 71.

9 Insb. durch Verfügbarkeit neuer, schnellerer und/oder günstigerer Verarbeitungstechnologien, s. *Hornung/Wagner*, CR 2019, 565.

10 So z.B. *BfDI* (o. Fußn. 5), S. 6; für die DS-RL *Art. 29-Datenschutzgruppe* (o. Fußn. 6), S. 8.

11 So z.B. *Ernst*, in: Paal/Pauly (o. Fußn. 2), Art. 4 Rn. 48; *Klabunde*, in: Ehmann/Selmayr, DS-GVO, 2. Aufl. 2018, Art. 4 Rn. 20; für das BDSG a.F. z.B. *Weichert,* in: Däubler/Klebe/Wedde/Weichert, BDSG, 5. Aufl. 2016, § 3 Rn. 35; *Schütze*, in: Breil, GMDS Abstractband, 2015, S. 101; *Metschke/Wellbrock,* Datenschutz in Wissenschaft und Forschung, 3. Aufl. 2002, S. 20.

12 *Herbst* (o. Fußn. 3), Art. 4 Nr. 2 Rn. 25; s. für das BDSG a.F. *Gola/Schomerus,* BDSG, 12. Aufl. 2015, § 3 Rn. 30; *Buchner,* in: Taeger/Gabel, BDSG, 2. Aufl. 2013, § 3 Rn. 30.

13 *Schild*, in: BeckOK DSR, 31. Ed. 2020, Art. 4 Rn. 44 f.; *Arning/Rothkegel* (o. Fußn. 8), Rn. 78; s. zum BDSG a.F. *Gola/Schomerus* (o. Fußn. 12), Rn. 31; *Dammann,* in: Simitis, BDSG, 8. Aufl. 2014, § 3 Abs. 1 Rn. 129; *Gierschmann/Saeugling*, Praxiskommentar Datenschutzrecht, 2014, § 3 Rn. 68; *Buchner* (o. Fußn. 12), Rn. 33; *Wójtowicz*, PinG 2013, 65 (67); zumindest für den Regelfall auch *Ambs,* in: Erbs/Kohlhaas, Strafrechtliche Nebengesetze, 211. EL. 2016, § 3 BDSG Rn. 22.

14 So für § 3 Abs. 4 Satz 2 Nr. 5 BDSG a.F. z.B. *Hanloser,* in: BeckOK DSR, 18. Ed. 2016, § 30 Rn. 37.

15 S. *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 4 Nr. 2 Rn. 30.

16 *Schild* (o. Fußn. 13), Rn. 53; *Ernst* (o. Fußn. 11), Rn. 34.

17 S. *Schild* (o. Fußn. 13), Rn. 54; *Roßnagel* (o. Fußn. 15), Rn. 30; zum BDSG a.F. *Dammann* (o. Fußn. 13), Rn. 174, 181; *Buchner* (o. Fußn. 12), Rn. 40; *Schild*, in: Roßnagel, Hdb. Datenschutzrecht, 2003, S. 521.

18 *Roßnagel* (o. Fußn. 15), Rn. 24.

19 *Roßnagel* (o. Fußn. 15), Rn. 10; *Schwartmann/Hermann*, in: Schwartmann/Jaspers/Thüsing/Kugelmann, DSGVO/BDSG, 2018, Art. 4 Rn. 35.

20 Dies entspricht der bereits im Volkszählungsurteil formulierten Erkenntnis, dass es „unter den Bedingungen der automatischen Datenverarbeitung kein ‚belangloses' Datum mehr" gibt, s. BVerfGE 65, 1 (45).

der Vernichtung vergleichbar (s.o.). Beide sind indes eindeutig als erlaubnisbedürftige Datenverarbeitungen geregelt, die dem Verbotsprinzip unterfallen.[21]

Allerdings schützt die DS-GVO ausweislich von Art. 1 Abs. 1, 2 DS-GVO Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere Art. 8 GRCh. Eine Anonymisierung stellt in aller Regel keine Beeinträchtigung von Grundrechten und Grundfreiheiten dar, sondern ist ein Schutzinstrument, um die Auswirkungen einer Datenverarbeitung auf die betroffene Person zu minimieren und sie so vor negativen Folgen zu schützen. Dementsprechend regelt Art. 5 Abs. 1 lit. e DS-GVO, dass personenbezogene Daten in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Hier wird zumindest mittelbar geregelt, dass personenbezogene Daten, wenn möglich, anonymisiert werden sollten.[22]

Allerdings wäre diese Überlegung nur dann eine überzeugende Basis für eine einschränkende Interpretation der Definition des Verarbeitens, wenn eine Anonymisierung niemals mit den Zielen der Art. 1 Abs. 1, 2 DS-GVO in Konflikt kommen würde. Dies ist indes nicht der Fall, wie schon der Vergleich mit der Löschung personenbezogener Daten zeigt. Neben Löschungsgeboten enthält das Datenschutzrecht nämlich auch Löschungsverbote, indem es z.B. handels- oder steuerrechtliche Aufbewahrungspflichten (wie etwa in § 147 AO oder § 257 HGB) oder Dokumentationspflichten (z.B. § 630f BGB) zulässt.[23] Dies erkennt Art. 17 Abs. 3 lit. b DS-GVO an, der den Löschungsanspruch ausschließt, wenn eine rechtliche Verpflichtung die Verarbeitung erfordert; dies bezieht sich insbesondere auf Aufbewahrungspflichten.[24]

Jenseits der Anwendungsbereiche dieser Verbote kann die betroffene Person weitere schutzwürdige Interesse daran haben, dass ihre Daten erhalten bleiben – z.B. um vertragliche Aufbewahrungspflichten Dritten gegenüber zu erfüllen, die personenbezogenen Daten später in einem Rechtsstreit als Beweismittel vorzulegen oder auch nur aus ideellen Gründen weiter verfügbar zu halten.[25] Wenn etwa Cloud-Computing-Dienste für die ausgelagerte Speicherung persönlicher Daten verwendet werden, wäre es ganz offensichtlich unsinnig, dem Anbieter ein voraussetzungsloses und uneingeschränktes Recht zur Löschung, Vernichtung oder Anonymisierung dieser Daten zu gewähren. Derartige Interessen der betroffenen Person am Erhalt ihrer personenbezogenen Daten werden grundrechtlich durch Art. 8 GRCh und das informationelle Selbstbestimmungsrecht geschützt.[26]

Eine teleologische Reduktion müsste damit zumindest auf Fälle beschränkt werden, in denen solche Interessen nicht betroffen sind. Auch insoweit ist sie aber wegen der weitgehend identischen Problematik in den Fällen der Löschung und Vernichtung nicht überzeugend. I.E. ist die Anonymisierung daher eine datenschutzrechtliche Verarbeitung nach Art. 4 Nr. 2 DS-GVO und fällt in den Anwendungsbereich der DS-GVO.[27]

2. Rechtsfolgen

Folgt man dieser Einschätzung, so verlangt Art. 6 Abs. 1 DS-GVO für die Zulässigkeit der Anonymisierung eine der dort genannten Rechtsgrundlagen. Eine explizite Erlaubnisnorm für die Anonymisierung existiert nicht;[28] ein entsprechender Änderungsvorschlag des *Ausschusses für Industrie, Forschung und Energie*[29] wurde nicht berücksichtigt.

a) Tatbestände des Art. 6 Abs. 1 DS-GVO

Wenn bereits die ursprüngliche Erhebung durch Einwilligungen legitimiert wird, so enthalten diese vielfach ohnehin Formulierungen, wonach Daten anonymisiert werden, sobald der Personenbezug nicht mehr erforderlich ist. Sollte dies nicht der Fall sein, müsste die Erklärung lediglich dahingehend angepasst werden, auch eine etwaige spätere Anonymisierung zu umfassen. Dass aus diesem Grund grundsätzlich einwilligungsbereite Personen von einer Einwilligung absehen, ist unwahrscheinlich.

Ist eine Einwilligung nicht möglich, so kann eine Anonymisierung auf andere Alternativen in Art. 6 Abs. 1 DS-GVO gestützt werden. Neben der Erfüllung einer rechtlichen Verpflichtung (Art. 6 Abs. 1 UAbs. 1 lit. c DS-GVO), wie sie z.B. in § 287 Abs. 2 SGB V normiert ist, können sich private Verantwortliche insbesondere auf überwiegende berechtigte Interessen nach Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO berufen.[30] Den schutzwürdigen Interessen der betroffenen Person wird dabei i.R.d. Abwägung Rechnung getragen: Die Anonymisierung der Daten hat zu unterbleiben, sofern die Interessen oder Grundrechte und Grundfreiheiten, die den Schutz personenbezogener Daten erfordern, überwiegen.

Mit dieser Regelung können in aller Regel angemessene Ergebnisse erzielt werden: Soweit im typischen Fall die betroffene Person selbst ein Interesse an oder zumindest kein der Anonymisierung entgegenstehendes Interesse hat, ist diese zulässig. Besteht dagegen ein überwiegendes schutzwürdiges Interesse am Erhalt des Personenbezugs, so darf jedenfalls keine Anonymisierung des originären Datensatzes selbst erfolgen, sondern allenfalls die Anonymisierung einer Kopie.

Behörden können sich gem. Unterabsatz 2 nicht auf Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO berufen, wohl aber – in Deutschland[31] – auf Verarbeitungsbefugnisse, die Bund und Länder in Ausübung der Öffnungsklausel in Art. 6 Abs. 1 UAbs. 1 lit. e, Abs. 2, Abs. 3 DS-GVO erlassen haben und die an die behördlichen Aufgaben anknüpfen, z.B. § 3 BDSG, § 3 Abs. 1 HDSIG. Voraussetzung ist, dass die behördliche Aufgabe die Anonymisierung erfordert. Da es sich um Generalklauseln handelt, können die Normen zwar nur Verarbeitungen mit geringen Eingriffsgewicht tragen, eine Anonymisierung wird aber im Regelfall sogar gar keinen Eingriff darstellen (s.o.) und ist damit zulässig. Soweit gegenläufige Interessen der betroffenen Personen bestehen, ist diesen i.R.v. Ermessens- und Verhältnismäßigkeitserwägungen Rechnung zu tragen. I.E. besteht damit weitgehender Gleichlauf mit Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO.

b) Art. 9 Abs. 1 DS-GVO

Allerdings gilt für beide Lösungen, dass bei besonderen Kategorien personenbezogener Daten i.S.v. Art. 9 Abs. 1 DS-GVO zu-

---

21 § 35 Abs. 2 Satz 1 BDSG a.F. enthielt für das Löschen sogar eine explizite Rechtsgrundlage.

22 *Art. 29-Datenschutzgruppe* (o. Fußn. 6), S. 8, für Art. 6 Abs. 1 UAbs. 1 lit. e DS-RL. Noch deutlicher formulierte dies § 3a Satz 2 BDSG a.F.; s. dazu unter IV.1.

23 *Kamann/Braun*, in: Ehmann/Selmayr (o. Fußn. 11), Art. 17 Rn. 59; *Stollhoff*, in: Auernhammer (o. Fußn. 8), Art. 17 Rn. 63; s. für das BDSG a.F. *Dammann* (o. Fußn. 13), Rn. 172 ff.

24 *Paal*, in: Paal/Pauly (o. Fußn. 2), Art. 17 Rn. 43.

25 Diese Überlegungen lagen § 35 Abs. 2 Satz 1 i.V.m. Abs. 3 Nr. 2 BDSG a.F. zu Grunde.

26 S. für die Löschung nach BDSG a.F. *Brink,* in: BeckOK DSR, 23. Ed. 2017, § 35 Rn. 5; *Gola/Schomerus* (o. Fußn. 12), § 35 Rn. 10.

27 So auch *BfDI* (o. Fußn. 5), S. 6; *Art. 29-Datenschutzgruppe* (o. Fußn. 6), S. 3.

28 Dies entspricht DS-RL und BDSG a.F., solange man nicht – dogmatisch zweifelhaft – in § 3a Satz 2 BDSG a.F. eine gesetzliche Erlaubnisnorm hätte sehen wollen.

29 Stellungnahme v. 26.2.2013 (PE496.562), Art. 6 Abs. 1 lit. fe DS-GVO-E (Änderungsvorschlag 105).

30 So für die DS-RL *Art. 29-Datenschutzgruppe* (o. Fußn. 6), S. 3.

31 Andere EU-Staaten haben ähnliche Normen erlassen, z.B. Frankreich (Art. 5-5 de la loi informatique et libertés) oder Irland (Sec. 38 Data Protection Act 2018), sodass eine europaweite Lösung gangbar sein dürfte.

sätzlich eine der Ausnahmen des Art. 9 Abs. 2 DS-GVO vorliegen muss.[32] Ob diese eine Anonymisierung tragen, ist im Einzelfall zu beurteilen. Für Forschungszwecke eröffnet z.B. Art. 9 Abs. 2 lit. j DS-GVO i.V.m. nationalen Normen (z.B. § 27 Abs. 1 BDSG, § 24 Abs. 1 HDSIG) den Weg zu entsprechenden Abwägungsentscheidungen. Auch bleibt die Einwilligung möglich und muss gem. Art. 9 Abs. 2 lit. a DS-GVO lediglich ausdrücklich erteilt werden. I.E. wird aber – jenseits der bislang teilweise ungeklärten Reichweite einzelner Tatbestände des Art. 9 Abs. 2 DS-GVO – in vielen Fällen keine dieser Ausnahmen greifen.

3. Zwischenergebnis

Dies führt zu widersinnigen Ergebnissen. Art. 9 Abs. 2 DS-GVO geht nämlich in vielen Fällen davon aus, dass die zu legitimierende Datenverarbeitung ohne oder sogar gegen den Willen der betroffenen Person, d.h. nicht in ihrem Interesse, erfolgt.[33] Wie gezeigt, liegt die Anonymisierung aber typischerweise gerade in diesem Interesse.

In dieser Konstellation ist Art. 9 Abs. 2 DS-GVO für beide Beteiligten keine angemessene Regelung: Die Norm ließe, anders als Art. 6 Abs. 1 UAbs. 1 lit. e und lit. f DS-GVO, eine Anonymisierung ohne Einwilligung noch nicht einmal dann zu, wenn sie im Interesse aller Beteiligten ist – wieso dies bei „normalen", nicht aber bei sensiblen Daten zulässig sein soll, ist auf einer Wertungsebene schlechterdings nicht erklärbar. Umgekehrt enthält die Vorschrift aber auch keine allgemeine Ausnahme zur Berücksichtigung etwaiger Interessen der betroffenen Person am Ausschluss einer Anonymisierung.

Vergegenwärtigt man sich zusätzlich die Wertung des Art. 5 Abs. 1 lit. e DS-GVO, so wird deutlich, dass dies nicht das Endergebnis der rechtlichen Bewertung sein kann. Sensible Daten, die nach Art. 9 DS-GVO einen besonderen Schutz genießen, dürften nur in ausgewählten Situationen anonymisiert werden, wodurch der betroffenen Person gerade bei risikoreichen Datenkategorien ein Schutzinstrument vorenthalten werden würde.

IV. Lösungsansätze

Damit die Wertung des Gesetzgebers und das grundsätzliche Interesse der betroffenen Personen an einer Anonymisierung mit den ggf. im Einzelfall bestehenden Interessen an einem Erhalt der personenbezogenen Daten in Einklang gebracht werden können, kommen unterschiedliche Lösungswege in Betracht, um auch bei sensiblen Daten in interessengerechten Fällen eine Anonymisierung zu ermöglichen:

- die Anwendung von Art. 5 Abs. 1 lit. e DS-GVO,
- die Annahme einer Löschungsbefugnis nach Art. 6 Abs. 1 UAbs. 1 lit. c i.V.m. Art. 17 DS-GVO mit nachfolgender analoger Anwendung auf die Anonymisierung,
- eine direkte oder analoge Anwendung von Art. 6 Abs. 4 DS-GVO,
- eine teleologische Reduktion von Art. 6 Abs. 1 DS-GVO, sowie
- eine teleologische Reduktion von Art. 9 Abs. 1 DS-GVO.

1. Art. 5 Abs. 1 lit. e DS-GVO

Anonymisierung ist eine Möglichkeit, um dem Grundsatz der Speicherbegrenzung in Art. 5 Abs. 1 lit. e DS-GVO zu genügen (s.o.). Allerdings enthält Art. 5 DS-GVO systematisch keine Verarbeitungsgrundlagen, sondern Grundsätze, die die Verordnung durchziehen. Art. 6 Abs. 1 DS-GVO ist insoweit abschließend und enthält keinen Normteil, der Art. 5 DS-GVO in Bezug nehmen würde. Eine Einordnung von Art. 5 Abs. 1 lit. e DS-GVO als Erlaubnisnorm ist damit abzulehnen.

2. Art. 6 Abs. 1 UAbs. 1 lit. c i.V.m. Art. 17 DS-GVO

Die DS-GVO enthält keine explizite Anonymisierungsbefugnis (s.o.). Soweit es im Datenschutzrecht explizite Löschungsbefugnisse gibt, lässt sich aber erwägen, diese angesichts der weitgehend parallelen Interessenlagen[34] analog auf die Anonymisierung anzuwenden. Allerdings enthält die DS-GVO auch keine explizite Löschungsbefugnis, wie sie in § 35 Abs. 2 Satz 1 BDSG a.F. enthalten war.[35] Dasselbe gilt für das BDSG n.F.[36] Art. 17 DS-GVO ist systematisch keine Verarbeitungsgrundlage, sondern ein Betroffenenrecht.

Der *BfDI* versucht diese Lücke durch Art. 6 Abs. 1 UAbs. 1 lit. c DS-GVO zu schließen[37] und versteht Art. 17 DS-GVO dementsprechend als „rechtliche Verpflichtung ..., der der Verantwortliche unterliegt". Diese Überlegung verursacht jedoch mehrere Schwierigkeiten. Das größte Problem für den hiesigen Fall ist, dass die Anbindung an Art. 6 DS-GVO die Lösung auf „normale" personenbezogene Daten beschränkt und damit keinerlei Antwort auf das – vom *BfDI* insgesamt ignorierte – Problem der Daten nach Art. 9 Abs. 1 DS-GVO bietet.

Des Weiteren setzt Art. 17 DS-GVO schon systematisch ein entsprechendes Begehren der betroffenen Person voraus und deckt deshalb die o.g. Szenarien der Anonymisierung nur unvollständig ab (insbesondere nicht die Erstellung anonymisierter Kopien). Dem ließe sich möglicherweise durch eine – durch den *BfDI* nicht thematisierte – Analogie abhelfen. Es verbleibt aber wertungsmäßig das Problem, dass Art. 17 DS-GVO die Interessen der betroffenen Person am Ausschluss der Löschung bzw. Anonymisierung nicht berücksichtigt, weil die Norm in direkter Anwendung ein Löschungsbegehren voraussetzt, das in den hier relevanten Konstellationen vielfach fehlt.

I.E. erscheint eine (teilweise analoge) Anwendung von Art. 17 DS-GVO zwar konstruktiv möglich. Die besseren Argumente sprechen aber gegen diesen Weg, zumal das Problem der Daten nach Art. 9 DS-GVO ohnehin ungelöst bliebe.

3. Art. 6 Abs. 4 DS-GVO

Denkbar erscheint, eine Anonymisierung auf Art. 6 Abs. 4 DS-GVO zu stützen. Sie wäre dann eine Weiterverarbeitung der ursprünglich zu einem anderen Zweck erhobenen Daten und bei Vorliegen eines positiven Kompatibilitätstests zulässig.[38]

Eine direkte Anwendung von Art. 6 Abs. 4 DS-GVO dürfte allerdings bereits daran scheitern, dass die Norm erkennbar davon ausgeht, dass nach der Zweckänderung weiterhin personenbezogene Daten vorliegen. Die Vorschrift schränkt Zweckänderungen ein, um die mit ihnen verbundenen Risiken für die betroffene Person zu reduzieren. Typischerweise bestehen derartige Risi-

---

32 *Art. 29-Datenschutzgruppe* (o. Fußn. 6), S. 7 ff. und *BfDI* (o. Fußn. 5), thematisieren dieses Problem nicht.

33 Interessen der betroffenen Person werden nicht beeinträchtigt bei lit. a und (ggf.) verfolgt in lit. b, c, h, i. Auch in lit. d, e kann es zu gleichgerichteten Interessen kommen. Diese Fälle decken aber bei weitem nicht alle Konstellationen von Art. 9 Abs. 2 DS-GVO ab.

34 Insoweit zutreffend *BfDI* (o. Fußn. 5), S. 9 f.

35 Diese berücksichtigten auch etwaige Interessen der betroffenen Person am Ausschluss der Löschung. Eine Analogie hätte sich mit dem Problem einer planwidrigen Regelungslücke auseinandersetzen müssen. Der Gesetzgeber hatte andernorts Befugnisse und Pflichten zur Anonymisierung geschaffen (z.B. §§ 30a Abs. 3 Satz 1, 40 Abs. 2 Satz 1 BDSG a.F., § 287 Abs. 2 SGB V), es gibt aber keine Anhaltspunkte dafür, dass ihm die Konsequenzen eines Fehlens einer allgemeinen Anonymisierungsbefugnis für besondere Arten personenbezogener Daten klar waren. Alternativ hätte man die Anonymisierung entgegen der h.M. unter den Löschungsbegriff in § 3 Abs. 4 Nr. 5 BDSG a.F. subsumieren (*Hanloser* (o. Fußn. 14), Rn. 37) und § 35 Abs. 2 Satz 1 BDSG a.F. direkt anwenden können.

36 § 35 Abs. 2 i.V.m. Abs. 1 BDSG n.F. entsprechen zwar weitgehend § 35 Abs. 3 Nr. 1 und 2 BDSG a.F. Eine Löschungsbefugnis analog § 35 Abs. 2 Satz 1 BDSG a.F. ist aber nicht mehr enthalten.

37 *BfDI* (o. Fußn. 5), S. 8 ff.

38 Als Möglichkeit vorgeschlagen durch den *BfDI* (o. Fußn. 5), S. 6 ff.

ken aber nur, wenn diese nach der Zweckänderung noch identifizierbar ist – nicht bei der Weiterverwendung der Daten in anonymisierter Form.

Dieses Problem könnte man ggf. durch eine analoge Anwendung lösen. Auch dann bietet Art. 6 Abs. 4 DS-GVO aber keine angemessenen Kriterien für die Zulässigkeit einer Anonymisierung: Warum soll es relevant sein, ob der mit den anonymisierten Daten verfolgte Zweck eine Verbindung zum ursprünglichen Zweck aufweist (lit. a) oder welcher Art das Verhältnis zur betroffenen Person ist (lit. b)? Auf anonymisierte Daten ist das Datenschutzrecht nicht anwendbar; eine Beschränkung auf bestimmte Zwecke ist daher nach wirksamer Anonymisierung unangemessen. Eine Verbindung zur betroffenen Person wird zudem in vielen Fällen fehlen,[39] da der Verantwortliche die Daten häufig losgelöst von der Beziehung zu ihr verwenden möchte. Die Berücksichtigung von lit. a und lit. b erscheint überdies unangemessen, da die verfolgten Zwecke gerade keine Interessen der betroffenen Person tangieren.

Auch die anderen Abwägungskriterien passen nicht wirklich auf die Anonymisierung: lit. c geht davon aus, dass es für die Risikobewertung der Zweckänderung relevant ist, ob sensible Daten nach Art. 9 oder Art. 10 DS-GVO vorliegen. Wenn Daten tatsächlich anonymisiert sind, besteht ein solches abstufbares Risiko aber nicht. Die möglichen Folgen der Weiterverarbeitung „für die betroffene Person" nennt lit. d; solche Folgen können bei Anonymisierung aber allenfalls sehr mittelbar eintreten (wenn z.B. in den anonymisierten Daten statistische Zusammenhänge ermittelt und auf deren Basis individuelle Entscheidungen gefällt werden). Wieso es schließlich relevant sein soll, ob anonymisierte (!) Daten nach der Zweckänderung zusätzlich verschlüsselt oder pseudonymisiert werden (lit. e), erschließt sich vollends nicht.

Art. 6 Abs. 4 lit. a-e DS-GVO sind zwar nicht abschließend („u.a."). Da die fünf verbindlichen Kriterien jedoch sämtlich nicht passen, verbliebe es bei einer allgemeinen Abwägung, für die der Rechtsanwender kaum Faktoren finden würde. Angesichts der Unangemessenheit der Anwendung von lit. a-e spricht außerdem nichts dafür, dass man die Norm analog auf die Anonymisierung anwenden kann; dies würde gerade eine vergleichbare Interessenlage erfordern.

Hinzu kommt, dass der Weg über Art. 6 Abs. 4 DS-GVO für das – der Anonymisierung wertungsmäßig eng verwandte – Löschen und Vernichten versperrt ist. Für diese lässt sich eine Zweckänderung i.S.v. Art. 6 Abs. 4 DS-GVO kaum vertreten, da kein anderer Zweck mit den Daten verfolgt wird; diese sind schlicht nicht mehr vorhanden. Unterwirft man die Anonymisierung also Art. 6 Abs. 4 DS-GVO, würde die rechtliche Bewertung von Anonymisierung, Löschung und Vernichtung auseinanderfallen.[40]

4. Teleologische Reduktionen

Will man das unsinnige – und vom europäischen Gesetzgeber schwerlich gewollte – Ergebnis vermeiden, dass das Anonymisieren, Löschen und Vernichten „normaler" Daten über Art. 6 Abs. 1 UAbs. 1 lit. e und lit. f DS-GVO gerechtfertigt sein kann, Art. 9 DS-GVO diesen aber gerade bei sensiblen Daten in vielen Fällen entgegensteht, bedarf es einer interpretatorischen Lösung. Da Löschung, Vernichtung und Anonymisierung wertungsmäßig vergleichbar sind und im vorliegenden Fall gleichbehandelt werden sollten, wird im Folgenden eine Lösung vorgeschlagen, die nicht nur für die Anonymisierung, sondern – was nicht jedes Mal erwähnt wird – auch für Löschung und Vernichtung anwendbar ist.

a) Methodischer Ausgangspunkt

Hierfür kommen eine teleologische Reduktion des Verbotsprinzips aus Art. 6 Abs. 1 DS-GVO oder des Verarbeitungsverbots aus Art. 9 Abs. 1 DS-GVO in Betracht. Methodisch könnte zwar eingewandt werden, dass ein Vorschlag für eine explizite Rechtsgrundlage für die Anonymisierung nicht in die DS-GVO aufgenommen wurde.[41] I.E. greift dies jedoch nicht durch, weil zumindest anhand der veröffentlichten Materialien nicht erkennbar ist, aus welchem Grund dies erfolgte. Die Nichtaufnahme kann eine Absage an eine Anonymisierungsbefugnis gewesen sein (dies würde einer teleologischen Reduktion entgegenstehen) oder der Überlegung entsprungen sein, Anonymisierungen seien ohnehin zulässig und bedürften keiner expliziten Befugnis (dies würde die Reduktion zulassen). Von Ersterem sollte angesichts der problematischen Folgen nicht ohne weitere Anhaltspunkte ausgegangen werden.

Voraussetzung für eine teleologische Reduktion ist, dass die vom Wortlaut erfassten Fälle der Zielsetzung des Gesetzes widersprechen.[42] Insofern ließe sich argumentieren, dass eine Reduktion von Art. 9 DS-GVO sensible Daten den allgemeinen Rechtfertigungstatbeständen unterwerfen würde, was die Norm gerade ausschließen soll. Eine Reduktion von Art. 6 DS-GVO würde die Anonymisierung sogar vollständig aus dem wichtigen Schutzinstrument des Verbotsprinzips ausnehmen. Beides widerspricht dem Ziel der DS-GVO jedoch zumindest nicht grundsätzlich, da Daten ausweislich Art. 5 Abs. 1 lit. e DS-GVO möglichst häufig anonymisiert werden sollen und Anonymisieren insofern – genau wie Löschen und Vernichten – eben keine normale Datenverarbeitung darstellt, sondern eine Maßnahme, die die Risiken für die betroffene Person reduziert.

b) Reduktion von Art. 6 Abs. 1 DS-GVO

Eine teleologische Reduktion des Verbotsprinzips würde dazu führen, dass eine Anonymisierung keiner Rechtsgrundlage bedürfte, obwohl es sich um eine Verarbeitung i.S.v. Art. 4 Nr. 2 DS-GVO handelt. Verantwortliche dürften somit stets anonymisieren. Dies würde zumindest im Regelfall zu einem verbesserten Schutz der betroffenen Person führen, indem das von den personenbezogenen Daten ausgehende Risiko, wenn nicht komplett beseitigt, so doch ganz erheblich gemindert würde.

Gegen eine solche Lösung sprechen jedoch die teilweise bestehenden Interessen der betroffenen Person am Erhalt ihrer Daten. Wie gesehen, kann nämlich auch das Anonymisieren einen Eingriff in das Recht auf informationelle Selbstbestimmung bzw. den Schutz personenbezogener Daten (Art. 8 GRC) darstellen.[43] Solche Aspekte fänden an keiner Stelle Beachtung, wenn eine Anonymisierung von vornherein rechtfertigungslos zulässig wäre.

Diesem Problem könnte man begegnen, indem man die Interessen der betroffenen Person über den Grundsatz der Verarbeitung nach Treu und Glauben (Art. 5 Abs. 1 lit. a 2. Alt. DS-GVO) berücksichtigt. Dieser soll vor unklaren Verarbeitungsvorgängen schützen,[44] daneben aber auch als Auffangklausel dienen, um eine „als unklar zu beanstandende Datenverarbeitung auch bei Fehlen einer einschlägigen Regelung als rechtswidrig qualifizieren zu können."[45] Dies ließe sich hier fruchtbar machen: Art. 5

39 Die durch den *BfDI* genannte Konstellation einer Optimierung der der betroffenen Person angebotenen Dienstleistung (*BfDI* (o. Fußn. 5), S. 7 f.) dürfte eher einen Sonderfall darstellen.

40 Dies wird wohl übersehen durch den *BfDI* (o. Fußn. 5), obwohl dort gerade für eine wertungsmäßige Übereinstimmung argumentiert wird, S. 9 f.

41 S. Fußn. 29.

42 Statt vieler *Schwacke*, Juristische Methodik, 5. Aufl. 2011, S. 140.

43 S.o. III.2.a).

44 *Albrecht/Jotzo,* Das neue Datenschutzrecht der EU, 2017, S. 51.

45 *Dammann/Simitis,* EG-DSRL, 1997, Art. 6 Rn. 3, für Art. 6 Abs. 1 UAbs. 1 lit. a DS-RL; für die DS-GVO *Reimer*, in: Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 5 Rn. 14; *Herbst* (o. Fußn. 3), Art. 5 Rn. 17; *Roßnagel* (o. Fußn. 15), Art. 5 Rn. 47.

Abs. 1 lit. a 2. Alt. DS-GVO würde dann eine Beschränkung der teleologischen Reduktion von Art. 6 Abs. 1 DS-GVO auf solche Fälle verlangen, in denen die betroffene Person kein Interesse an dem Erhalt der Daten oder ihrer Personenbeziehbarkeit hat oder es um die Anonymisierung einer eigens zu diesem Zweck erzeugten Kopie geht. Verstößt der Verantwortliche hiergegen, wäre das Anonymisieren treuwidrig und damit rechtswidrig. Diese Lösung würde weitgehend der o.g. Rechtslage nach Art. 6 Abs. 1 UAbs. 1 lit. e (i.V.m. nationalen Regelungen) bzw. lit. f DS-GVO entsprechen.

Auch wenn sich auf diesem Weg angemessene Ergebnisse erzielen ließen, ist eine teleologische Reduktion des für das Datenschutzrecht zentralen Verbotsprinzips aber abzulehnen. Dieses sollte nicht durch offene Wertungskriterien eingeschränkt werden, weil andernfalls die Gefahr bestünde, Grundprinzipien des Datenschutzrechts durch unbestimmte Rechtsbegriffe auszuhebeln. Dies gilt umso mehr, als es mit der teleologischen Reduktion des Art. 9 Abs. 1 DS-GVO einen deutlich kleineren Eingriff in das Regelungssystem der DS-GVO gibt.

c) Reduktion von Art. 9 Abs. 1 DS-GVO

Durch eine teleologische Reduktion des Verbots in Art. 9 Abs. 1 DS-GVO würde für eine Anonymisierung sensibler Daten Art. 6 Abs. 1 UAbs. 1 lit. e und lit. f DS-GVO zur Anwendung gelangen. Die schutzwürdigen Interessen der betroffenen Person würden in die Abwägung einfließen und wären damit gewahrt (s.o.).

Zwar etabliert Art. 9 DS-GVO einen höheren Schutzstandard für sensible Daten, der nicht leichtfertig teleologisch reduziert werden sollte. Allerdings fehlt es nicht nur für die Anonymisierung, sondern auch für die vergleichbare Löschung und Vernichtung an einer Verarbeitungsbefugnis, soweit sensible Daten betroffen sind. Art. 9 Abs. 2 DS-GVO enthält zu dieser Frage auch keine Öffnungsklausel. Es spricht daher alles dafür, dass der europäische Gesetzgeber das Problem der Rechtsgrundlage auch für die explizit geregelten Verarbeitungsformen des Löschens und Vernichtens sensibler Daten schlicht übersehen hat.

Dass die Verarbeitung sensibler Daten nur unter den zusätzlichen Voraussetzungen des Art. 9 Abs. 2 DS-GVO erlaubt ist, ergibt nämlich nur für die Fälle Sinn, in denen durch die Verarbeitung ein erhöhtes Risiko für Grundrechte und -freiheiten entsteht. Dies trifft auf Löschen, Vernichtung und Anonymisierung aber in aller Regel nicht zu. Das Beharren auf dem grundsätzlichen Verarbeitungsverbot für sensible Daten würde in diesen Fällen vielmehr zu einem erhöhten Risiko für die Rechte der betroffenen Person führen und somit der Zielsetzung des Gesetzes widersprechen.

Die Voraussetzungen für eine teleologische Reduktion des Art. 9 Abs. 1 DS-GVO liegen mithin vor. Löschen, Vernichten und Anonymisieren sensibler Daten sollten daher nicht eine der zusätzlichen Vorgaben des Art. 9 Abs. 2 DS-GVO erfüllen müssen, sondern sich, wie die Verarbeitung „normaler" personenbezogener Daten generell, nach den Erlaubnisnormen des Art. 6 Abs. 1 UAbs. 1 DS-GVO, insbesondere lit. e und lit. f, richten. Die Anwendung dieser Normen auf die erläuterten Sonderfälle eines ausnahmsweise bestehenden berechtigten Interesses am Erhalt der Daten ist für die Rechtsanwendung auch handhabbarer als eine Begrenzung einer teleologischen Reduktion von Art. 6 Abs. 1 DS-GVO durch den Grundsatz von Treu und Glauben. I.E. ist deshalb „nur" Art. 9 DS-GVO für Löschen, Vernichtung und Anonymisierung personenbezogener Daten teleologisch zu reduzieren.

V. Ergebnis

Das Anonymisieren personenbezogener Daten fällt unter den Begriff der Verarbeitung nach Art. 4 Nr. 2 DS-GVO und damit in den sachlichen Anwendungsbereich der Verordnung. Diese scheint auf den ersten Blick mit Art. 6 Abs. 1 UAbs. 1 lit. e (i.V.m. nationalen Normen) und lit. f DS-GVO angemessene Lösungen für die Zulässigkeit der Anonymisierung – ebenso wie die des Löschens und der Vernichtung – „normaler" personenbezogener Daten bereitzustellen, nicht jedoch für besondere Kategorien personenbezogener Daten i.S.v. Art. 9 Abs. 1 DS-GVO.

Da auch das Anonymisieren sensibler Daten in aller Regel dem Schutz der betroffenen Person dient, ist ein Gleichlauf von „normalen" und sensiblen personenbezogenen Daten zu erzielen. Hierzu sollte eine teleologische Reduktion von Art. 9 Abs. 1 DS-GVO gewählt werden. Insbesondere gegenüber einer teleologischen Reduktion von Art. 6 Abs. 1 DS-GVO oder des Anwendungsbereichs der DS-GVO insgesamt erscheint eine solche Reduktion als vorzugswürdig. Denn im Vergleich stellt diese den „kleineren Eingriff" in das Normenwerk der DS-GVO dar, weil lediglich eine spezielle Norm für unanwendbar erklärt wird, statt das zentrale Verbotsprinzip auszuhebeln. Da teleologische Reduktionen schon unter Gewaltenteilungsgesichtspunkten auf das Notwendigste beschränkt werden sollten,[46] sollte dieser Weg beschritten werden.

Abschließend bleibt festzuhalten, dass in jedem Fall einer der diskutierten Lösungswege zu wählen ist. Die weitgehende Unzulässigkeit der Anonymisierung, Löschung und Vernichtung sensibler personenbezogener Daten bei gleichzeitiger Zulässigkeit der Anonymisierung, Löschung und Vernichtung „normaler" Daten ist ein eklatanter Wertungswiderspruch und dementsprechend abzulehnen. Sofern – wie im Regelfall – keine Anhaltspunkte für entgegenstehende Interessen der betroffenen Person bestehen, ist das Anonymisieren personenbezogener Daten folglich nach der DS-GVO ein zulässiger Datenverarbeitungsvorgang.

Professor Dr. Gerrit Hornung, LL.M.,
ist Leiter des Fachgebiets Öffentliches Recht, IT-Recht und Umweltrecht und Leiter der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) im Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) der Universität Kassel sowie Mitglied des Wissenschaftsbeirats der ZD.

Dr. Bernd Wagner
ist Rechtsreferendar in Nürnberg und ehemaliger Mitarbeiter des ITeG.

Der Text geht auf eine Anfrage aus der Praxis zurück.

46 Vgl. z.B. *Flume,* Das Rechtsgeschäft, 4. Aufl. 1992, S. 297 ff.