Stellungnahme zum öffentlichen Konsultationsverfahren des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Thema:

Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche

Karlsruhe/Bonn, 9. März 2020

Prof. Dr. Franziska Boehm[1], Prof. Dr. Michael Meier[2] und Prof. Dr. Thorsten Strufe[3]
Unter Mitwirkung von Saffija Kasem-Madani[4] und Stephanie von Maltzahn, Oliver Vettermann und Dr. Dara Hallinan[5]

[1] Bereichsleiterin Immaterialgüterrechte, FIZ Karlsruhe und Professorin des Karlsruher Insitut für Technologie, Zentrum für Angewandte Rechtswissenschaft (ZAR).

[2] Lehrstuhlinhaber Abteilung Sicherheit und Vernetzte Systeme, Insitut für Informatik, Universität Bonn, Abteilungsleiter Cyber Security Fraunhofer FKIE.

[3] Lehrstuhlinhaber Institut für Praktische Sicherheit, Karlsruhe Institute of Technology, Professor für Privacy und Netzwerksicherheit, TU Dresden, Sprecher des Exzellenzclusters Center for Tactile Internet with Human-in-the-Loop (CeTI)

[4] Wissenschaftliche Mitarbeiterin, Abteilung Sicherheit und Vernetzte Systeme, Insitut für Informatik, Universität Bonn.

[5] Wissenschaftliche Mitarbeiter/innen, FIZ Karlsruhe, Immaterialgüterrechte.

Zusammenfassung

Die folgende Stellungnahme adressiert folgende Punkte im Besonderen:

- die **Definition der Anonymisierung**, die im Entwurf des BfDI-Positionspapiers wichtige Aspekte ungeklärt lässt. Ein Beispiel dafür ist die Frage, welche Anforderungen an die Berücksichtigung des Wissens und der Mittel Dritter zu stellen sind und wann für welche Beteiligten eine Anonymisierung gegeben ist.
- das **Risiko der (Re-)Identifizierung**, das auch nach erfolgter Anonymisierung besteht und entsprechend beurteilt werden muss.
- die nicht erfolgte **Abgrenzung der Anonymisierung zur Pseudonymisierung**, die notwendig ist, um Missverständnissen und Unklarheiten auf rechtlicher und technischer Ebene vorzubeugen.
- die **Anonymisierung in der Forschung**, deren Begriff unklar bleibt; das Positionspapier aber dazu beitragen könnte, den Anonymisierungsbegriff in der Forschung zu spezifizieren.
- die **Rechtsgrundlage(n) zur Weiterverarbeitung von Daten**, die im Entwurf des BfDI-Positionspapiers sehr umstritten ausgelegt werden (insbesondere EWG 50 DSGVO) und bei deren Interpretation auch andere Ansichten Berücksichtigung erfahren sollten.
- die grundsätzliche **Gleichsetzung von Löschung und Anonymisierung**, deren Darstellung im Entwurf des BfDI-Positionspapiers wichtige Aspekte, u.a. die Systematik der DSGVO und die Schutzrichtung des Löschungsrechts, außer Acht lässt.
- die fehlenden Hinweise auf **technische Anonymisierungsmaßnahmen und Kriterien zur Bestimmung angemessener Verfahrensparameter**.

FIZ Karlsruhe
Leibniz-Institut für Informationsinfrastruktur

Karlsruhe Institute of Technology

UNIVERSITÄT BONN

Einleitung

Mit großem Interesse haben wir die öffentliche Konsultation des BfDI in Vorbereitung eines Positionspapiers zur Anonymisierung zur Kenntnis genommen und beteiligen uns mit dieser Stellungnahme aus der Forschungsperspektive an diesem Verfahren. Die Bedeutung eines zukünftigen Positionspapiers schätzen wir angesichts der technischen sowie gesellschaftlichen Entwicklung als hoch ein, gibt es doch bisher nur wenig gefestigte Aussagen in diesem, nicht nur für die Forschung, relevanten Bereich. Das Positionspapier wird zur Konkretisierung des Anonymisierungsbegriffs sowie zur Klärung einiger bisher offener Fragestellungen beitragen und verdient deswegen besondere Aufmerksamkeit. Der bisherige Text adressiert zwar wesentliche Fragen der Diskussion um den Begriff der Anonymität, lässt, aus unserer Sicht, jedoch wichtige Aspekte außen vor, die in dieser Stellungnahme angesprochen werden sollen. Die Stellungnahme erhebt keinen Anspruch auf Vollständigkeit, sondern ist auf bestimmte kritische Punkte fokussiert. Sie gliedert sich wie folgt:

1. Definition der Anonymisierung

Die bisherigen Definitionsversuche des Anonymisierungsbegriffs aus Literatur, Rechtsprechung[1] und einer Stellungnahme der Art. 29 Datenschutzgruppe[2] lassen kein einheitliches Bild entstehen. Der vorliegende Text geht ohne eine Auseinandersetzung mit diesen, teilweise unterschiedlichen, Ansichten davon aus, dass eine Anonymisierung „in der Regel als ausreichend" betrachtet wird, wenn „der Personenbezug derart aufgehoben wird, dass eine Re-Identifizierung praktisch nicht durchführbar ist, weil der Personenbezug nur mit einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften wiederhergestellt werden kann".[3]

Vor dem Hintergrund der zahlreichen technischen Möglichkeiten und der verschiedenen Abstufungen der Entfernung des Personenbezugs wäre allerdings eine tiefergehende Auseinandersetzung mit den bisher verfügbaren Definitionsansätzen notwendig. Hierbei wären vor allem die unterschiedlichen technischen Ansätze mit ihren Garantien zu berücksichtigen und die Tatsache dass mit Ausnahme von Ansätzen zur differentiellen Privatsphäre keine Möglichkeiten bekannt sind, Garantien über die Wirksamkeit einer Anonymisierung zu geben. Außerdem wäre der Kenntnisstand zu berücksichtigen, dass es für Verhaltensdaten, um die es sich im benannten Fall der TK-Branche üblicherweise handelt (Geodaten, Verkehrsdaten, DNS-/Webseitenaufrufe), derzeit kaum Ansätze zur wirksamen Anonymisierung gibt, da sie starke interne Abhängigkeiten und Regelmäßigkeiten besitzen[4], die eine Re-Identifikation inhärent ermöglichen. Darauf aufbauend, oder sich abgrenzend, kann ein Begriffsverständnis erarbeitet werden.

So schlägt z.B. die **Artikel-29-Datenschutzgruppe** in ihrer Stellungnahme zu Anonymisierungstechniken einen höheren Schwellenwert für eine erfolgreiche Anonymisierung vor: „... das Ergebnis der Anonymisierung als ein auf personenbezogene Daten angewandtes technisches

[1] Vor allem EuGH, Urt. v. 19.10.2016, Az. C-582/14 – Breyer –, Rn. 46-47.

[2] *Art.-29-Datenschutzgruppe*, Stellungnahme 5/2014 (WP 216) zu Anonymisierungstechniken, S. 5 ff – https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec4.

[3] Entwurf des BfDI-Positionspapiers, S. 5.

[4] Vgl. z.B. *De Monjtoye et al.*, „Unique in the Crowd: The privacy bounds of human mobility" für Geolokation, *Deusser et al.*, "Browsing Unicity: On the Limits of Anonymizing Web Tracking Data" für Verkehrsdaten.

Verfahren nach dem aktuellen Stand der Technik so dauerhaft sein sollte wie eine Löschung, d. h., es darf nicht möglich sein, die personenbezogenen Daten weiter zu verarbeiten".[5]

In der **DSGVO** selbst finden sich vor allem in EWG 26 Angaben zur Anonymisierung, die auch teilweise im Text wiedergegeben sind. Informationen, „die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen", sind danach personenbezogene Daten. Bei der Frage, ob ein Datum als anonym betrachtet werden kann, sind dann „alle Mittel" zu berücksichtigen, „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".[6] Es kommt also auf das vorhandene mögliche Zusatzwissen des Verantwortlichen an, wobei auch Faktoren wie die „Kosten der Identifizierung und der dafür erforderliche Zeitaufwand" und „die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen eine Rolle spielen".[7] Maßgeblich ist daher für die Bestimmung, ob personenbezogene Daten vorliegen, der Umstand, ob der Verantwortliche in der Lage ist, die Daten und sein erreichbares Zusatzwissen zu nutzen, um die betroffene Person zu identifizieren.

Dieses Zusatzwissen Dritter ist dem Verantwortlichen nach dem **EuGH Urteil *Breyer*** dann zurechenbar, wenn das Zusatzwissen des Dritten „ein Mittel darstellt, das vernünftigerweise zur Bestimmung der betreffenden Person eingesetzt werden kann".[8] Dieses verfügbare Zusatzwissen kann jedoch von Verantwortlichem zu Verantwortlichem unterschiedlich sein. Es ist also eine Risiko(wahrscheinlichkeits)prognose zu erstellen. Weiter ist entscheidend, ob die Identifizierung der Person „gesetzlich verboten oder praktisch nicht durchführbar" ist.[9] Existiert eine rechtliche Möglichkeit, den Personenbezug wiederherzustellen, handelt es sich nicht um anonyme Daten.[10]

Auch wenn sich dieser Fall zunächst nur auf dynamische IP-Adressen bezieht, hat er für weitergehende Diskussionen gesorgt. Insbesondere ist **unklar**, ob die Verwendung *rechtswidriger*

[5] *Art.-29-Datenschutzgruppe*, WP 216 (Fn. 2), S. 6/7.

[6] EWG 26 S. 3 DSGVO.

[7] EWG 26 S. 4 DSGVO.

[8] EuGH (Fn. 1) – Breyer –, Rn. 45.

[9] EuGH (Fn. 1) – Breyer –, Rn. 46; siehe dazu auch die ausführliche Diskussion*: Klar/Kühling,* in: Kühling/Buchner, DSGVO/BDSG Kommentar (2. Auflage 2018), Art. 4 DSGVO, Rn. 25 ff.

[10] EuGH (Fn. 1) – Breyer.

Mittel ganz zu vernachlässigen ist (wenn z.B. eine gewisse Wahrscheinlichkeit des Einsatzes besteht)[11] oder ob ein gesetzliches Verbot auch in allen anderen Zusammenhängen den Personenbezug entfallen lassen soll. Letzteres wäre sehr weitgehend und das geplante Positionspapier könnte wertvolle Hinweise in Bezug auf die Fragen, welche Anforderungen an die Berücksichtigung des Wissens und die Mittel Dritter zu stellen sind, und wann für welche Beteiligten eine Anonymisierung gegeben ist, geben. In der Praxis stehen häufig rechtlich nicht gestattete, aber technisch leicht umzusetzende Maßnahmen zur Wiederherstellung des Personenbezugs zur Verfügung. Bei der Beurteilung der Re-Identifikations-Möglichkeiten eines Verarbeiters sollten daher nicht nur dessen rechtlich zulässige sondern auch die für ihn technisch möglichen Maßnahmen betrachtet werden.

2. Risiko der (Re-)Identifizierung

Aus den obigen Ausführungen ergibt sich, dass der Personenbezug eines Datums kontext- und personenabhängig ist und somit regelmäßig überprüft werden muss, ob ein Datum (noch) als anonym bewertet werden kann. Dabei ist vor allem in Betracht zu ziehen, dass der Personenbezug im Rahmen der Anonymisierung dynamisch und **risikoabhängig** zu bestimmen ist und eine Änderung der Situation auch zu einer Änderung des Risikos der (Re-)Identifizierung führen kann. Diese wird beispielsweise vom Wissen Dritter, dem Zeitverlauf oder von neuen Entwicklungen der (De-)Anonymisierungstechniken beeinflusst.[12] Eine einmalige Risikoanalyse ist somit unzureichend. Dieser risikobasierte Ansatz findet im bisherigen Positionspapiervorschlag keine Berücksichtigung. Stattdessen wird sich stark auf die Unterscheidung in personenbezogen und anonym fokussiert, ohne Kriterien zur genaueren Bestimmbarkeit der Anonymisierung zu thematisieren. Grundsätzlich unterliegt die Entscheidung zur Anonymisierung einer Reihe von Unsicherheiten – nicht zuletzt, weil die relevanten technischen und sozialen Umstände im Laufe der Zeit raschen Änderungen unterworfen sind. Als Folge dieser Tatsache kann trotz einer Anonymisierung ein Restrisiko für die betroffene Person verbleiben.[13] Um mit diesem Restrisiko sinnvoll umzugehen, sollte der

[11] *Klar/Kühling,* in: Kühling/Buchner, DSGVO/BDSG Kommentar (Fn. 9), Art. 4 DSGVO, Rn. 29.

[12] Siehe auch *Art- 29-Datenschutzgruppe*, WP 216 (Fn. 2), S. 10.

[13] *Art.-29-Datenschutzgruppe*, WP 216 (Fn. 2), S. 7, 28, 29.

risikobasierte Ansatz des europäischen Datenschutzrechts eine Rolle spielen.[14] Danach kann es, in bestimmten Fällen und trotz einer Anonymisierung, notwendig sein, bestimmte Anforderungen der DSGVO einzuhalten um einen adäquaten Schutzstandard für die betroffenen Personen zu gewährleisten. Ein Beispiel sind KI-Verarbeitungen mit größeren anonymisierten Datensätzen, die es zumindest stark erschweren, ein künftiges Re-Identifizierungsrisiko abzuschätzen. Aufgrund dieser Unsicherheit und des verbleibenden Restrisikos für die betroffenen Personen[15] könnte es in bestimmten Fällen angemessen sein, Grundsätze der DSGVO einzuhalten. Das Positionspapier könnte sich mit dem hier genannten risikobasierten Ansatz und der Anwendung der DSGVO im Rahmen des Re-Identifizierungsrisikos nach einer erfolgten Anonymisierung auseinandersetzen.

3. Abgrenzung zur Pseudonymisierung

Vor dem Hintergrund des genannten Re-Identifizierungsrisikos, und um Missverständnissen und Begriffsunklarheiten vorzubeugen, ist die **Abgrenzung zur Pseudonymisierung**, die teilweise anonymisierende Wirkung haben kann[16], unerlässlich. Insbesondere bestehen in diesem Zusammenhang Unsicherheiten, die u.a. die grundsätzliche Klassifizierung von pseudonymisierten Daten als personenbezogene Daten oder die Einstufung von technischen und organisatorischen Maßnahmen, die als Pseudonymisierungsmaßnahmen und nicht als Anonymisierungsmaßnahmen gelten, betreffen.[17] Angesichts der bestehenden Unsicherheiten und des Umstands, dass unterschiedliche rechtliche Wirkungen bei mehreren Verantwortlichen durch unterschiedliches verfügbares Zusatzwissen eintreten können, ist eine stufenbasierte Unterscheidung der anonymisierenden bzw. pseudonymisierenden Wirkung notwendig. Der Verantwortliche unterliegt also risikoabhängigen Pflichten, die unterschiedlich betrachtet werden müssen. Das geplante Positionspapier könnte sich mit dem Unterschied zwischen pseudonymisierten und anonymisierten Daten sowie den jeweils vorzunehmenden technischen Maßnahmen zur besseren Abgrenzung und Unterscheidung auseinandersetzen und dadurch Klarheit in diese Diskussion bringen.

---

[14] Siehe exemplarisch *Art.-29-Datenschutzgruppe*, Statement on the role of a risk-based approach in data protection legal frameworks (WP 218) – https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf.

[15] *Art.-29-Datenschutzgruppe*, WP 216 (Fn. 2), S. 7, 28, 29.

[16] Siehe *Roßnagel*, ZD 2018, 243 ff.

[17] Siehe nur *Murby/Mackey/Elliot et. al.*, Computer Law and Security Review Vol. 34 (2018), 222 (224 f).

Vor diesem Hintergrund wäre auch eine Auseinandersetzung mit neuen und zukünftigen technologischen Entwicklungen notwendig, wie beispielsweise dem Einsatz künstlicher Intelligenz, der Verwendung von Trainingsdatenbanken oder auch mit Model-Inversion Attacks[18] und deren Auswirkungen auf die Anonymisierung. Letztlich wäre es auch erforderlich zu klären, wann und innerhalb welchen Zeitraums Daten nicht anonymisiert werden dürfen, um beispielsweise die Ausübung des Auskunftsrechts zu ermöglichen.[19]

4. Anonymisierung in der Forschung

Auch wenn der Schwerpunkt des geplanten Positionspapiers auf der Anonymisierung im TK-Sektor liegen soll, findet sich dennoch die generalisierende Aussage, dass für „viele Forschungsprojekte" die „Analyse von Datensätzen ausreichend (ist), deren abstrakter Gehalt erhalten bleibt, der Personenbezug jedoch aufgehoben wird".[20] Für viele Forschungsvorhaben wird jedoch die Arbeit mit und die **(Nach-)Nutzung von gerade nicht anonymisierten Daten** immer wichtiger. Unter anderem aus diesen Gründen profitiert die Forschung von den in Art. 89 DSGVO und § 27 BDSG genannten Ausnahmen bei der Datennutzung und Verarbeitung. Daher wird angeregt, über diese sehr generalisierende Aussage in einem endgültigen Positionspapier nachzudenken. Letzteres könnte auch zur Klärung der Frage nach der Anwendbarkeit der DSGVO auf Forschungsdatensätze beitragen und unterschiedlichen Auslegungen des Anonymisierungsbegriffs in der Forschung[21] entgegentreten.

5. Rechtsgrundlage für die Weiterverarbeitung / Verhältnis von Art. 5(1)(b), 6(4) und EWG 50 DSGVO

Der vorliegende BfDI-Entwurf bietet eine nicht unumstrittene Auslegung von Art 5(1)(b), Art. 6(4) und EWG 50 DSGVO an: „Eine anschließende Anonymisierung stellt deshalb in diesen Fällen eine Weiterverarbeitung dar, deren Zweck mit dem ursprünglichen Erhebungszweck vereinbar sein muss,

---

[18] Siehe *Zhang, Y., Jia, R., Pei, H., Wang, W., Li, B., & Song, D.X.* (2019). The Secret Revealer: Generative Model-Inversion Attacks Against Deep Neural Networks. ArXiv, abs/1911.07135.

[19] EuGH, Urt. v. 7.5.2009, Az. C-553/07 – Rijkeboer –, Rn. 70.

[20] Entwurf des BfDI-Positionspapiers, S. 3.

[21] Bsp. für unterschiedliche Definitionsansätze: *Runge*, „Digitalisierung, Datenschutz, Impact: RatSWD debattiert aktuelle EU-Wissenschaftspolitik" in Informationsdienst Wissenschaft, 16.7.2018 – https://idw-online.de/de/news699425; *Murby/Mackey/Elliot et. al.* (Fn. 17), 222 (225 ff).

vgl. Art. 5 Abs. 1 Buchst. b) DSGVO. Ist diese Vereinbarkeit gegeben, ist die Rechtsgrundlage für die zweckändernde Weiterverarbeitung weiterhin die Rechtsgrundlage, die die ursprüngliche Verarbeitung legitimiert hat, vgl. Erwägungsgrund 50 Satz 2 DSGVO".[22]

Diese Auslegung entspricht zwar dem Wortlaut des EWG 50 DSGVO, lässt jedoch außer Acht, dass nach **europäischem Rechtsverständnis** die Erwägungsgründe nur Auslegungshilfe bei der Interpretation einer Verordnung sind und diese im Kontext des europäisches Datenschutzrechtes, d.h. im Lichte der Entstehungsgeschichte und vor dem Hintergrund der Charta der Grundrechte der EU, ausgelegt werden müssen.[23] Die bisher im Entwurf des Positionspapiers getroffene Auslegung widerspricht u.a. der kürzlich vom Europäischen Datenschutzbeauftragten (EDPS) veröffentlichten Argumentation, nach der EWG 50 nicht die in Art. 8 der Charta beschriebene Pflicht, dass jede Verarbeitung „mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage [legitimiert werden sollte]", aufheben kann.[24] Ein endgültiges Positionspapier sollte die genannten Ansichten in Betracht ziehen und begründen – wenn die bisherige Interpretation beibehalten wird – warum die Auslegung von EWG 50 auf den reinen Wortlaut reduziert wird.

Unter diesem Aspekt sei auf die **Differenzierung hinsichtlich der Weiterverarbeitung** von personenbezogenen Daten aus einem Vertragsverhältnis i.S.d. Art. 6(1)(b) DSGVO hingewiesen, der sich im Entwurf exemplarisch gewidmet wird. So weist lt. BfDI die Anonymisierung der Daten zu Analysezwecken und zur Verbesserung eigener Services einen engen Zusammenhang mit dem eigentlichen Vertragszweck des Art. 6(1)(b) DSGVO auf.[25] Übersehen wird dabei aber die, auch in der Literatur bereits diskutierte[26], davon abweichende Zielrichtung der Regelung: Die Rechtsgrundlage des Vertragsverhältnisses dient zur beiderseitig bewussten Datenverarbeitung im Rahmen des festgelegten Vertragszwecks und -verhältnisses. Mithin manifestiert der Vertrag als solches die

[22] Entwurf des BfDI-Positionspapiers, S. 6/7.

[23] Siehe auch EDPS, Stellungnahme *„A Preliminary Opinion on data protection and scientific research"*, S. 22-23 – https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf.

[24] EDPS, Stellungnahme (Fn. 23), S. 22-23.

[25] Entwurf des BfDI-Positionspapiers, S. 7.

[26] *Buchner/Petri*, in: Kühling/Buchner, DSGVO/BDSG-Kommentar (Fn. 9), Art. 6 DSGVO, Rn. 42 f; *Schantz*, in: Simitis/Hornung/Spiecker gen. Döhmann, Art. 6 DSGVO, Rn. 24 f; vgl. Albers/Veit, in: Wolff/Brink, BeckOK Datenschutzrecht, Art. 6 DSGVO, Rn. 30 f.

Selbstbestimmung und (datenschutzrechtliche) Privatautonomie. Wird das auf dieser Grundlage erhobene Datum anonymisiert und über den Vertragsrahmen hinaus zur Verbesserung eigener Services genutzt, kann dies schon mangels einer Vereinbarung beider Vertragsparteien nicht Gegenstand des Art. 6(1)(b) DSGVO sein. Dass dies zumindest mittelbar beide Vertragspartner tangiert, ändert hieran nichts. Eine Verbesserung des Services verkörpert überwiegend wirtschaftliche Interessen des Dienstleisters, welche höchstens als berechtigtes Interesse i.S.d. Art. 6(1)(f) DSGVO zu qualifizieren wären. Das im Entwurf angeführte Beispiel eignet sich daher nicht durchgehend oder müsste konkret auf einen Vertragsschluss zur Verbesserung des Services gerichtet sein. Ein derartiges praxisrelevantes Beispiel lässt sich aber angesichts anderer, im Einsatz befindlicher Praktiken schwer finden.

Positiv anzuerkennen ist dagegen, dass sich dem Aspekt der Zweckänderung bzw. Weiterverarbeitung gem. Art. 5(1)(b), 6(4) DSGVO und der schrittweisen Prüfung gewidmet wird. Wünschenswert wären aber inhaltlich geeignete Positiv- und Negativ-Beispiele zugunsten einer Verständlichkeit der Regelungen für die Öffentlichkeit, insbesondere für den Forschungsbereich.

6. Gleichsetzung von Löschung und Anonymisierung

Der Entwurf des Positionspapiers enthält eine Gleichsetzung von Löschung und Anonymisierung. Es wird argumentiert: „Soweit die personenbezogenen Daten der Pflicht zur unverzüglichen Löschung gemäß Art. 17 Abs. 1 DSGVO unterfallen, können diese ggf. auch gemäß Art. 6 Abs. 1 Buchst. c) DSGVO anonymisiert werden. Dies ist unter der Prämisse möglich, dass die Anonymisierung dem Löschen gleichgesetzt werden kann“.[27] Angeführt wird hierfür eine Entscheidung der österreichischen Datenschutzbehörde, die in einem Verfahren eine erfolgte Anonymisierung mit einer Löschung nach Ausübung des Löschungsrechts gem. Art 17(1) DSGVO gleichsetzt.

Die im Entwurf des Positionspapiers dargelegte Argumentation ist aus unterschiedlichen Gründen wenig überzeugend. So wird nicht nur die **Schutzrichtung des Löschungsrechts** vernachlässigt, sondern auch die **Systematik der DSGVO** außer Acht gelassen.

Das Löschungsrecht des Art. 17(1) DSGVO dient in erster Linie der Durchsetzung von grundlegenden Betroffeneninteressen; die Anonymisierung ist eher ein Mittel des Verantwortlichen, seinen

[27] Entwurf des BfDI Positionspapiers S. 8.

Pflichten aus der DSGVO nachzukommen und die Risiken für den Betroffenen zu verringern. Die Schutzrichtung des Rechts auf Löschung kann sich dabei von der Möglichkeit der Anonymisierung unterscheiden. Auch wenn es Fallbeispiele geben mag, in denen die Rechte des Betroffenen durch eine Anonymisierung realisiert werden können, trifft dies nicht pauschal auf alle in Art. 17(1) genannten Möglichkeiten zu. Die Löschung zielt auf „die (faktische) Unmöglichkeit, die zuvor in den zu löschenden Daten verkörperte Information wahrzunehmen".[28] Selbst wenn diese Definition in Teilen einer Anonymisierung entsprechen kann, ist bisher nicht geklärt, welche Anonymisierungstechniken den Personenbezug dauerhaft entfallen lassen, welche Techniken davon mit einer Löschung gleichzusetzen wären und welcher Definition der Anonymisierungsbegriff der DSGVO unterliegt.[29] Ohne eine Auseinandersetzung mit diesen Fragen ist eine Gleichstellung von Anonymisierung und Löschung zum jetzigen Zeitpunkt nicht möglich.

Auch darf das Löschungsrecht als Ausprägung des Rechts auf informationelle Selbstbestimmung[30] nicht in jedem Fall mit einer Anonymisierung gleichgesetzt werden. So liegt z.B. dem Widerruf der Einwilligung[31] des Betroffenen nach Art. 17(1) DSGVO das Recht zu Grunde zu entscheiden, wann und zu welchem Zweck die eigenen personenbezogenen Daten verarbeitet werden dürfen. Die Gründe für die Entscheidung liegen nur bei dem Betroffenen selbst und reflektieren so die digitale Souveränität. Dies beinhaltet auch das Recht „zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden"[32] bzw. ob die Zwecke eines Verarbeiters durch die Verarbeitung der eigenen Daten unterstützt werden sollen. Das Löschungsrecht als Ausprägung des Rechts auf informationelle Selbstbestimmung beinhaltet also auch eine normative Wertung der Betroffenen, ob eine bestimmte Verarbeitung unter Nutzung ihrer Daten stattfinden sollte, oder nicht[33]. Eine „bloße" Anonymisierung der Daten würde diesem Recht nur teilweise entsprechen – da

[28] *Herbst*, in: Kühling/Buchner, DSGVO/BDSG-Kommentar (Fn. 9), Art. 17 DSGVO, Rn. 37.

[29] *Winter/Battis/Halvani*, ZD 2019, 489.

[30] BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983 - 1 BvR 209/83 = BVerfGE 65, 1 (42) noch allgemein. Bestätigt in BVerfG, Urt. v. 6.11.2019, Az. 1 BvR 16/13 – Recht auf Vergessenwerden I –, Rn. 84 f, 90 f.

[31] Siehe hierzu grundlegend *Artikel-29-Datenschutzgruppe*, „Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679" (WP 259 rev.01 2018), S. 4.

[32] BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983 - 1 BvR 209/83 = BVerfGE 65, 1 (42); BVerfG, Urt. v. 6.11.2019, Az. 1 BvR 16/13 – Recht auf Vergessenwerden I –, Rn. 84 f, 90 f.

[33] Hierauf bezugnehmend BVerfG, Urt. v. 6.11.2019, Az. 1 BvR 16/13 – Recht auf Vergessenwerden I –, Rn. 84 f.

nicht deutlich ist, welcher Grad von Anonymisierung gemeint ist und ob Daten auch in einer nicht näher definierten anonymisierten Form weiterhin die Zwecke einer Verarbeitung unterstützen können.[34]

Darüber hinaus wird bei einer Gleichsetzung von Löschung und Anonymisierung die Systematik der DSGVO außer Acht gelassen. Der Entwurf des Positionspapiers erkennt selbst, dass zwischen der Verpflichtung der Speicherbegrenzung nach Art. 5(1)(e) DSGVO und dem Recht auf Löschung nach Art. 17(1) DSGVO unterschieden werden muss[35], deutet dann aber an, dass Art. 5(1)(e) und Art. 17(1)(a) DSGVO auf die gleichen Situationen anwendbar sind: „Art. 17 Abs. 1 Buchst. a) nimmt mithin die in Art. 5 Abs. 1 Buchst. b), c), und e) festgelegten Grundsätze der Zweckbindung und Datenminimierung in Bezug. Das in Art. 5 Abs. 1 Buchst. e) normierte Prinzip der Speicherbegrenzung kann daher Grundlage für einen Anspruch auf Löschung nach Art. 17 Abs. 1 Buchst. a) DSGVO sein.“[36]

Diese Argumentation lässt außer Acht, dass Art. 5(1)(e) DSGVO auf ein viel breiteres Spektrum von Verarbeitungstätigkeiten als Art. 17(1)(a) DSGVO anwendbar ist. Das Löschen oder die Anonymisierung sind jeweils nur eine von mehreren Möglichkeiten, der Verpflichtung aus Art. 5(1)(e) DSGVO nachzukommen und den Personenbezug zu entfernen. Ausdrücklich genannt werden diese Begriffe allerdings in Art. 5(1)(e) DSGVO nicht. Eine irgendwie geartete Wertung für Art. 17(1) (a) oder eine Aussage, welche Form des Löschens i.S.d. Art. 17 relevant ist, ergibt sich daher nicht. Weder bezieht sich Art. Art. 5(1)(e) DSGVO direkt auf Art 17 DSGVO, noch finden sich Ähnlichkeiten im Wortlaut oder der Struktur der Artikel. Wertungen für eine Gleichsetzung des Löschungsrechts mit der Anonymisierung finden sich auch nicht in der Entstehungsgeschichte dieser Artikel. Dass Art. 17 DSGVO Elemente der grundlegenden Datenschutzprinzipien der Zweckbindung, Datenminimierung und Speicherbegrenzung enthält, steht dem nicht entgegen.

[34] Beispiel: Wenn ein Proband nicht mit den moralischen Aspekten einer bestimmten Art der Forschung einverstanden ist und aus diesem Grund seine Einwilligung widerruft, dann würde die Anonymisierung und die weitere Verarbeitung dieser Daten für die gleichen Forschungszwecke gegen die Gründe des Widerrufs wirken. Siehe hierzu *Beyleveld/Histed*, Medical Law International Vol. 4 (2000), 277 ff.

[35] Entwurf des BfDI-Positionspapiers, S. 8.

[36] Entwurf des BfDI-Positionspapiers, S. 9.

Ebenso wenig überzeugend ist die im Entwurf genannte Argumentation, dass die Vernichtung i.S.d. Art. 4 Nr. 2 DSGVO von der Löschung abzugrenzen ist. So führt der Entwurf des Positionspapiers aus, „dass beide Vorgänge – Löschung und Anonymisierung – eine Entfernung des Personenbezugs nach sich ziehen und auch die Löschung nicht zwangsläufig zu einer endgültigen Vernichtung der Daten führt. Dass es sich bei der Löschung und der Vernichtung um zwei alternative Verarbeitungsvorgänge handelt, wird auch durch die Formulierung ‚das Löschen oder die Vernichtung' in Art. 4 Nr. 2 DSGVO klargestellt."[37]

Auch hierin zeigt sich die Schwäche der Gleichsetzung von Löschung und Anonymisierung, wenn ausschließlich auf den Zweck der Entfernung des Personenbezuges und damit aus dem Herrschaftsbereich eines Betroffenen abgestellt wird. Dies mag aus faktischer Perspektive stimmen, verkennt aber die bereits erwähnte Re-Identifizierung und die erwähnte „flexible" Bestimmbarkeit des Anonymitätsgrades. Hiervon unterscheidet sich schon die Löschung im technischen Sinne, da sie von Vornherein nicht nur auf das Entfernen eines oder mehrerer bestimmter Merkmale, sondern auf die vollumfängliche Unlesbarkeit der Daten unabhängig vom Datengehalt gerichtet ist. Kurz: Eine Anonymisierung verfremdet Daten ganz oder teilweise, aber hinterlässt sie lesbar. Eine Löschung hinterlässt – zumindest perspektivisch – unlesbare Daten. Auf den Fakt, dass nach mehrmaligem Überschreiben mit sehr geringer Wahrscheinlichkeit minimale nutzbare Artefakte erhalten bleiben können[38] kann es für das Verständnis des Begriffes der Anonymisierung nicht ankommen. Vielmehr ist der Vorgang der Löschung von der Anonymisierung abzugrenzen – wie der BfDI zutreffend in Art. 4 Nr. 2 DSGVO erkennt – und als digitaler Vernichtungsvorgang zu verstehen. Die Vernichtung i.S.d. Art. 4 Nr. 2 DSGVO definiert sich als physikalischer Vorgang i.S.e. Zerstörung des Datenträgers.[39] Beides sind daher unterschiedliche Begriffe, da es sich um unterschiedliche Handlungen mit unterschiedlichem Restrisiko und damit unterschiedlichen Verpflichtungen nach der DSGVO handelt.

[37] Entwurf des BfDI-Positionspapiers, S. 9 f.

[38] *Wright, C., Kleiman, D., and Sundhar RS, S.* "Overwriting hard drive data: The great wiping controversy", International Conference on Information Systems Security. Springer, Berlin, Heidelberg, 2008.

[39] *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann, DSGVO/BDSG-Kommentar (Fn. 26), Art. 4 Nr. 2 DSGVO, Rn. 33; *Schild*, in: Wolff/Brink, BeckOK Datenschutzrecht (Stand: 1.11.2019), Art. 4 DSGVO, Rn. 53 und 56.

Anonymisierung, Löschung und Vernichtung weisen in dieser Reihenfolge ein abnehmendes Restrisiko für die Interessen des Betroffenen auf.

7. Technische Aspekte

Im Entwurf des Positionspapiers fehlen **Hinweise auf geeignete (oder ungeeignete) Anonymisierungstechniken**. Das Positionspapier könnte wertvolle Orientierung geben, indem es Leitfragen zur Bestimmung geeigneter Anonymisierungsverfahren formuliert sowie Kriterien zur Bestimmung angemessener Verfahrensparameter (z.B. geeignete Werte für k im Kontext der k-Anonymität) thematisiert. Vorbild könnte die vom Bundesamt für Sicherheit in der Informationstechnik herausgegebene und regelmäßg aktualisierte Technische Richtlinie „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“[40] sein, die für kryptogaphische Verfahren entsprechende Empfehlungen gibt.

Prof. Dr. Franziska Boehm
Bereichsleiterin
Immaterialgüterrechte
FIZ Karlsruhe – Leibniz Institut
für Informationsinfrastruktur
Hermann-von Helmholtz-Platz 1
76344 Eggenstein-Leopoldshafen
Karlsruhe Institute of Technology,
Zentrum für angewandte
Rechtswissenschaft (ZAR)

Prof. Dr. Thorsten Strufe
Institut für Praktische
Sicherheit
Karlsruhe Institute of
Technology
Am Fasanengarten 5
76131 Karlsruhe

Prof. Dr. Michael Meier
Universität Bonn
Lehrstuhl IT-Sicherheit
Institut für Informatik
Endenicher Allee 19A
53115 Bonn

[40] BSI, Technische Richtlinie BSI TR-02102-1 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“, Version: 2019-01 – https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf.