Stellungnahme zur Konsultation des BfDI zum Thema „Anonymisierung unter der DS-GVO unter besonderer Berücksichtigung der TK-Branche“

I. Zielsetzung der Konsultation

Zielsetzung der Konsultation ist nach Angabe des BfDI, den geltenden Rechtsrahmen für die Anonymisierung personenbezogener Daten durch Verantwortliche aufzuzeigen und eine öffentliche Diskussion hierüber anzustoßen. Ob und unter welchen Voraussetzungen personenbezogene Daten anonymisiert (weiter-)verarbeitet werden dürfen, bedarf nach Auffassung der GDD allerdings einer streng juristischen Betrachtung. Anders als bei der Auslegung unbestimmter Rechtsbegriffe oder der Sammlung von Kriterien im Rahmen der Interessenabwägung verbleibt insoweit wenig Spielraum für das Einbringen gesamtgesellschaftlicher oder wirtschaftlicher Erwägungen insbesondere durch die betroffenen Interessengruppen.

II. Anonymisierung als Verarbeitung personenbezogener Daten

Bei einer Anonymisierung handelt es sich um eine Verarbeitung von personenbezogenen Daten. Ziel der Anonymisierung ist das unumkehrbare Entfernen des Personenbezugs. Das Resultat ist ein anonymisierter Datenbestand. Eine Identifizierung der betroffenen Personen ist demnach ausgeschlossen. Da die Daten vor der Anonymisierung personenbezogen vorliegen, unterfallen die Verarbeitungsvorgänge der Anonymisierung selbst dem Datenschutzrecht.[1] Davon getrennt zu betrachten sind solche anonymen Informationen, die von vornherein keinen Personenbezug aufweisen und daher auch keiner Anonymisierung unterliegen. Auch die vom BfDI zitierte Art.-29-Datenschutzgruppe ging davon aus, dass die Anonymisierung das Ergebnis personenbezogener Datenverarbeitung ist.[2] Personenbezogene Daten dürfen aber nur auf Basis einer entsprechenden Rechtsgrundlage verarbeitet werden (Erwägungsgrund 40, sog. Verbot mit Erlaubnisvorbehalt).

Dies gilt auch dann, sofern die personenbezogene Datenverarbeitung nur „on-the-fly“ erfolgt. Mit „on-the-fly“ wird in der Computertechnik ein Vorgang bezeichnet, der auf das dauerhafte oder temporäre Speichern von Daten, insbesondere Ausgabedaten, im permanenten Datenspeicher verzichtet. Eine Datenverarbeitung ist nach Art. 4 Nr. 2 DS-GVO jeder Vorgang bzw. jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten. Auf die zeitliche Dauer der Datenverarbeitung kommt es ebenso wenig an wie darauf, ob die Daten (zwischen-)gespeichert werden.

Anonymisierungen können auch nicht unter Hinweis auf ein fehlendes Risiko aus dem Anwendungsbereich der DS-GVO ausgenommen werden. Art. 4 Nr. 2 DS-GVO sieht sogar das Löschen und Vernichten personenbezogener Daten als Verarbeitung an. Für die Anonymisierung, die im Verhältnis zum Löschen bzw. Vernichten ein Weniger darstellt, musss dies erst recht gelten. Einer Anonymisierung geht im Übrigen stets eine legitimationsbedürftige Verarbeitung personenbezogener Daten voraus, nämlich deren Erhebung. Diese Erhebung bedarf – unabhängig davon, ob die Daten in der Folge sofort wieder anonymisiert werden – einer entsprechenden Rechtsgrundlage.

---

[1] Vgl. Hansen in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Auflage 2019, Art. 4 Nr. 5 Rn. 23.

[2] *Art.-29-Datenschutzgruppe*, Stellungnahme 5/2014 zu Anonymisierungstechniken, angenommen am 10.04.14 S. 3.

III. Legitimation der Pseudonymisierung und Transparenzpflichten (DS-GVO)

1. Allgemeines

Prinzipiell kommt eine Einwilligung als Rechtsgrundlage der mit der Anonymisierung verbundenen Datenverarbeitung in Betracht, die in der Praxis allerdings vielfach nicht vorliegen wird. Praktisch relevant ist daher vor allem die Frage, inwiefern gesetzliche Erlaubnistatbestände entsprechende Datenverarbeitungen legitimieren können. Entscheidend für die einschlägige Rechtsgrundlage ist dabei, ob der Zweck der anonymisierten Verarbeitung bereits bei Datenerhebung bestand.

2. Anonymisierte Verarbeitung als Primärzweck

Handelt es sich um einen sog. Primärzweck, d.h. einen Zweck, der bereits bei Datenerhebung bestand, ist maßgebliche Rechtsgrundlage der Anonymisierung im nicht telekommunikationsrechtlichen Bereich regelmäßig Art. 6 Abs. 1 lit. f) DS-GVO. Im Rahmen der Abwägung ist zu berücksichtigen, dass der Verordnungsgeber bereits pseudonymisierte Verarbeitungen als weniger eingriffsinvasiv und daher förderungswürdig angesehen hat (vgl. Art. 6 Abs. 4 lit. e) DS-GVO sowie Erwägungsgrund 28 DS-GVO). Dies muss erst recht gelten, wenn Ziel eine nur anonymisierte Datenverarbeitung ist.

Im Fall des Primärzwecks ist über den Zweck der anonymisierten Verarbeitung gemäß Art. 13 Abs. 1 lit. c) DS-GVO zu informieren, sofern die Datenerhebung beim Betroffenen selbst erfolgt. Im Übrigen gilt Art. 14 Abs. 1 lit. c) DS-GVO.

Soweit personenbezogene Daten nicht bei der betroffenen Person erhoben werden, enthält Art. 14 Abs. 5 DS-GVO Ausnahmen von der Informationspflicht. Relevant ist vorliegend insbesondere Art. 14 Abs. 5 lit. b) DS-GVO, wonach die Informationspflicht entfällt, wenn sich die Erteilung der Information als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordert. Art. 14 Abs. 5 lit. b) DS-GVO soll nach dem Gesetzeswortlaut insbesondere für die Verarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke vorbehaltlich der in Art. 89 Abs. 1 DS-GVO genannten Bedingungen und Garantien gelten oder soweit die in Art. 14 Abs. 1 DS-GVO genannte Pflicht voraussichtlich die Verwirklichung der Ziele der Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt. Wird von der Ausnahme nach Art. 14 Abs. 5 lit. b) DS-GVO Gebrauch gemacht, hat der Verantwortliche geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person zu ergreifen, einschließlich der Bereitstellung dieser Informationen für die Öffentlichkeit. Unverhältnismäßig kann eine Informationserteilung sein, wenn die Anzahl der betroffenen Personen groß ist und deren Interessen nur gering beeinträchtigt werden von der Datenverarbeitung.[3]

Für den Fall der Datenerhebung bei der betroffenen Person selbst enthält Art. 13 DS-GVO keinen Art. 14 Abs. 5 lit. b) DS-GVO entsprechenden Ausnahmetatbestand von der Informationspflicht. Eine analoge Anwendung von Art. 14 Abs. 5 lit. b) DS-GVO im Rahmen von Art. 13 DS-GVO wird in der Literatur zum Teil per se mit der Begründung abgelehnt, dass es sich um unterschiedliche Fallgestaltungen handele und auch keine planwidrige Regelungslücke vorliege, die eine Analogie rechtfertigen könnte.[4] Nur bei einer Datenerhebung, die nicht bei der betroffenen Person erfolgt, bestehe ein praktisches Bedürfnis, den Verantwortlichen von unüberschaubaren Informationspflichten freizustellen.[5] Nach Auffassung der GDD erscheinen Ausnahmen von Art. 13 DS-GVO aufgrund unverhältnismäßigen Aufwands der Information zwar nicht generell ausgeschlossen, da es sich bei der Unverhältnismäßigkeit letztlich um einen

---

3 Heidelberger Kommentar/*Schwartmann/Schneider* DS-GVO/BDSG, 2018, Art. 14 Rn. 68.

4 Simitis/Hornung/Spiecker gen. Döhmann/*Dix* Datenschutzrecht, 2019, Art. 13 Rn. 22; BeckOK DatenschutzR/*Schmidt-Wudy* DS-GVO Art. 13 Rn. 93 ff.; zumindest für diskutabel halten eine entsprechende Anwendung Paal/Pauly/*Paal/Hennemann* DS-GVO Art. 13 Rn. 35.

5 Simitis/Hornung/Spiecker gen. Döhmann/*Dix* a.a.O.

allgemeinen Rechtsgrundsatz für das Entfallen einer Pflichtigkeit handelt.[6] Allerdings wird sich bei einem unmittelbaren Kontakt mit der betroffenen Person ein unverhältnismäßiger Aufwand praktisch regelmäßig nicht begründen lassen. Zu beachten ist auch, dass die Transparenz der Datenverarbeitung aus Sicht des Verordnungsgebers ein zentrales Prinzip ist, das nicht durch nicht gesetzlich vorgesehene Ausnahmen ausgehöhlt werden darf.

3. Anonymisierte Verarbeitung als Sekundärzweck

Stellt die anonymisierte Verarbeitung lediglich einen Sekundärzweck dar, war diese also bei Datenerhebung noch nicht intendiert, ist Art. 6 Abs. 4 DS-GVO ausschlaggebend, wonach eine Kompatibilitätsprüfung durchzuführen ist, d.h., es ist die Vereinbarkeit der Anonymisierung bzw. anonymisierten Weiterverarbeitung mit dem ursprünglichen Erhebungszweck zu prüfen. Wie ein Erst-Recht-Schluss aus Art. 6 Abs. 4 lit. e) DS-GVO zeigt, wird eine Kompatibilität regelmäßig angenommen werden können.

In diesem Fall stellt sich die Frage nach der Verpflichtung zur Nachinformation bzgl. des neuen Zwecks der anonymisierten Weiterverarbeitung (Art. 13 Abs. 3, 14 Abs. 4 DS-GVO). Die Ausnahmetatbestände nach Art. 14 Abs. 5 DS-GVO gelten auch für die Nachinformation nach Art. 14 Abs. 4 DS-GVO.

Rechtlicher Argumentationsspielraum kann sich ggf. im Einzelfall daraus ergeben, dass Art. 13 Abs. 2, 14 Abs. 2 DS-GVO keine absoluten Informationspflichten enthalten, sondern die dort genannten Informationen nur zur Verfügung gestellt werden müssen, wenn diese „notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten“. Allerdings bezieht sich dieser Spielraum nicht auch auf die Information über den Zweck der Datenverarbeitung. Die Information über die Zwecke der Datenverarbeitung ist entsprechend ihrer zentralen Relevanz für die betroffene Person gemäß Art. 13 Abs. 1, 14 Abs. 1 DS-GVO eine Pflichtinformation.

IV. Anonymisierung statt Löschung

Aus Sicht der GDD zutreffend führt der BfDI unter Verweis auf eine Entscheidung der österreichischen Datenschutzbehörde[7] aus, dass eine Löschung von Daten i.S.v. Art. 17 DS-GVO auch durch Anonymisierung der Daten erfolgen kann, sofern es sich um ein valides Anonymisierungsverfahren handelt. Insofern kann sich eine Berechtigung zur Anonymisierung auch aus Art. 6 Abs. 1 lit. c) i.V.m. Art. 17 Abs. 1 DS-GVO ergeben. Diese Erwägung hilft allerdings dann nicht weiter, wenn Geschäftsmodelle darauf basieren, dass personenbezogene Daten von vornherein mit dem Interesse der unmittelbaren Anonymisierung erhoben werden. Denn in diesen Fällen stellt sich zunächst die Frage nach der Zulässigkeit der Datenerhebung. Die Anwendung von Art. 6 Abs. 1 lit. c) i.V.m. Art. 17 Abs. 1 DS-GVO setzt die Zulässigkeit der Datenerhebung aber voraus.

V. Besonderheiten bei Anonymisierung von bes. Kategorien personenbezogener Daten (Art. 9 DS-GVO)

Wie oben ausgeführt, ist maßgebliche Rechtsgrundlage für die Anonymisierung personenbezogener Daten im nicht telekommunikationsrechtlichen Bereich regelmäßig Art. 6 Abs. 1 lit. f) DS-GVO. Auf diese Regelung kann allerdings nicht zurückgegriffen werden, sofern besondere Kategorien personenbezogener Daten i.S.v. Art. 9 Abs. 1 DS-GVO anonymisiert werden sollen, z.B. Gesundheitsdaten. Insofern sind die strengeren Regelungen aus Art. 9 DS-GVO und § 22 BDSG zu beachten, welche die Möglichkeit einer Interessenabwägung nicht vorsehen.

VI. Besonderheiten bei der Anonymisierung von Telekommunikationsdaten

Soweit die Anonymisierung von Telekommunikationsdaten betroffen ist, sind die spezialgesetzlichen Datenschutzvorschriften im TKG zu beachten. Als

---

6 Sydow/*Ingold*, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 13 Rn. 11; für eine teleologische Reduktion von Art. 13 DS-GVO „in Einzelfällen“ Heidelberger Kommentar/*Schwartmann/Schneider* DS-GVO/BDSG, 2018, Art. 14 Rn. 68.

7 Entscheidung der österreichischen Datenschutzbehörde vom 05.12.2018, Az.: DSB-D123.270/0009DSB/2018

Umsetzung der ePrivacy-Richtlinie (2002/58/EG, zuletzt geändert durch Richtlinie 2009/136/EG) genießen die TKG-Datenschutzregelungen Vorrang vor den allgemeinen Regelungen der DS-GVO (Art. 95 DS-GVO).[8] Mit Blick auf die enge Zweckbindung bei der Verarbeitung von Verkehrs- und Standortdaten ist hinsichtlich der Anonymisierung ein Rückgriff auf Art. 6 Abs. 1 lit. f) bzw. Art. 6 Abs. 4 lit. e) DS-GVO nicht möglich.

Der Ansatz des BfDI, wonach eine Anonymisierung einer Löschung gleichzustellen ist und demgemäß Verkehrsdaten nach Beendigung der Verbindung nicht zwingend zu löschen sind, sondern auch anonymisiert weiterverarbeitet werden dürfen (§ 96 Abs. 1 S. 3 TKG), ist eine vertretbare juristische Argumentation, um eine Weiterverarbeitung von Verkehrsdaten außerhalb der engen Zulässigkeitsregeln des TKG zu ermöglichen.[9] Mit Blick auf die hohe Sensibilität von Verkehrsdaten sind aus Sicht der GDD allerdings hohe Anforderungen an die Sicherheit des Anonymisierungsverfahrens zu stellen. Im Übrigen hilft die Argumentation eines die Löschung ersetzenden Anonymisierens nur dann, wenn TK-Verkehrsdaten anonymisiert weiterverarbeitet werden sollen, die ansonsten tatsächlich reif für die Löschung wären, d.h. nicht mehr erforderlich sind für Zwecke nach § 96 Abs. 1 S. 2 TKG. Ansonsten fehlt es an der Löschpflicht als juristischem Ansatzpunkt.

Sofern Standortdaten als Verkehrsdaten verarbeitet werden, gilt ebenfalls § 96 TKG (vgl. Abs. 1 Nr. 1). [10]

Im Übrigen dürfen Standortdaten gemäß § 98 TKG nur im zur Bereitstellung von Diensten mit Zusatznutzen erforderlichen Maß und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden, wenn sie anonymisiert wurden oder wenn die Teilnehmer ihre Einwilligung gegeben haben. Eine Anonymisierung von Standortdaten zu anderen Zwecken als der Bereitstellung von Diensten mit Zusatznutzen lässt sich über die Norm nicht legitimieren. Werden Standortdaten im Rahmen der Bereitstellung von Diensten mit Zusatznutzen anonymisiert (§ 98 Abs. 1 Alt. 1 TKG), dann wird man die anonymisierten Daten allerdings zusätzlich auch für andere Zwecke verwenden dürfen, denn mit der Anonymisierung entfallen die Daten den Beschränkungen des TKG. Darüber hinaus wird man auch hinsichtlich der Standortdaten auf die oben dargestellte Argumentation eines die Löschung ersetzenden Anonymisierens zurückgreifen können, sobald bei einem Dienst mit Zusatznutzen die Standortdaten zur Diensterbringung nicht mehr benötigt werden und daher zu löschen wären.

VII. Ansätze für eine gesetzliche Weiterentwicklung

Im Sinne der Rechtssicherheit wäre es wünschenswert, dass der europäische Gesetzgeber eine Definition der Anonymisierung in die DS-GVO aufnimmt und diese der Löschung gleichsetzt.

Gesellschaft für Datenschutz und Datensicherheit e.V.
Heinrich-Böll-Ring 10, 53119 Bonn
info@gdd.de | www.gdd.de

8 Heidelberger Kommentar/*Richter* DS-GVO/BDSG, 2018, Art. 95 Rn. 7 f.

9 Für die Möglichkeit der Anonymisierung statt Löschung etwa auch Scheurle/Mayen/*Büttgen* TKG § 96 Rn. 10-13; Arndt/Fetzer/Scherer/Graulich/*Lutz* TKG 2. Aufl. 2015, § 96 Rn. 15; Königshofen/Ulmer, Datenschutzhandbuch Telekommunikation, 2006, § 96 Rn. 16.

10 Scheurle/Mayen/*Löwnau/Müller* TKG § 98 Rn. 2.