bitkom

Auf einen Blick

BfDI Konsultation zur Anonymisierung

Ausgangslage

Am 10. Februar veröffentlichte der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ein Positionspapier zur Anonymisierung unter der Europäischen Datenschutz-Grundverordnung (DS-GVO) und startete den öffentlichen Konsultationsprozess hierzu.

Bitkom-Bewertung

Geht in die richtige Richtung: Aus unserer Sicht enthält das Konsultationspapier einige richtige Ansätze, bedarf jedoch an einigen Stellen dringend noch weiterer Ausführungen und inhaltlicher Anpassungen. Aus unserer Sicht sollten in die Positionierung des BfDI aus dieser Konsultation einige wesentliche Klarstellungen Eingang finden. **Unser Ziel ist** mehr Rechtssicherheit für Anwender. Wir halten ausdefinierte Kriterien für notwendig, die bei der Beantwortung der Frage helfen, wann eine Anonymisierung vorliegt. Der Erarbeitungsprozess sollte bereits hier mit der Konsultation angestoßen werden und dann entlang der verschiedenen Anonymisierungsmethoden, Anwendungsfeldern und Datengruppen spezifiziert werden.

Das Wichtigste

Im Bitkom sind neue Anbieter genauso wie Mitglieder mit großer Nähe zu den klassischen Diensten vertreten. Unser Papier zeichnet daher mögliche Kompromisslinien vor:

- **Relativer statt absoluter Anonymisierungsbegriff**
  Wir begrüßen, dass das Konsultationspapier sich klar für den relativen statt den absoluten Anonymisierungsbegriff positioniert.
- **Verarbeitung und Rechtsgrundlage**
  Wir sehen keine triftigen juristischen Gründe für die geänderte Auffassung, dass die Anonymisierung eine Verarbeitung i.S.d. DS-GVO ist. Selbst wenn die Anonymisierung als Verarbeitung bewertet wird, bedarf sie jedenfalls keiner (gesonderten) Rechtsgrundlage. Vielmehr ist die Anonymisierung als Ausprägung der datenschutzrechtlichen Grundprinzipien der Datenminimierung privilegiert und damit stets auch ohne Rechtsgrundlage zulässig.
- **Definition von Bedingungen und Kriterien**
  Statt den Vorgang der Anonymisierung in rechtlich nicht passende DS-GVO Kriterien zu fassen, wäre es für alle Beteiligten dienlicher präzise zu definieren, unter welchen Bedingungen von einer erfolgreichen Anonymisierung auszugehen ist.

Stellungnahme

BfDI Konsultation – Anonymisierung unter der DS-GVO unter besonderer Berücksichtigung der TK-Branche

23.März 2020

1. Zusammenfassung

Am 10. Februar veröffentlichte der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ein Positionspapier zur Anonymisierung unter der Europäischen Datenschutz-Grundverordnung (DS-GVO) und startete den öffentlichen Konsultationsprozess hierzu. Bitkom bedankt sich ausdrücklich für die Gelegenheit zur Stellungnahme. Die Anonymisierung ist vor dem Hintergrund der strategischen Relevanz personenbezogener Daten für datengetriebene Geschäftsmodelle einerseits sowie für die sekundäre Nutzung im Rahmen der Digitalisierung anfallender (personenbezogener) Daten andererseits einer der zentralen Aspekte rund um die Anwendung der DS-GVO. Der Mehrwert anonymisierter Daten liegt auf der Hand: Im Bereich der Forschung, etwa für das Trainieren von Künstlicher Intelligenz (KI) oder für die Entwicklung von Produkten können auch ohne personenbezogene Daten signifikante Fortschritte erzielt werden. Diese sind essentiell für die Datenökonomie und damit auch für das Gelingen der deutschen und europäischen Datenstrategie. Auch der mit der KI-Strategie angestoßene Kurs, nämlich die Förderung von KI-Anwendungen und der Aufbau Deutschlands und Europas als Exzellenzzentrum für KI werden nur gelingen, wenn Daten für das Trainieren von KI nutzbar sind. Anonymisierung ist eine der vielversprechendsten Lösungen, um diese Anforderung mit den berechtigten Interessen des Datenschutzes in Einklang zu bringen. Die politische Bedeutung der Diskussion rund um die Anonymisierung könnte daher kaum höher sein.

Aus unserer Sicht enthält das Konsultationspapier einige richtige Ansätze, bedarf jedoch an einigen Stellen dringend noch weiterer Ausführungen und inhaltlicher Anpassungen. Aus unserer Sicht sollten in die Positionierung des BfDI aus dieser Konsultation einige wesentliche Klarstellungen Eingang finden.

Ohne mehr Praktikabilität und Klarstellungen liegt die (weitere) Zurückhaltung gegenüber Investitionen in Anonymisierungsverfahren auf der Hand und die Innovation treibende Kraft hinter der Implementierung datenschutzfreundlicher Verfahren wird gehemmt. Denn ohne ausreichende Gewissheit darüber, (i) wann ein anonymisiertes Datum nach Ansicht der Aufsichtsbehörden vorliegt, (ii) wie eine Anonymisierung

Bitkom
Bundesverband
Informationswirtschaft,
Telekommunikation
und Neue Medien e.V.

Rebekka Weiß, LL.M.
Leiterin Vertrauen & Sicherheit
T +49 30 27576 161
r.weiss@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Achim Berg

Hauptgeschäftsführer
Dr. Bernhard Rohleder

im Einklang mit der DS-GVO erreicht werden kann und (iii) welche Eigenschaften eine zulässige technische Realisierung der Anonymisierung beinhaltet, werden Investitionsentscheidungen nicht getroffen werden.

Wir halten vor diesem Hintergrund ausdefinierte Kriterien für notwendig, die den Anwendern bei der Beantwortung der Frage helfen, wann eine Anonymisierung vorliegt. Der Erarbeitungsprozess sollte bereits hier mit der Konsultation angestoßen werden und dann entlang der verschiedenen Anonymisierungsmethoden, Anwendungsfeldern und Datengruppen spezifiziert werden. Im Rahmen dessen sollten auch die nach der DS-GVO in den Artikeln 40ff. vorgesehenen Möglichkeiten in Betracht gezogen werden.

Im Rahmen des Konsultationsverfahrens und der daraus resultierenden Positionierung des BfDI weisen wir daher auf folgende Kernaspekte hin:

- Wir begrüßen, dass das Konsultationspapier sich klar für den relativen statt den absoluten Anonymisierungsbegriff positioniert.
- Wir begrüßen, dass Anonymisierung als wirkgleiches Mittel der Löschung anerkannt wird.
- Wir sehen keine triftigen juristischen Gründe für die geänderte Auffassung, dass die Anonymisierung eine Verarbeitung i.S.d. DS-GVO ist.
- Selbst wenn die Anonymisierung als Verarbeitung bewertet wird, bedarf sie jedenfalls keiner (gesonderten) Rechtsgrundlage. Vielmehr ist die Anonymisierung als Ausprägung der datenschutzrechtlichen Grundprinzipien der Datenminimierung privilegiert und damit stets auch ohne Rechtsgrundlage zulässig.
- Sofern eine Rechtsgrundlage tatsächlich für notwendig gehalten wird, zeigt eine detaillierte Prüfung des Gesetzes, dass die Rechtsgrundlagen zum Anonymisierungsvorgang nicht passen.
- Hierbei darf vor allem nicht aus dem Blick geraten, dass im Anwendungsbereich von Art. 9 DS-GVO eine Anonymisierung nur in den engen Grenzen des Art. 9 Abs. 2 DS-GVO möglich wäre, was aus gesellschaftspolitischen Gründen nicht gewünscht sein kann.
- Im Interesse der Wettbewerbsfähigkeit deutscher Unternehmen und einer verbesserten Nutzung anonymisierter Daten im europäischen Datenraum, halten wir es für erforderlich, dass sich der BfDI für eine Harmonisierung auf europäischer Ebene einsetzt.
- Es bedarf einer Klarstellung, dass die Anonymisierung rechtmäßig erhobener personenbezogener Daten auch vor Ablauf der festgelegten Speicherdauer jederzeit zulässig ist.

- Wir halten es außerdem für erforderlich erneut zu betonen, dass anonymisierte Daten nicht der DS-GVO unterfallen, da im Konsultationspapier die Grenzen der Anwendbarkeit zu verschwimmen drohen.
- Statt den Vorgang der Anonymisierung unbedingt der DS-GVO zuzuordnen wäre es für alle Beteiligten dienlicher präzise zu definieren, unter welchen Bedingungen von einer erfolgreichen Anonymisierung auszugehen ist.

2. Details zum Konsultationspapier

Nachfolgend möchten wir auf die oben angesprochenen Einschätzungen näher eingehen.

2.1. Warum die Anonymisierung keine Verarbeitung im Sinne der DS-GVO sein kann

Bei Auslegung der DS-GVO nach dem Normzweck, dem Wortlaut und auf systematische Weise, können wir die Annahme, dass es sich bei der Anonymisierung um eine Verarbeitung im Sinne der DS-GVO handelt, nicht nachvollziehen.

Schutzzweck der DS-GVO ist das Recht des Einzelnen auf informationelle Selbstbestimmung. Durch die Anonymisierung wird dem Schutzzweck Rechnung getragen, indem der Personenbezug oder die Personenbeziehbarkeit von Daten entfernt wird und damit die Gefahr einer Verletzung der Privatsphäre verhindert wird. Eine Verletzung des Einzelnen in seinem Recht auf informationelle Selbstbestimmung ist ausgeschlossen.

Der Schutzzweck der DS-GVO erstreckt sich nicht auf anonymisierte Daten, die zuvor personenbezogene oder personenbeziehbare Daten waren. Daher entfallen hier auch alle Rechte der betroffenen Personen, die sich aus der DS-GVO ergeben: z. B. das Widerrufs bzw. Widerspruchsrecht, das Recht auf Information oder auf Löschung.

Das Konsultationspapier selbst stellt in seiner Einleitung klar: »Die Anonymisierung kann auch als ein Mittel angesehen werden, im Einzelfall eine Verarbeitung von Daten gar erst zu ermöglichen, wenn die Verarbeitung bei bestehendem Personenbezug datenschutzrechtlich unzulässig wäre«. Die Anonymisierung wird also ganz im Sinne der Grundsätze aus Art. 5, 32 DS-GVO als Maßnahme bzw. als Erfordernis im Rahmen einer risikobasierten Ausgestaltung der DS-GVO verstanden, die eine Verarbeitung erst ermöglicht. Damit ist sie – lediglich – eine technische Bedingung für eine (intendierte) Datenverarbeitung. Die Anonymisierung wird Bestandteil dieser Datenverarbeitung und bedarf daher keiner eigenständigen Rechtsgrundlage. Exakt diesen Gedankengang legt auch Erwägungsgrund 26 DS-GVO offen: Mit den Ausführungen in Erwägungsgrund 26 DS-GVO stellt der Gesetz-

geber klar, dass er keinerlei Anlass sieht, anonyme Daten und deren Nutzung datenschutzrechtlich zu reglementieren. Diese Aussage bezieht er sowohl auf Daten, die schon originär nicht personenbeziehbarer Natur sind, als auch auf solche die nach dem Durchlaufen eines entsprechenden Verfahrens anonym geworden sind. Unabhängig von der Frage, weshalb Daten anonym (geworden) sind, entziehen sie sich vollständig der datenschutzrechtlichen Bewertung und lassen sich insbesondere im Hinblick auf mit ihnen verfolgten Zwecke nicht am Maßstab datenschutzrechtlicher Normen messen. Das ist auch nur konsequent: Über die Prüfung von Tatbestandsmerkmalen einer datenschutzrechtlichen Rechtsgrundlage wird im Einzelfall ein Ausgleich zwischen dem Grundrecht auf informationelle Selbstbestimmung bzw. dem Grundrecht auf Datenschutz einerseits und den grundrechtlich verbürgten wirtschaftlichen Interessen der Unternehmen herbeigeführt (Praktische Konkordanz). Für Praktische Konkordanz besteht aber in Fällen anonymisierter Daten kein Anlass, weil mit ihnen kein Eingriff in grundrechtlich geschützte Positionen verbunden ist. Insofern besteht kein Erfordernis für eine Rechtsgrundlage.

Indiziert die Verarbeitung anonymer Daten also keinerlei Erfordernis normativer datenschutzrechtlicher Kontrolle, ist kein Grund erkennbar, weshalb derjenige technische Vorgang, mit welchem personenbezogene Daten in den Zustand der Anonymität versetzt werden, seinerseits datenschutzrechtlich überlagert werden muss – freilich mit der Maßgabe, dass das entsprechende technische Verfahren am Maßstab des relativen Anonymitätsbegriffs in zuverlässiger Weise zum Zustand anonymer Daten führt.

Die Anonymisierung ist ein Mittel, welches den Schutz der Grundrechte natürlicher Personen gewährleistet. Dieses Mittel als Verarbeitung zu charakterisieren und für diese Verarbeitung eine Rechtsgrundlage zu fordern, erscheint geradezu paradox. Vielmehr sollte die Anonymisierung schon gar keine Verarbeitung darstellen. Die Anonymisierung wird deshalb zu Recht nicht als Art der Verarbeitung in Art. 4 DS-GVO aufgeführt. Sie erfüllt vielmehr den Schutzzweck der DS-GVO als eine technische Maßnahme, die eine Verarbeitung und damit Nutzung personenbezogener Daten reduziert.

Gegen die Anonymisierung als Verarbeitung spricht auch der Wortlaut der DS-GVO. Die Anonymisierung wird – anders als beispielsweise die Pseudonymisierung – in der DS-GVO nirgends als Verarbeitung definiert. Hätte der Gesetzgeber die Anonymisierung als Verarbeitung angesehen, leuchtet es nicht ein, dass er diese in Art. 4 DS-GVO nicht als Verarbeitung definiert hat. Dies hätte er entweder in Art. 4 Nr. 2 DS-GVO oder als extra Punkt entsprechend der Pseudonymisierung in Art. 4 Nr. 5 DS-GVO tun können.

Da Art. 4 die Löschung aufführt, sei an dieser Stelle erwähnt, dass Anonymisierung nicht unter den Begriff »löschen« subsummiert werden kann, da der Anonymisierungs-Vorgang nicht zwingend die Löschung der originären personenbezogenen Daten zur Folge hat – es entstehen andere, anonymisierte Daten und die originären personenbezogenen Daten können weiterhin vorhanden sein, wenn sie nicht explizit gelöscht werden. Anonymisierung fällt auch nicht unter den Begriff »verändern«, denn hier werden die Daten manipuliert und erhalten dadurch bei gleicher Form eine andere Aussagekraft oder anderen Wahrheitsgehalt.

Unter der DS-GVO ist es nicht zu einer grundlegenden Änderung des Verarbeitungsbegriffs gekommen, welcher der Datenschutzrichtlinie 95/46/EG und damit dem deutschen Datenschutzregime rund um das Bundesdatenschutzgesetz 2009 zugrunde lag. Insofern ist die Aussage des BfDI aus seinem 6. Tätigkeitsbericht, S. 170 (»Eine Anonymisierung von Daten gilt nicht als Verarbeitung und ist somit zulässig. Dies gilt auch für sensible Daten, wie etwa Standortdaten von Mobilfunknutzern«.) von höchst aktueller Relevanz. Denn beinhaltet die DS-GVO bereits auf konzeptioneller Ebene eine grundsätzliche Privilegierung der Anonymisierung, besteht kein Anlass, die darin zum Ausdruck kommende datenschutzrechtliche Einschätzung aus der Vergangenheit zu ändern oder auch nur zu relativieren. Vielmehr müssen wir den heutigen Standpunkt des BfDI, eine Anonymisierung bedürfe einer Rechtsgrundlage, grundsätzlich und kritisch hinterfragen.

2.2. Die im Konsultationspapier getroffene Aussage »Die Anonymisierung bedarf immer einer gesonderten Rechtsgrundlage« sehen wir kritisch

Bei der Anonymisierung handelt es sich um eine Ausprägung der datenschutzrechtlichen Grundprinzipien der Datenminimierung und Speicherbegrenzung aus Art. 5 DS-GVO. Deren Umsetzung bedarf keiner Rechtsgrundlage aus der DS-GVO oder sonstiger spezialgesetzlicher Regelungen. Im Gegenteil setzt der Gesetzgeber offenbar voraus, dass diese als gesetzgeberischer Auftrag und Primärpflicht des Verantwortlichen immer umgesetzt werden darf. Eine anderweitige Interpretation kommt nicht nur in argumentations- sondern auch in aussagelogische Widersprüche. Es kann nicht richtig sein, dass der Verantwortliche einerseits personenbezogene Daten nicht länger als nötig speichern darf und diese löschen muss, andererseits aber die Anonymisierung ohne gesonderte Rechtgrundlage unzulässig sein soll.

Dies zeigt sich auch in den praktischen Folgen und Wertungen. Die Anonymisierung ist im Rahmen des Art. 6 Abs. 1 lit. c DS-GVO als wirkgleiches Mittel anerkannt, soweit der Betroffene ein Löschverlangen gem. Art. 17 DS-GVO äußert. Dies gilt und muss erst Recht

gelten in den Fällen, in denen die Löschung aus den allgemeinen Grundsätzen des Art. 5 DS-GVO folgt. Die Relevanz anonymisierter Daten und der gesamtgesellschaftliche Mehrwert daraus abzuleitender allgemeiner Aussagen kann nicht unterschätzt werden. Dies zeigen aktuellste Ereignisse (leider) allzu deutlich. Da es sich hierbei um eine Ableitung der allgemeinen Prinzipien (Datenminimierung) handelt, kann es hierbei auch zu keinen Wertungsunterschieden zwischen Art. 6 und Art. 9 DS-GVO kommen. Wenn überhaupt ergeben sich erhöhte Anforderungen an die Voraussetzungen ab wann (relative) anonyme Daten vorliegen.

Dass eine Anonymisierung auch ohne Rechtsgrundlage möglich sein muss, zeigt sich auch an der ePrivacy Richtlinie (2002/58 EG). In Art. 6 und 9 ePrivacy Richtlinie (Verkehrs- und Standortdaten) wird jeweils festlegt, dass die Daten gelöscht oder anonymisiert werden müssen, sobald sie nicht mehr benötigt werden. Eine Rechtsgrundlage wird aber neben den engen Verarbeitungstatbeständen gerade nicht aufgeführt.

Mit Blick auf Art 6 Abs. 1 lit. e Richtlinie 95/46/EG (= Art. 5 Abs. 1 lit. e DS-GVO) und die Vorschriften der ePrivacy Richtlinie hat die Art. 29-Gruppe den Schluss gezogen, dass personenbezogene Daten zumindest »standardmäßig« anonymisiert werden sollten.

»In itself, this provision makes a strong point that personal data should, at least, be anonymized »by default« (subject to different legal requirements, such as those mentioned in the ePrivacy Directive regarding traffic data).« (0829/14/EN WP216, S. 7).

Würde für diesen Vorgang jeweils eine Rechtsgrundlage, wie etwa die Prüfung der Weiterverarbeitung zu kompatiblen Zwecken oder zur Erfüllung eines berechtigten Interesses gefordert, wäre dies ein rein formalistischer Vorgang. Die Umsetzung der Datenschutzgrundprinzipien wäre immer vereinbar mit dem ursprünglichen Zweck und eine Vereinbarkeitsprüfung obsolet. Entsprechendes gilt bei der Prüfung des berechtigten Interesses. Ein berechtigtes Interesse des Verantwortlichen personenbezogene Daten zu anonymisieren ist aus seinem gesetzlichen Auftrag und seiner Primärpflicht gem. Art. 5 DS-GVO immer anzunehmen. Einer Interessenabwägung bedarf es somit nicht, da ein überwiegendes Interesse des Betroffenen daran, nicht zu anonymisieren – also Klardaten zu verwenden – kaum vorstellbar erscheint. Demzufolge müsste über die Anonymisierung auch nicht gesondert informiert werden.

Vor diesem Hintergrund wäre es – vorausgesetzt eine Rechtsgrundlage wird, wovon wir nicht ausgehen, überhaupt als notwendig erachtet – daher vorzugswürdig, die Anonymisierung als solche als Umsetzung der Datenschutzgrundprinzipien zu privilegieren z. B. über eine Heranziehung des Grundsatzes von Art. 5 Abs. 1 lit. e DS-GVO.

2.3. Die Rechtsgrundlagen der DS-GVO passen nicht zum Anonymisierungsvorgang

Unterstellt man aber einmal, dass die Anonymisierung einer eigenen Rechtsgrundlage bedarf, so offenbart gerade die Prüfung der in Frage kommenden Varianten des Art. 6 und Art. 9 DS-GVO, dass diese für den Fall der Anonymisierung nicht recht passen wollen und sowohl dogmatische wie auch praktische Fragen aufwerfen.

2.3.1. Rechtsgrundlagen aus Artikel 6 DS-GVO

Die Einwilligung aus Art. 6 Abs. lit a DS-GVO, deren Bedingungen Art. 7 DS-GVO klar aufzeigt, würde in vielfacher Hinsicht nicht richtig umgesetzt werden können und ist daher entgegen den Ausführungen des BfDI als Rechtsgrundlage für eine Anonymisierung nicht tauglich. So kämen bei einer einwilligungsgetragenen Anonymisierung sowohl die diesbezügliche Dokumentationspflicht als auch die Widerrufbarkeit zu kurz. Um seiner Rechenschaftspflicht aus Art. 5 Abs. 2 DS-GVO nachkommen zu können, müsste der Verantwortliche die Einwilligungserklärung des Betroffenen aufbewahren. Dies würde aber dem Grundgedanken der Anonymisierung, die Re-Identifizierbarkeit aufzuheben, entgegenlaufen. Würde man dagegen verlangen die Einwilligungserklärung zu löschen oder ebenfalls zu anonymisieren, könnte der Verantwortliche im Zweifel nicht beweisen, dass die Anonymisierung rechtmäßig erfolgt ist. Hinsichtlich der Widerrufbarkeit hat das BAG zwar entschieden, dass in bestimmten Fällen ein Widerruf auch treuwidrig sein könne, dies ist jedoch die Ausnahme und merkt man schon hier ganz deutlich, dass der Rechtfertigungsgrund der Einwilligung nicht für die Anonymisierung gemacht worden ist.

Was Art. 6 Abs. 1 lit. f DS-GVO anbelangt, müssen auch hier gleichermaßen systematische wie dogmatische Ungereimtheiten festgestellt werden: Denn wie sollten vor allem die Transparenzanforderungen in der Praxis umgesetzt werden? Gemäß Art. 21 Abs. 1 Satz 1 DS-GVO steht dem Betroffenen ein Widerspruchsrecht zu, welches seinerseits natürlich eine adäquate Information im Sinne der Art. 12 ff. DS-GVO voraussetzt. Dies hätte zur Folge, dass jeder Betroffene vor der Anonymisierung hierüber und über die Interessensabwägung informiert werden müsste. Dann müsste es konsequenterweise eine Art »retardierendes Moment« geben, also einen zeitlichen Verzug, da anderenfalls ein erfolgter Widerspruch nicht mehr berücksichtigt werden könnte. Da es sich hier zudem noch um ein relatives Widerspruchsrecht handelt, könnte es zu einem langwierigen hin und her zwischen Verantwortlichen und widersprechendem Betroffenen kommen. Dies kann offensichtlich vom Gesetzgeber nicht gewollt sein und würde bei Anwendung der Norm nahezu zwingend zu einem Rechtsverstoß führen.

Vielleicht sind die vorgenannten Ausführungen der Grund dafür, warum im Konsultationspapier, in dem der BfDI offenbar davon ausgeht, dass eine Rechtsgrundlage erforderlich wäre, nicht ausreichend begründet wird, warum Art. 6 Abs. 1 lit. f DS-GVO keine praktische Relevanz zukommen soll. Denn lässt man die dargestellten systematischen und dogmatischen Argumente einmal außen vor, so dient die Anonymisierung natürlich gerade dem Betroffenenschutz. Daher sollte im Regelfall die Interessenabwägung – sowohl bei der Anonymisierung als auch bei der Pseudonymisierung – »zu Gunsten« des Verantwortlichen ausfallen, da kein Risiko für den Betroffenen besteht. Schließlich wird durch die Anonymisierung der Personenbezug aufgehoben und dem Recht auf informationelle Selbstbestim-mung genüge getan. Eine anschließende Verarbeitung der anonymisierten Daten fällt dagegen nicht mehr in den Anwendungsbereich der DS-GVO und kann daher auch nicht in die Interessensabwägung einbezogen werden. Ebenso sollte zu Gunsten des Verantwortlichen berücksichtigt werden, wenn eine Anonymisierung oder Pseudonymisierung möglichst frühzeitig erfolgt, wie z. B. zum Zeitpunkt der Extraktion aus dem Stammsystem.

2.3.2. Rechtsgrundlagen aus Artikel 9 DS-GVO

Hält man für die Anonymisierung stets eine Rechtsgrundlage für erforderlich, wäre die mitunter gesellschaftspolitisch gewünschte Anonymisierung von Gesundheitsdaten im privatwirtschaftlichen Bereich nur in den engen Grenzen des Art. 9 Abs. 2 DS-GVO möglich. Insbesondere (i) nur mit Einwilligung des Betroffenen (vgl. Art. 9 Abs. 2 lit. a DS-GVO) oder (ii) unter der Voraussetzung, dass das Anonymisierungsinteresse des Unternehmens das Interesse des Betroffenen an der Nicht-Anonymisierung erheblich überwiegt (vgl. Art. 9 Abs. 2 lit. j DS-GVO i.V.m. § 27 Abs. 1 Satz 1 BDSG). Dies könnte die im europäischen und deutschen Verfassungsrecht sowie im Datenschutzrecht zum Ausdruck kommende Privilegierung von Wissenschaft und Forschung unterlaufen.

Begreift man die Anonymisierung nicht als wirkgleiches Mittel, sondern als Unterfall der Löschung käme auf den ersten Blick Art. 9 Abs. 2 lit. f DS-GVO in Betracht. Anders als Art. 6 Abs. 1 lit. c DS-GVO bezieht sich dieser allerdings auf Rechtsansprüche des Verarbeitenden und ist somit nicht anwendbar ist. Eine Analogie wäre nur durch einen juristischen Kunstgriff möglich. Zum anderen könnte man an Art. 9 Abs. 2 lit. g DS-GVO denken, hier bedarf es aber zum einen einer gesonderten unionsrechtlichen oder nationalen Regelung und zum anderen eines besonderen öffentlichen Interesses. Also nicht dem Interesse desjenigen, der die Löschung verlangt, sondern dem Interesse der gesamten Bevölkerung bzw. der sozialen Gemeinschaft.

In der Praxis führt dies dazu, dass im Zweifel personenbezogene Daten in größerem Umfang verarbeitet werden z. B. auf Basis einer breiten Einwilligungserklärung.

2.3.3. Weiterverarbeitung gem. Art. 6 Abs. 4 DS-GVO i.V.m. der ursprünglichen Rechtsgrundlage

Wir begrüßen und unterstützen ausdrücklich die Interpretation des BfDI, dass die Rechtsgrundlage für die zweckändernde Weiterverarbeitung unverändert die Rechtsgrundlage bildet, die die ursprüngliche Verarbeitung legitimiert hat, soweit die Vereinbarkeit nach Art. 6 Abs. 4 DS-GVO gegeben ist. Eine gesonderte Rechtfertigung der eigentlichen Datenverarbeitung muss daher nicht erfolgen und die »neue« Verarbeitung muss nur noch gemäß Art. 6 Abs. 4 DS-GVO gerechtfertigt werden. Der Erwägungsrund 50 besagt ausdrücklich, dass keine gesonderte Rechtsgrundlage mehr erforderlich ist.

Allerdings sollte klargestellt werden, dass die Kriterien des Art. 6 Abs. 4 DS-GVO auch für die zweckändernde Weiterverarbeitung von besonderen personenbezogenen Daten (wie z. B. Gesundheitsdaten) gelten.

Sofern Daten initial rechtmäßig erhoben wurden, kann eine anonymisierte Weiterverarbeitung nicht von einer Rechtsgrundlage abhängig sein. Die Rechtfertigungsbedürftigkeit einer Datenverarbeitung knüpft an ein normatives Bedürfnis zur Herbeiführung der praktischen Konkordanz zwischen dem Grundrecht auf informationelle Selbstbestimmung sowie der Wirtschaftsgrundrechte andererseits an. Weder die Überführung personen bezogener Daten in einen im Sinne der Definition anonymen Zustand und schon gar nicht die darauf basierende Verarbeitung anonymer, d. h. nicht personenbezogener Daten, werfen vor dem Hintergrund der zitierten praktischen Konkordanz Fragen des Schutzes der Privatsphäre auf. Insofern besteht kein normativ zwingender Grund, die Anonymisierung vom Bestehen einer Rechtsgrundlage abhängig zu machen. Und genau deshalb muss die Kompatibilitätsprüfung überflüssig sein. Demgegenüber entscheidend ist selbstverständlich die Frage, ob die Daten tatsächlich anonymisiert sind. Diese Frage muss sehr genau geprüft werden, denn ansonsten greift die Argumentation ins Leere. Maßstab hierfür sind angemessene technische und organisatorische Maßnahmen, über die der Verantwortliche gebietet. Ist unter diesen Gesichtspunkten eine Re-Anonymisierung ausgeschlossen, sind die Daten anonym. Das muss aus der Sicht eines anderen Verantwortlichen für denselben Datensatz nicht zwangsläufig der Fall sein. Das macht den relativen Anonymisierungsbegriff aus (s. o.). Letzterer führt im Übrigen automatisch zu einem relativen Begriff vom Personenbezug.

Bei der Prüfung der Weiterverarbeitung zum Zweck der Anonymisierung personenbezogener Daten kommt es im Rahmen des Art. 6 Abs. 4 DS-GVO außerdem nicht darauf an, welcher Verarbeitungszweck anschließend mit den anonymisierten Daten verfolgt wird.

Der BfDI führt aus, dass im Regelfall die personenbezogenen Daten, die anonymisiert werden sollen, zu einem bestimmten anderen Zweck ursprünglich erhoben wurden. Eine anschließende Anonymisierung stelle deshalb in diesen Fällen eine Weiterverarbeitung dar, deren Zweck mit dem ursprünglichen Erhebungszweck vereinbar sein müsse. In dem dann als Beispiel aufgeführten Fall sollen Kundenbestandsdaten anonymisiert werden, »um diese einer Auswertung im Hinblick auf die Verteilung der Dienstleistungen nach Alterskohorten in einer bestimmten Region zuzuführen«.

In der anschließend beispielhaften Prüfung der Voraussetzungen für die Weiterverarbeitung aus Art. 6 Abs. 4 DS-GVO wird fälschlich der ursprüngliche Zweck (Begründung und Ausgestaltung des Vertragsverhältnisses) mit dem Zweck verglichen, der mit der Verarbeitung der dann anonymen Daten verfolgt werden soll. Legt man hier wie der BfDI eine Verarbeitung zugrunde, ist unter der Weiterverarbeitung nach Art. 6 Abs. 4 DS-GVO die Anonymisierung der Daten selbst zu verstehen und nicht die anschließende Verarbeitung der anonymisierten Daten. Der Zweck dieser (Weiter-)Verarbeitung ist die Entfernung des Personenbezugs. Der mit der Verarbeitung der anonymen Daten verfolgte Zweck kann für die datenschutzrechtliche Beurteilung und Zulässigkeit nicht entscheidend sein, da auf diese Verarbeitung die DS-GVO keine Anwendung findet. Dies entspricht dem Schutzgedanken der DS-GVO, welche gerade dann nicht anwendbar ist, wenn es sich um anonyme Daten handelt. Entsprechend wurde auch in dem WP216 (a. a. o. Seite 8) festgestellt, »dass die Anonymisierung als eine Form der Weiterverarbeitung personenbezogener Daten mit dem ursprünglichen Verarbeitungszweck vereinbar ist, allerdings nur unter der Voraussetzung, dass das Anonymisierungsverfahren geeignet ist, zuverlässig anonymisierte Informationen in dem in dieser Stellungnahme beschriebenen Sinne hervorzubringen.«

Würde wie vom BfDI scheinbar angenommen, bei der Anonymisierung der Daten der Zweck geprüft, der bei der späteren Verarbeitung der anonymen Daten verfolgt wird, würde somit die DS-GVO auch für anonyme Daten außerhalb ihres Anwendungsbereichs gelten. Damit würde sich zudem die Frage stellen, ob die Verarbeitung der anonymen Daten dann auf den Zweck begrenzt ist, der im Rahmen der Anonymisierung geprüft wurde. Die DS-GVO würde dann entgegen ihrem Wortlaut auch Geltung für die Verarbeitung nicht personenbezogener Daten beanspruchen.

2.4. Interpretation des TKG

2.4.1. Allgemein

Die ePrivacy Richtlinie nennt in Art. 6 und 9 Anonymisierung und Löschung alternativ, ohne Hinzuziehung einer Rechtsgrundlage. Der Richtliniengeber ist also erkennbar davon ausgegangen, dass es sich nicht um eine Verarbeitung handelt. Demzufolge ist eine Anonymisierung / Löschung von Verkehrsdaten jederzeit möglich, ohne dass es eines Rückgriffs auf die DS-GVO bedarf.

Selbst wenn man mit dem BfDI davon ausgeht, dass die Löschung / Anonymisierung gem. § 96 Abs. 1 TKG einer Rechtsgrundlage bedarf, stehen in diesem Fall für eine Anonymisierung von Verkehrsdaten gem. § 96 Abs. 1 TKG alle Rechtsgrundlagen des Art. 6 DS-GVO zur Verfügung. Eine Reduzierung der Rechtsgrundlagen für die Anonymisierung von Verkehrsdaten durch § 96 Abs. 1 S. 2 Alt. 2 TKG auf Art. 6 Abs. 1 lit. c DS-GVO greift zu kurz.

2.4.2. § 96 Abs. 3 TKG

Der BfDI geht davon aus, dass Verkehrsdaten zu den in § 96 Abs. 3 TKG genannten Zwecken nur anonymisiert werden dürfen, wenn der Betroffene eingewilligt hat. Diese Ansicht geht fehl, da der nationale Gesetzgeber mit § 96 Abs. 3 TKG die Regelung des Art. 6 Abs. 3 ePrivacy Richtlinie (Richtlinie 2002/58/EG nun in der Fassung der Richtlinie 2009/136/EG) umgesetzt hat. Danach dürfen die Daten personenbezogen verarbeitet werden, sofern eine Einwilligung des Betroffenen vorliegt. Die Anonymisierung ist gerade nicht Voraussetzung für die Verarbeitung der Daten des Anrufenden. Lediglich die Daten des Angerufenen (sog. B-Teilnehmers) sind zu anonymisieren, weil der anrufende Teilnehmer nicht über die Informationsfreiheit des B-Teilnehmers disponieren darf.

Darüber hinaus benennen sowohl der europäische Richtlinien – als auch der nationale Gesetzgeber die Anonymisierung von Verkehrsdaten als Verpflichtung des Verantwortlichen zum Schutz der Daten des Betroffenen, nicht als rechtfertigungspflichtige Datenverarbeitung. Die Auslegung des BfDI entspricht an dieser Stelle weder dem Gesetzeswortlaut noch dem der zugrundeliegenden Richtlinie.

2.4.3. § 96 Abs. 1 TKG

Entgegen den Ausführungen des BfDI bedarf es auch bei § 96 Abs. 1 S. 2 Alt. 2 und § 96 Abs. 1 S. 3 TKG keines Rekurses auf Art. 6 Abs. 1 lit. c DS-GVO. Die Regelungen des TKG setzen hier nur teilweise Art. 6 Abs. 1 ePrivacy Richtlinie um, der anordnet, dass Verkehrsdaten »zu löschen oder zu anonymisieren« sind. Der Richtliniengeber sieht offenbar die

Möglichkeit der Löschung und Anonymisierung unabhängig voneinander. Zum einen regelt die ePrivacy Richtlinie in Art. 6 Abs. 1 die Löschung von Verkehrsdaten. Mit dem BfDI ist davon auszugehen, dass eine Löschung wirkgleich auch durch die Anonymisierung erzielt werden kann. Zum anderen regelt Art. 6 Abs. 1 ePrivacy Richtlinie aber auch die Anonymisierung als zweite Alternative, wenn sie nicht (ausschließlich) zum Zweck der Löschung erfolgt. Der Richtliniengeber hat dies durch die gesonderte Nennung von Anonymisierung und Löschung deutlich gemacht.

Der nationale Gesetzgeber hat in § 96 Abs. 1 a. E. TKG nur das Tatbestandsmerkmal des Löschens aufgenommen. Dies war mit Blick auf die Regelung des § 3 Abs. 4 und 6 BDSG a. F. auch verständlich, da das Anonymisieren gerade keine Verarbeitung im Rechtssinn darstellte. Der nationale Gesetzgeber ist – wie der Richtliniengeber – davon ausgegangen, dass ein Anonymisieren dem Löschen gleichkommt. Demzufolge bedarf es keiner Rechtsgrundlage für die Anonymisierung von Verkehrsdaten. Anonymisierung und Löschung sind jederzeit möglich.

Selbst wenn man der Auffassung des BfDI folgt, dass die Anonymisierung eine Verarbeitung sei, stehen als Rechtsgrundlagen der Anonymisierung nicht nur wie vom BfDI angenommen § 96 Abs. 1 S. 2 Alt. 2 TKG /Art. 6 Abs. 1 lit. c DS-GVO i.V.m. § 96 Abs. 1 S. 3 TKG zur Verfügung. Eine Anonymisierung der Verkehrsdaten ist auch auf Basis eines berechtigten Interesses (§ 96 Abs. 1 S. 3 TKG i.V.m. Art. 6 Abs. 1 lit. f DS-GVO) oder der Weiterverarbeitung (Art. 6 Abs. 4 DS-GVO) möglich. Allerdings hat der deutsche Gesetzgeber nicht berücksichtigt, dass die Richtlinie nicht nur das Löschen durch Anonymisieren sondern auch das Anonymisieren zu anderen Zwecken regelt.

Die Artikel 29-Gruppe hat in ihrer Stellungnahme 5/2014 zu Anonymisierungstechniken, WP 216 ausgeführt, dass eine Anonymisierung in Art. 6 Abs. 1 ePrivacy Richtlinie ausdrücklich zulässig ist (WP 216, Seite 9). In diesem Fall ist laut WP 216 »eine entsprechende Rechtsgrundlage nach Artikel 7 der Datenschutzrichtlinie gegeben«. Daher konnte in dem dort beschriebenen Fall auf Artikel 7 f) der Richtlinie 95/46 zurückgegriffen werden, der eine Anonymisierung aufgrund des berechtigten Interesses erlaubt. Dieser Gedanke ist ohne weiteres auf das Verhältnis der ePrivacy Richtlinie zur DS-GVO übertragbar. Etwaige zusätzliche Beschränkungen im TKG für einen Rückgriff auf die allgemeinen Rechtsgrundlagen des Art. 6 DS-GVO, die keine Grundlage in der ePrivacy Richtlinie finden, können keine Berücksichtigung finden (vgl. auch EuGH C-582/14 (Breyer) Rz. 57 f.). Das gilt insbesondere auch, da die in Art. 6 Abs. 1 der ePrivacy Richtlinie vorgesehene Möglichkeit der Anonymisierung entgegen der Richtlinie nicht in deutsches Recht umgesetzt wurde, da die Möglichkeit zur Anonymisierung zu anderen Zwecken als der Löschung fehlt.

Datenschutzrechtlich kommt es bei der Anonymisierung nicht auf den später mit den anonymisierten Daten verfolgten Zweck an. Dieser liegt außerhalb des Anwendungsbereichs der DS-GVO. Gleiches gilt bei einer Anonymisierung zum Zweck der Löschung. Auch in diesem Fall ist der Zweck die Beseitigung des Personenbezugs. Damit wird aber eine Weiterverwendung der nicht personenbezogenen Daten nicht ausgeschlossen.

2.4.4 § 98 Abs. 1 TKG

Bei der Anwendung des § 98 TKG ist zu beachten, dass es sich dabei um andere Standortdaten als Verkehrsdaten handelt (Art. 9 ePrivacy Richtlinie). Diese dürfen nicht gleichgesetzt werden. Zudem kann eine zu enge Wortlautauslegung, nach der anonymisierte Daten für einen »Dienst mit Zusatznutzen« zu verwenden seien, die freie Anwendung von anonymisierten Daten enorm einschränken. Lässt man den Einwilligungstatbestand außer Betracht, bedeutet die Position des BfDI, dass anonymisierte Standortdaten ausschließlich zur Bereitstellung von Diensten mit Zusatznutzen verarbeitet werden dürften. Ein anderer Zweck der Verarbeitung anonymisierter Standortdaten wäre versperrt. Der Umkehrschluss des BfDI ist nicht nur methodisch fragwürdig, er steht auch dem gesetzgeberischen Willen entgegen. Der Gesetzgeber hat die anonymisierte Verarbeitung von Standortdaten nicht auf den Zweck der Erbringung von Diensten mit Zusatznutzen beschränkt. Dies wäre auch vom Wortlaut der ePrivacy Richtlinie, an dem sich der nationale Gesetzgeber orientiert hat, nicht gedeckt gewesen. Danach dürfen auch spezielle Standortdaten in anonymisierter Form zu jedem anderen Zweck verarbeitet werden.

Der Vollständigkeit halber sei angemerkt, dass der nationale Gesetzgeber mit § 98 Abs. 1 Alt. 1 TKG auch keine Rechtsgrundlage für eine Anonymisierung schaffen wollte. Wie bereits oben erwähnt ist grundsätzlich eine Löschung durch Anonymisierung möglich und das BDSG a.F. ging bei der Anonymisierung gar nicht von einem Verarbeitungstatbestand aus. Insofern dürften die Auslegungen des BfDI wohl auch dem rechtshistorischen Kontext entrissen sein.

3. Harmonisierung auf europäischer Ebene erforderlich / Einheitliche Linie auf europäischer Ebene notwendig

Der deutsche Gesetzgeber normiert in § 27 Abs. 3 Satz 2 BDSG eine Art Anonymisierungsgebot. Danach sind besondere personenbezogene Daten zu anonymisieren, sobald dies nach dem Forschungszweck möglich ist und berechtigte Interessen des Betroffenen nicht entgegenstehen. Zwar hat der deutsche Gesetzgeber die Wichtigkeit der Anonymisierung von beispielsweise Gesundheitsdaten im Bereich der Forschung erkannt und unter

Nutzung der Öffnungsklausel in Art. 9 Abs. 2 j), Art 89 Abs. 1 DS-VGO geregelt. Allerdings bereiten dieser deutsche Sonderweg und die europäische Fragmentierung in der Praxis erhebliche Schwierigkeiten. Ausländische Geschäftspartner und Investoren lassen sich nur ungern auf nationale Sonderregelungen ein. Vielmehr sollte die Anonymisierung in einer einheitlichen behördlichen Stellungnahme als Ausprägung der datenschutzrechtlichen Grundprinzipien der Datenminimierung ohne Erfordernis einer ausdrücklichen Rechtsgrundlage privilegiert werden.

4. Anforderung an die Anonymität nach der DS-GVO und Notwendigkeit klarerer Kriterien

Durch die Entfernung des Personenbezugs wird den Datenschutzgrundprinzipien der Datenminimierung und Speicherbegrenzung Rechnung getragen. Bei anonymisierten Daten entfällt das datenschutzrechtliche Schutzbedürfnis und somit die Anwendbarkeit der Datenschutzgrundverordnung (DS-GVO) sowie spezialgesetzlicher Datenschutzgesetze wie z. B. das Telekommunikationsgesetz (TKG). Zugleich wird dadurch der für die digitale gesellschaftliche, wirtschaftliche und wissenschaftliche Entwicklung so wichtige Zugang zu Daten erheblich verbessert.

Die »Anonymität« besteht als Gegenbegriff zum »Personenbezug«. Art. 4 Nr. 5 DS-GVO enthält eine Definition der Pseudonymisierung. Eine eigene Definition von Anonymisierung enthält die DS-GVO dagegen nicht – sie ergibt sich aber im Umkehrschluss aus der Definition der »personenbezogenen Daten« (Art. 4 Nr. 1 DS-GVO) und wird in Erwägungsgrund 26 Satz 5 DS-GVO näher erläutert:

»*Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d. h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natür--liche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann.*«

Wann der Zustand erreicht ist, dass die betroffene Person nicht mehr identifiziert werden kann, ist umstritten und zugleich von wesentlicher Bedeutung für die Abgrenzung zwischen Pseudonymisierung und Anonymisierung. Unternehmen brauchen klare Kriterien, ab wann Daten als anonym angesehen werden können.

4.1. Relativer Personenbezug nach der DS-GVO

Wir sind der Ansicht, dass die DS-GVO einem relativen Ansatz hinsichtlich der Frage nach der Bestimmbarkeit einer Person folgt. Dies ergibt sich insbesondere aus Erwägungsgrund

26 Satz 3 DS-GVO, wonach alle Mittel berücksichtigt werden sollten, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person zu identifizieren und dabei insbesondere der Zeit- und Kostenaufwand zu berücksichtigen ist. Auch der EuGH stellt in seinem Urteil vom 18.10.2016 – C-582/14 »Breyer« auf ein im Grunde relatives Verständnis des Personenbezugs ab. Wir begrüßen daher, dass für eine Anonymisierung ausdrücklich auf die EuGH Entscheidung in Sachen Breyer Bezug genommen wird. Danach kommt es darauf an, ob ein Verantwortlicher mit eigenen oder ihm zur Verfügung stehenden fremden Mitteln vernünftigerweise eine natürliche Person re-identifizieren kann. Das ist dann nicht der Fall, »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.«

4.2. »Faktische Anonymität« nach der DS-GVO

Wir begrüßen, dass der BfDI offenbar davon ausgeht, dass eine absolute Anonymisierung derart, dass die Re-Identifizierung für jeden unmöglich sein muss, datenschutzrechtlich nicht gefordert ist. Ausreichend sei, dass eine Re-Identifizierung praktisch nicht durchführbar ist, weil der Personenbezug nur mit einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften wiederhergestellt werden kann. Der deutsche Gesetzgeber spricht in § 16 Abs. 6 Nr. 1 BstatG in einem vergleichbaren Fall von »faktischer Anonymisierung«. Nach erfolgter Anonymisierung muss das Herstellen des Personenbezugs nicht absolut, sondern nur faktisch unmöglich sein, weil der Aufwand zur Re-Identifizierung unverhältnismäßig groß ist. Die De-Anonymisierung von faktisch anonymisierten Daten muss nicht mit absoluter Sicherheit ausgeschlossen werden.

Über faktische Anonymität entscheidet vielmehr eine Kosten-Nutzen-Analyse.

Wir würden es begrüßen, wenn der BfDI seine Auffassung von einer datenschutzrechtlich ausreichenden Anonymisierung als »faktische Anonymisierung« bezeichnet. Verbunden mit dem klaren Bekenntnis, dass beide Arten eine ausreichende Anonymisierung im Sinne der DS-GVO darstellen.

4.3. Verschiedene Arten der Anonymisierung

Die Anonymisierung von Daten bzw. Datensätzen kann auf verschiedene Arten erfolgen. Neben der Löschung von Daten in Datensätzen können Daten auch generalisiert, aggregiert oder verfälscht werden, so dass eine Bezug zu natürlichen Personen nicht mehr

besteht. Gerade bei strukturierten Daten, etwa in einer Datentabelle, lassen sich so auf unterschiedliche Arten Daten verarbeiten, die für sich, d. h. ohne direkte Verknüpfung zu einem persönlichen Merkmal, nicht personenbezogen sind.

4.4. Technische Realisierung der Anonymisierung

Um den relative oder faktischen Anonymisierungsansatz technisch zu realisieren, existieren verschiedene Ansätze aus der öffentlichen Forschung, u.a., k-Anonymity, l-Diversity oder auch Differential Privacy. Diese Ansätze wurden auch in der Opinion 5/2014[1] erwähnt. Die Verfahren haben folgende Eigenschaften gemein:

- Die Art und Weise, wie ein Verfahren anonymisiert transparent/öffentlich bekannt ist; insbesondere auch mögliche Schwächen und Grenzen der Anwendung. Denn dadurch ist eine Beurteilung des Einsatzes möglich.
- Die Verfahren geben klare und quantifizierbare Garantien bezüglich der resultierenden Anonymität. Maße aus der öffentlichen Forschung wie z. B. die Re-Identifikationswahrscheinlichkeit und das Inferenz Risiko können empirisch belegt werden. Solche Maße reflektieren den erwähnten Aspekt aus Erwägungsgrund 26 und somit, ob ein »motivierter Eindringling« fähig ist eine Anonymisierung zu »umgehen«.

Verfahren, die diesen Eigenschaften genügen, erlauben auf technischer Ebene zum einen eine sichere Anonymisierung und zum anderen die automatisierte Feststellung, ob eine Anonymisierung ausreichend ist. Eine behördliche Stellungnahme zum Einsatz von standardisierten Anonymisierungsverfahren würde einen Beitrag zur Erhöhung der Transparenz schaffen und zugleich die Sicherheit für die Betroffenen und das Vertrauen der Betroffenen in diese Verfahren erheblich erhöhen. Zugleich sollte dabei aber sichergestellt sein, dass die Entwicklung von weiteren Verfahren möglich und wirtschaftlich sinnvoll bleibt – d. h. dass kein de-facto unumstößlicher Standard geschaffen wird.

4.5. Konkrete Kriterien

Es fehlen konkrete Kriterien, anhand derer Daten zweifelsfrei daraufhin überprüft werden können, ob ein Personenbezug vorhanden ist oder ob die Daten anonym sind. Wir halten ein Verfahren für angemessen, bei dem geprüft wird, ob ein objektiver Dritter, in der Lage ist, den Betroffenen anhand des Datums zu re-identifizieren. Dabei ist stets auf den vertretbaren Aufwand abzustellen, geltende Standards zur Prüfung, der Stand der Technik sind heranzuziehen. Zu diskutierende Kriterien könnten sein:

[1] ↗ https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

- Der Dritte hat keine speziellen Fähigkeiten (wie z. B. Computer-Hacking-Fähigkeiten), ist aber durchschnittlich kompetent.
- Er hat angemessenen Zugang zu öffentlich zugänglichen Informationen (z.B. aus dem Internet oder anderen öffentlichen Quellen hat), und
- Zugang zu weitergehende Ermittlungstechniken, um zusätzliche Informationen zu erhalten, ohne zugleich einen Rechtsverstoß zu begehen.

Dabei ist grundsätzlich die Beurteilung zum Zeitpunkt der Verarbeitung ausschlaggebend. Gefordert ist also nicht die absolute Irreversibilität der Anonymisierung für alle Zeiten, sondern ein Zustand, in dem aller Wahrscheinlichkeit nach keine De-Anonymisierung vorgenommen werden kann, weil sie etwa technisch viel zu aufwändig und schwierig oder rechtlich nicht zulässig wäre. Hier sollte auch auf technisch standardisierte Lösungen zur Anonymisierung abgestellt werden.

Es bedarf einer einheitlichen behördlichen Stellungnahme auf europäischer Ebene mit eindeutigen Kriterien, ab wann Daten als anonym gelten.

4.6. Risikobasierter Ansatz

Der DS-GVO liegt ein risikobasierter Ansatz zu Grunde. So hat beispielsweise die Wahl der technischen und organisatorischen Maßnahmen nach Art. 32 DS-GVO in Abhängigkeit der Eintrittswahrscheinlichkeit und des mit der Verarbeitung verbundenen Risikos zu erfolgen. Ausgehend vom risikobasierten Ansatz sollte auch die Wahl des geeigneten Anonymisierungsverfahrens bzw. der Anonymisierungstechnik auf Basis einer detaillierten Risikoprognose erfolgen. Im Rahmen der Risikoprognose sollte das Risiko der Re-Identifizierung ermittelt werden (das »Re-Identifizierungsrisiko«).

Im Rahmen der Prüfung des Re-Identifizierungsrisikos sollten zunächst die mit der De-Anonymisierung verbundenen möglichen Folgen für den Betroffenen identifiziert werden. Anschließend sollte die Eintrittswahrscheinlichkeit evaluiert werden. Dazu sind der mögliche Nutzen der De-Anonymisierung (und der daraus folgende Anreiz) und das mögliche Zusatzwissen Dritter zu ermitteln. Zuletzt müssten die Eintrittswahrscheinlichkeit und die mit der De-Anonymisierung verbundenen möglichen Folgen in ein Verhältnis gesetzt werden. Aus der Eintrittswahrscheinlichkeit und den möglichen Folgen ergibt sich sodann das Re-Identifizierungsrisiko (z.B. ein geringes, mittleres, erhöhtes oder hohes Risiko).

Je höher das Re-Identifizierungsrisiko ist, desto effektiver sollte die Schutzwirkung des Anonymisierungsverfahrens sein.

5. Fazit

Festzuhalten bleibt, dass die Anonymisierung unserer Ansicht nach keine Verarbeitung im Sinne der DS-GVO darstellt.

Sollte die Anonymisierung dagegen als Verarbeitung angesehen werden, muss klargestellt werden, dass sie jedenfalls keiner gesonderten Rechtsgrundlage bedarf, sondern vielmehr als Ausprägung der datenschutzrechtlichen Grundprinzipien der Datenminimierung privilegiert und damit ohne Rechtsgrundlage jederzeit zulässig ist.

Die Industrie braucht klare Kriterien, ab wann Daten als anonym gelten. Bitkom bringt sich gern in die Erstellung eines entsprechenden Katalogs ein.

Im Interesse der Wettbewerbsfähigkeit deutscher Unternehmen und einer verbesserten Nutzung anonymisierter Daten im europäischen Datenraum, halten wir es für erforderlich, dass sich der BfDI für eine Klarstellung unserer Forderungen in einer einheitlichen behördlichen Stellungnahme auf europäischer Ebene einsetzt.

Bitkom vertritt mehr als 2.700 Unternehmen der digitalen Wirtschaft, davon gut 1.900 Direktmitglieder. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.