Stellungnahme der Deutschen Telekom anlässlich des öffentlichen Konsultationsverfahrens des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Thema:

Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche

Vorbemerkung

Die Deutsche Telekom begrüßt die Initiative des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) mehr Rechtssicherheit im Umgang mit der Anonymisierung personenbezogener Daten herbeizuführen und bedankt sich für die Möglichkeit, im Rahmen des Konsultationsverfahrens Stellung nehmen zu können.

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 (DSGVO) 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.[1] Vor diesem Hintergrund ist Rechtssicherheit bei der Anonymisierung personenbezogener Daten zwingend erforderlich. Dies umfasst neben der Klärung der rechtlichen Fragestellungen der Anonymisierung auch die Schaffung verlässlicher technischer Standards. Zugleich muss auch die Nutzbarmachung von Daten für weitere Zwecke durch Anonymisierung gewährleistet sein. Dies scheint auch der BfDI durch das folgende Statement in der Einleitung des Papiers zur Konsultation so zu sehen. „Die Anonymisierung kann auch als Mittel angesehen werden, im Einzelfall eine Verarbeitung von Daten gar erst zu ermöglichen, wenn die Verarbeitung bei bestehendem Personenbezug datenschutzrechtlich unzulässig wäre."

Vor diesem Hintergrund ist die Deutsche Telekom der Auffassung, dass die Anonymisierung personenbezogener Daten keine Verarbeitung im Sinne der DSGVO ist. Rechtmäßig erhobene personenbezogene Daten können ohne Rechtsgrundlage jederzeit auch vor Eintritt der gesetzlich festgelegten Lösch- bzw. Anonymisierungsverpflichtung zum Zweck der weiteren Verwendung anonymisiert werden. Letzteres gilt auch, wenn der BfDI dennoch zu dem Ergebnis kommen sollte, dass die Anonymisierung einer Rechtsgrundlage bedarf. Art. 6 Abs. 1 ePrivacy Richtlinie (2002/58/EG) ermöglicht alternativ zur Löschung auch die Anonymisierung zu anderen Zwecken als der Löschung. Diese Regelung ist im TKG nicht umgesetzt. In diesem Fall ist also der Rückgriff auf die DSGVO möglich und stehen für eine Anonymisierung von Verkehrsdaten gem. §96 Abs. 1 TKG alle Rechtsgrundlagen des Art. 6 DSGVO 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 c) ist mit europäischem Recht nicht vereinbar und darf, soweit eine richtlinienkonforme Auslegung nicht möglich ist, nicht zur Anwendung kommen.

[1] Vgl. zur Notwendigkeit Daten verfügbar zu machen: Eckpunkte einer Datenstrategie der Bundesregierung sowie „A European strategy for data" COM(2020) 66 final

1. Anonymisierung ist keine Verarbeitung i.S.d. DSGVO

Bei der Anonymisierung handelt es sich um eine Ausprägung der datenschutzrechtlichen Grundprinzipien der Datenminimierung und Speicherbegrenzung. Deren Umsetzung bedarf keiner Rechtsgrundlage aus der DSGVO oder sonstiger spezialgesetzlicher Regelungen. Die Umsetzung wird von der DSGVO vorausgesetzt. Bereits im Tätigkeitsbericht 2015-2016 hat der BfDI explizit aufgeführt: „Eine Anonymisierung von Daten gilt nicht als Verarbeitung und ist somit zulässig“ (BfDI 26. Tätigkeitsbericht 2015-2016, 17.2.4.4 „Big Data im TK-Bereich, S. 170). Dieser Feststellung lag der im BDSG aF auf Basis der Richtlinie 95/46/EG umgesetzte Verarbeitungsbegriff zugrunde. Der Verarbeitungsbegriff aus der Richtlinie 95/46/EG wurde nahezu wortgleich in die DSGVO übernommen. Es ist nicht erkennbar, wie sich daraus eine Änderung der Rechtslage ergeben kann, die nun eine Rechtsgrundlage für die Anonymisierung erforderlich machen würde.

Sinn und Zweck der Datenschutzgesetze ist der Schutz der informationellen Selbstbestimmung. Darunter fällt auch die zweckgebundene Verarbeitung personenbezogener Daten. Werden diese Daten anonymisiert, besteht das Schutzbedürfnis nicht mehr. Es ist denklogisch notwendig, einmal zulässig verwendete personenbezogene Daten hin zur Anonymisierung zu verändern. Anonymisierung ist somit zum einen ein rechtlich legitimes Mittel und zum anderen greift es den politischen Willen des Gesetzgebers auf.

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

Mit Blick auf Art 6 Abs. 1 e) Richtlinie 95/46/EG (= Art. 5 Abs. 1 e) DSGVO) 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 anonymised “by default” (subject to different legal requirements, such as those mentioned in the e-Privacy 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, d.h. die Anonymisierung von personenbezogenen Daten, wäre immer vereinbar mit dem ursprünglichen Zweck und eine Vereinbarkeitsprüfung obsolet. Entsprechendes gilt bei der Prüfung des berechtigten Interesses. Bei Wegfall des Personenbezugs durch Anonymisierung kann es kein überwiegendes Interesse des Betroffenen geben. Dennoch müsste formalistisch u.a. den Dokumentationsanforderungen gem. Art. 5 Abs. 2 DSGVO Rechnung getragen werden.

Die Forderung nach einer Rechtsgrundlage für die Anonymisierung erhöht die Komplexität, nicht aber den Schutz der Persönlichkeitsrechte. Maßgeblich für einen wirksamen Schutz der Persönlichkeitsrechte ist die Definition und Anwendung verlässlicher Anonymisierungsstandards.

2. Annahmen des BfDI zu den Rechtsgrundlagen

Die Deutsche Telekom ist der Auffassung, dass die Anonymisierung personenbezogener Daten keine Verarbeitung i.S.d. DSGVO ist und daher keiner Rechtsgrundlage bedarf. Sofern der BfDI an der in der Konsultation geäußerten Auffassung festhält, dass eine Rechtsgrundlage für die Anonymisierung erforderlich sei, soll nachfolgend auf einzelne Punkte der Ausführungen des BfDI eingegangen werden.

a) Anonymisierung gem. § 96 Abs. 1 S. 2 Alt. 2/Art. 6 Abs. 1 Buchst. c) DSGVO i.V.m. § 96 Abs. 1 S. 3 TKG

Der BfDI führt aus, dass nach § 96 Abs. 2 S. 2 Alt. 2 TKG Verkehrsdaten nur verwendet werden dürfen, soweit dies durch andere gesetzliche Vorschriften begründete Zwecke erforderlich sei. Art. 6 Abs. 1 Buchst. c) DSGVO erlaube eine Datenverarbeitung, die zur Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt, erforderlich ist. Insofern verpflichte § 96 Abs. 1 S. 3 TKG den Diensteanbieter die Verkehrsdaten nach Beendigung der Verbindung unverzüglich zu löschen. Da die personenbezogenen Daten auch durch deren Anonymisierung gelöscht werden könnten, sei die Anonymisierung von Verkehrsdaten gemäß § 96 Abs. 1 S. 2 Alt. 2 bzw. Art. 6 Abs. 1 Buchst. c) DSGVO möglich.

Es ist grundsätzlich zu begrüßen, dass der BfDI eine Löschung durch Anonymisierung als wirkungsgleich erachtet. In diesem Zusammenhang sei darauf hingewiesen, dass die zugrundeliegende ePrivacy Richtlinie in Art. 6 Abs. 1 die Möglichkeit der Löschung und Anonymisierung unabhängig voneinander ermöglicht („... zu löschen oder zu anonymisieren."). Geregelt wird also gerade nicht nur das Löschen durch Anonymisierung. Die ePrivacy Richtlinie geht erkennbar bei der Löschung und Anonymisierung von zwei unterschiedlichen Sachverhalten aus.

Zum einen regelt die ePrivacy Richtlinie in Art. 6 Abs. 1 die Löschung von Verkehrsdaten. Mit dem BfDI ist davon auszugehen, dass eine Löschung wirkungsgleich auch durch die Anonymisierung erzielt werden kann. Zum anderen regelt Art. 6 Abs. 1 ePrivacy Richtlinie aber auch die Anonymisierung, wenn sie nicht (ausschließlich) zum Zweck der Löschung erfolgt. Der Richtliniengeber hat dies durch die gesonderte Nennung von Anonymisierung und Löschung deutlich gemacht. In § 96 Abs. 1 TKG fehlt die zweite Alternative des Art. 6 Abs. 1 ePrivacy Richtlinie, die eine Anonymisierung zu anderen Zwecken als der Löschung ermöglicht.

Insofern besteht in § 96 Abs. 1 TKG ein Umsetzungsdefizit der ePrivacy Richtlinie in nationales Recht. Der Rückgriff auf die Erlaubnistatbestände der DSGVO ist also möglich.

(1) Anwendbarkeit der Rechtsgrundlagen des Art. 6 DSGVO auf die Anonymisierung von Verkehrsdaten

Folgt man der Auffassung des BfDI, dass die Anonymisierung eine Verarbeitung sei, stehen als Rechtsgrundlagen der Anonymisierung nicht nur wie vom BfDI angenommen § 96 Abs. 1 S. 2 Alt. 2/Art. 6 Abs. 1 Buchst. c) DSGVO 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 f) DSGVO) oder der Weiterverarbeitung (Art. 6 Abs. 4 DSGVO) möglich.

Die Artikel 29-Gruppe hat in ihrer Stellungnahme 5/2014 zu Anonymisierungstechniken (WP 216) ausgeführt, dass eine Anonymisierung in Art. 6 Abs. 1 der 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 DSGVO übertragbar. Etwaige zusätzliche Beschränkungen im TKG für einen Rückgriff auf die allgemeinen Rechtsgrundlagen des Art. 6 DSGVO, die keine Grundlage in der ePrivacy Richtlinie finden, können keine Berücksichtigung finden.[2] 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. Daher gelten in diesem Fall aufgrund des Umsetzungsdefizits alle Rechtsgrundlagen des Art. 6 DSGVO.

(2) Die Beschränkung des § 96 Abs. 1 S. 2 Alt. 2 TKG i.V.m. Art. 6 Abs. 1 c) DSGVO ist mit europäischem Recht nicht vereinbar

Eine Reduzierung auf Art. 6 Abs. 1 c) i.V.m. § 96 Abs. 1 S. 2 Alt. 2 TKG ist mit europäischem Recht nicht vereinbar und darf, soweit eine richtlinienkonforme Auslegung nicht möglich ist, nicht zur Anwendung kommen. Ebenso wie die fehlende Umsetzung der Möglichkeit zur Anonymisierung aus Art. 6 Abs. 1 ePrivacy Richtlinie ins TKG handelt sich um eine unzulässige Beschränkung der allgemeinen Grundsätze aus Art. 6 DSGVO.

In dem Verfahren Breyer (C-582/14) hat der EuGH festgestellt,

„*dass Art. 7 der Richtlinie 95/46 eine erschöpfende und abschließende Liste der Fälle vorsieht, in denen eine Verarbeitung personenbezogener Daten als rechtmäßig angesehen werden kann, und dass die Mitgliedstaaten weder neue Grundsätze in Bezug auf die Zulässigkeit der Verarbeitung personenbezogener Daten neben diesem Artikel einführen noch zusätzliche Bedingungen stellen dürfen, die die Tragweite eines der sechs darin vorgesehenen Grundsätze verändern würden.*" (a.a.O. Rz. 57).

Die Mitgliedstaaten dürfen zudem bei der Umsetzung der Richtlinie die Voraussetzungen näher bestimmen, unter denen die Verarbeitung personenbezogener Daten rechtmäßig ist. Allerdings dürfen die Mitgliedstaaten dabei in Bezug auf die Zulässigkeit der Verarbeitung personenbezogener Daten „*keine anderen als die in Art. 7 der Richtlinie 95/46 aufgezählten Grundsätze einführen und auch nicht durch zusätzliche Bedingungen die Tragweite der sechs in Art. 7 vorgesehenen Grundsätze verändern.*" (a.a.O. Rz. 58).

Gem. Art. 1 Abs. 2 ePrivacy Richtlinie ergänzt und detailliert diese die Richtlinie 95/46 EG. Die Mitgliedstaaten dürfen gem. Art. 15 ePrivacy Richtlinie die Rechte und Pflichten aus Art. 6 ePrivacy Richtlinie nur aus Gründen der nationalen Sicherheit einschränken. Die Beschränkung des § 96 Abs. 1 S. 2 Alt. 2 TKG i.V.m. Art. 6 Abs. 1 c) DSGVO ergibt sich weder aus Artikel 6 ePrivacy Richtlinie noch aus Art. 15 ePrivacy Richtlinie. Ebenso kann damit nicht die fehlende Umsetzung der Anonymisierung zu anderen Zwecken als der Löschung aus der ePrivacy Richtlinie gerechtfertigt werden.

Im Einklang mit der Rechtsprechung des EuGH handelt es sich somit um zusätzliche Bedingungen, die die Tragweite der allgemeinen Verarbeitungstatbestände unzulässig verändern. Eine Beschränkung auf § 96 Abs. 1 S. 2 Alt. 2 TKG i.V.m. Art. 6 Abs. 1 c) DSGVO ist daher nicht mit europäischem Recht vereinbar und darf,

[2] Siehe auch EuGH C-582/14 (Breyer) Rz. 57 f.

sofern nicht richtlinienkonform auslegbar, nicht zur Anwendung kommen. Gleiches gilt für die fehlende Umsetzung der Möglichkeit zur Anonymisierung zu anderen Zwecken als der Löschung. Stattdessen stehen zur Anonymisierung von Verkehrsdaten die Rechtsgrundlagen des Art. 6 DSGVO zur Verfügung.

Zu berücksichtigen ist bei diesen Überlegungen, dass es hier vor allem um die Anonymisierung bei Wegfall der Erforderlichkeit geht. Bestimmt wird also der Zeitpunkt, wann die Daten spätestens zu löschen / anonymisieren sind. Eine Anonymisierung als Äquivalent zur Löschung als „Standardeinstellung" muss aber auch zu einem früheren Zeitpunkt möglich sein und nicht erst bei Wegfall der Erforderlichkeit.

Datenschutzrechtlich kommt es zudem bei der Anonymisierung nicht auf den später mit den anonymisierten Daten verfolgten Zweck an (vgl. unter 2 c) die Ausführungen zu Art. 6 Abs. 4 DSGVO). Dieser liegt außerhalb des Anwendungsbereichs der DSGVO. 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.

b) Anonymisierung im Rahmen von § 96 Abs. 3 TKG

§ 96 Abs. 3 TKG ermöglicht eine Verarbeitung von teilnehmerbezogenen Verkehrsdaten zum Zwecke der Vermarktung von Telekommunikationsdiensten, zur bedarfsgerechten Gestaltung von Telekommunikationsdiensten oder zur Bereitstellung von Diensten mit Zusatznutzen, sofern der Betroffene eingewilligt hat. Anders als vom BfDI dargestellt, dürfen in diesem Fall die Daten sogar personenbezogen verarbeitet werden, sofern eine Einwilligung des Betroffenen vorliegt. Eine Anonymisierung ist dafür nicht erforderlich. Lediglich die Daten des Angerufenen (sog. B-Teilnehmer) sind zu anonymisieren, weil der A-Teilnehmer nicht über die Informationsfreiheit des B-Teilnehmers disponieren darf. Ob in § 96 Abs. 3 TKG eine generelle Rechtsgrundlage für eine grundsätzliche Anonymisierung von Verkehrsdaten gesehen werden kann, darf somit leider bezweifelt werden.

c) Anonymisierung im Rahmen von § 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 mit Standortdaten aus Verkehrsdaten 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. Anonyme Daten unterliegen gerade nicht dem Schutzgedanken der Datenschutzgesetze und dürfen somit frei verwendet werden.

d) Weiterverarbeitung gem. Art. 6 Abs. 4 DSGVO i.V.m. der ursprünglichen Rechtsgrundlage

Bei der Prüfung der Weiterverarbeitung zum Zweck der Anonymisierung personenbezogener Daten kommt es im Rahmen des Art. 6 Abs. 4 DSGVO nicht darauf an, welcher Verarbeitungszweck anschließend mit den anonymisierten Daten verfolgt wird. Die Anonymisierung ist immer mit dem ursprünglichen Zweck vereinbar.

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 DSGVO 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 DSGVO 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 nicht entscheidend sein, da auf diese Verarbeitung die DSGVO keine Anwendung findet. Dies entspricht dem Schutzgedanken der DSGVO, welche gerade dann nicht anwendbar ist, wenn es sich um anonyme Daten handelt.

Würde wie vom BfDI angenommen, bei der Anonymisierung der Daten der Zweck geprüft, der bei der späteren Verarbeitung der anonymen Daten verfolgt wird, würde somit die DSGVO 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 DSGVO würde dann entgegen ihrem Wortlaut auch Geltung für die Verarbeitung nicht personenbezogener Daten beanspruchen.

3. Praktische Auswirkungen im Fall einer erforderlichen Rechtsgrundlage

Wird wie vom BfDI eine Rechtsgrundlage für die Anonymisierung gefordert, führt dies zu einer formalistischen Verkomplizierung der Prozesse und zusätzlichem administrativen Aufwand, ohne den Schutz für die Betroffenen zu erhöhen.

Bei einer Anonymisierung auf Basis einer Rechtsgrundlage, ist der Zweck der Verarbeitung ausschließlich die beabsichtigte Anonymisierung. Der später mit der Verarbeitung der anonymen Daten verfolgte Zweck kann für die datenschutzrechtliche Beurteilung nicht entscheidend sein. Die DSGVO findet auf diese Verarbeitung keine Anwendung.

Eine wirksame Anonymisierung vorausgesetzt, wäre bei einer Verarbeitung zum Zweck der Anonymisierung im Fall des Art. 6 Abs. 1 f) DSGVO stets von einem zwingenden berechtigten Interesse des Verantwortlichen auszugehen. Ein entgegenstehendes überwiegendes Interesse des Betroffenen am Erhalt des Personenbezugs der Daten ist wegen der unwiderruflichen Aufhebung des Personenbezugs ausgeschlossen. Gleiches würde für eine Anonymisierung auf Basis von Art. 6 Abs. 4 DSGVO i.V.m. der ursprünglichen Rechtsgrundlage gelten. Die Entfernung des Personenbezugs als ultimative datenschutzrechtliche Maßnahme ist stets mit dem ursprünglichen Zweck vereinbar.

Nichts desto trotz, müsste der Verantwortliche bei der Anonymisierung sämtlichen formellen Anforderungen an eine Datenverarbeitung aus Art. 5 Abs. 2 DSGVO Rechnung tragen. Dies würde zu einem erheblichen administrativen Mehraufwand beim Verantwortlichen führen, der bei formalen Fehlern sogar bußgeldbewehrt wäre. Der Schutz des Betroffenen würde hingegen nicht erhöht, da die Verarbeitung immer zulässig wäre.

Für die spezialgesetzlich geregelten Verarbeitungstatbestände wie z.B. im TKG zeigen sich zudem Umsetzungsdefizite der ePrivacy Richtlinie in das nationale Recht. Der deutsche Gesetzgeber hat maßgebliche Regelungen zur Anonymisierung aus Art. 6 Abs. 1 ePrivacy Richtlinie im TKG nicht umgesetzt. Würde in diesen Fällen von einer Verarbeitung ausgegangen, müsste, wie bereits bei den Erläuterungen zu § 96 Abs. 1 TKG gezeigt, jeweils sehr aufwendig hergeleitet werden, dass eine Anonymisierung auf Basis der allgemeinen Verarbeitungstatbestände der DSGVO möglich und zudem immer zulässig wäre. Der Schutz der Betroffenen wäre damit nicht erhöht, die Anfälligkeit des Verantwortlichen für formale Fehler bei der Dokumentation gem. Art. 5 Abs. 2 DSGVO sowie bei den Betroffenenrechten hingegen beträchtlich.

Auch bei den Betroffenenrechten zeigt sich, dass die Forderung nach einer Rechtsgrundlage für die Anonymisierung den Schutz des Betroffenen nicht erhöhen, in der Praxis aber erheblichen Mehraufwand erzeugen würde.

Der Betroffene müsste über die beabsichtige Verarbeitung zum Zweck der Anonymisierung sowie im Fall des Art. 6 Abs. 1 f) DSGVO über etwaige Widerspruchsrechte informiert werden. Das Widerspruchsrecht könnte sich aber nur gegen die Verarbeitung zum Zweck der Anonymisierung richten, nicht aber gegen die spätere Verarbeitung der anonymen Daten. Von daher kann sich kein denkbarer Fall ergeben, bei dem ein überwiegendes Interesse an der Anonymisierung verneint werden könnte. Die Anonymisierung führt immer zum Abschneiden des Personenbezuges, so dass es für den Betroffenen kein Schutzbedürfnis mehr gibt, welches überhaupt berücksichtigt werden müsste.

Vor diesem Hintergrund erhöht die Forderung nach einer Rechtsgrundlage für die Anonymisierung zwar die Komplexität, nicht aber den Schutz der Persönlichkeitsrechte. Maßgeblich für einen wirksamen Schutz der Betroffenen muss stattdessen die Definition und Anwendung verlässlicher Anonymisierungsstandards sein, um die Entfernung des Personenbezugs sicher zu gewährleisten. Schlägt die Anonymisierung fehl, bleibt der Schutz der personenbezogenen Daten durch das fortgeltende Datenschutzrecht sichergestellt.

Wenn die Anonymisierung als Verarbeitung klassifiziert würde, dann hätte dies in der praktischen Umsetzung insbesondere folgende Auswirkungen: Betroffene müsste vor jeder Anonymisierung umfassend informiert werden, vgl. Art. 13 DSGVO. D.h. alle bisherigen Datenschutzhinweise, auch die der Bestandskunden, müssten angepasst werden. Wenn darüber hinaus eine „generelle“ Beschreibung der Anonymisierung nicht ausreichend sollte, sondern eine use-case-spezifische Beschreibung gefordert würde, wäre ein Ergebnis, dass vor jeder einzelnen Anonymisierung alle Kunden darüber informiert werden müsste. Der administrative Aufwand wäre enorm. Zudem würde dies flexible Big-Data-Anwendungen auf Basis von anonymen Daten verhindern. Dem Gedanken, anonyme Daten als Wirtschaftsmotor zu verstehen, würde dies entgegensprechen.

Darüber hinaus müssten alle Voraussetzungen einer z.B. einer Datenschutzfolgeabschätzung erfüllt sein, obwohl die Schutzrechte des Betroffenen mit einer Anonymisierung immer gewahrt sind. Dies ist unabhängig von der jeweiligen Rechtsgrundlage immer gegeben.

Zusätzlich müssten die Reichweite und Grenzen etwaiger Rechtsgrundlagen, z.B. die aus dem TKG berücksichtigt werden, für den Fall, dass die lex generalis-Regeln des Art. 6 DSGVO nicht anwendbar sein sollten. Gerade die TKG-Regelungen zeigen Grenzen für die Verwendung von anonymen Daten auf, vgl. § 98 TKG in Bezug „Dienste mit Zusatznutzen“. Diese würde die freie Verwendung von anonymen Daten unzumutbar eingrenzen.

Unabhängig von den praktischen Auswirkungen auf die Anonymisierung im konkreten Einzelfall kann die Forderung nach einer Rechtsgrundlage für die Anonymisierung auch in einer Gesamtbetrachtung zu unnötigen sowie unerwünschten Beschränkungen führen. „Im digitalen Zeitalter sind **Daten eine Schlüsselressource für gesellschaftlichen Wohlstand und Teilhabe, für eine prosperierende Wirtschaft und den Schutz von Umwelt und Klima, für den wissenschaftlichen Fortschritt und für staatliches Handeln.“**[3]

Mit der Forderung nach einer Rechtsgrundlage besteht die Gefahr einer übermäßig restriktiven Begrenzung der Möglichkeiten der Anonymisierung. Obwohl der Schutz der Betroffenen dadurch nicht erhöht würde, wären die Daten als Schlüsselressource formal aufgrund fehlender rechtlicher Möglichkeiten zur Anonymisierung nicht verfügbar.

4. Fazit

- Die Anonymisierung personenbezogener Daten ist keine Verarbeitung i.S.d. der DSGVO.
- Rechtmäßig erhobene personenbezogene Daten können ohne Rechtsgrundlage jederzeit auch vor Eintritt der gesetzlich festgelegten Lösch- bzw. Anonymisierungsverpflichtung auch zum Zweck der weiteren Verarbeitung anonymisiert werden.
- Letzteres gilt auch, wenn von einer Verarbeitung ausgegangen wird. In diesem Fall stehen für eine Anonymisierung von Verkehrsdaten gem. § 96 TKG alle Rechtsgrundlagen des Art. 6 DSGVO zur Verfügung.
- Art. 6 Abs. 1 ePrivacy Richtlinie ermöglicht neben der Löschung von Verkehrsdaten, wozu auch die Löschung durch Anonymisierung zählt, auch die Anonymisierung zu anderen Zwecken. Diese Regelung ist entgegen der ePrivacy Richtlinie in § 96 Abs. 1 TKG nicht umgesetzt. Daher kommen, eine Verarbeitung unterstellt, die allgemeinen Regelungen aus Art. 6 DSGVO für die Anonymisierung von Verkehrsdaten zur Anwendung.
- Eine Reduzierung der Rechtsgrundlagen für die Anonymisierung von Verkehrsdaten durch § 96 Abs. 1 S. 2 Alt. 2 TKG auf Art. 6 Abs. 1 c) ist mit europäischem Recht nicht vereinbar und darf, soweit eine richtlinienkonforme Auslegung nicht möglich ist, nicht zur Anwendung kommen.
- Der Zweck der (Weiter-)Verarbeitung zur Anonymisierung ist die Entfernung des Personenbezugs. Der später mit der Verarbeitung der anonymen Daten verfolgte Zweck kann für die datenschutzrechtliche Beurteilung nicht entscheidend sein, da auf diese Verarbeitung die DSGVO keine Anwendung findet.
- Die Forderung nach einer Rechtsgrundlage für die Anonymisierung erhöht die Komplexität, nicht aber den Schutz der Persönlichkeitsrechte. Maßgeblich für einen wirksamen Schutz der Persönlichkeitsrechte ist die Definition und Anwendung verlässlicher Anonymisierungsstandards sein.

[3] Eckpunkte einer Datenstrategie der Bundesregierung