Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Positionspapier

zur Anonymisierung unter der DSGVO

unter besonderer Berücksichtigung der TK-Branche

Stand: 29. Juni 2020

1. Einführung

Die Menge der verfügbaren personenbezogenen Daten steigt exponentiell an. Ihre Aussagekraft über das Verhalten der Menschen nimmt zu. Die Analyse von Datenbeständen und die Auswertung der daraus resultierenden Erkenntnisse werden zu einem immer wichtigeren Bestandteil der modernen Wirtschaft, Wissenschaft und Forschung.

Aufgrund der damit verbundenen Risiken für die Freiheiten des Einzelnen setzt das europäische Datenschutzrecht der ökonomischen, politischen oder wissenschaftlichen Verwertung personenbezogener Daten Grenzen.

Für viele Forschungsprojekte und Geschäftsmodelle ist die Analyse von Datensätzen ausreichend, deren abstrakter Gehalt erhalten bleibt, der Personenbezug jedoch aufgehoben wird. In diesen Fällen gebietet der Grundsatz der Datenminimierung im Sinne des Art. 5 Abs. 1 Buchst. c) DSGVO, die personenbezogenen Daten nur in anonymisierter Form zu verarbeiten. 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.

Trotz ihrer hohen praktischen Bedeutung ist die Anonymisierung datenschutzrechtlich nur rudimentär geregelt. In der DSGVO werden anonyme und anonymisierte Daten in den Sätzen 4 und 5 von Erwägungsgrund 26 adressiert. Danach sollten die Grundsätze des Datenschutzes nicht für anonyme Informationen gelten, „d. h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann“. Weitere Bestimmungen hierzu enthält die DSGVO nicht.

1.1. Öffentliches Konsultationsverfahren

Die unklare Rechtslage nahm der BfDI zum Anlass, in der Zeit vom 10. Februar bis zum 23. März 2020 ein öffentliches Konsultationsverfahren zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche durchzuführen.

Die Auswertung der eingegangenen Stellungnahmen ergab ein heterogenes, die Komplexität der Materie widerspiegelndes Meinungsbild.

Neben den eingegangenen Stellungnahmen wurden auch öffentlich zugängliche Fachbeiträge in die Analyse miteinbezogen. Insgesamt soll mit dem Positionspapier ein Beitrag zur Rechtssicherheit im Kontext der Anonymisierung geleistet werden.

1.2. Anonymisierung: eine begrifflich-terminologische Klarstellung

Anonymisierung ist ein Vorgang, der darauf gerichtet ist, den Personenbezug von Daten aufzuheben. Mit anderen Worten soll mit dem Einsatz von Anonymisierungstechniken erreicht werden, dass die betroffene Person nicht mehr identifiziert werden kann[1].
Einige Datenschutzgesetze der Länder definieren die Anonymisierung – mit Abweichungen im Detail – als das Verändern personenbezogener Daten dergestalt, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können[2].
Eine hinreichende Anonymisierung führt dazu, dass die Grundsätze des Datenschutzrechts – wie z.B. der Grundsatz der Zweckbindung – nicht mehr anwendbar sind (vgl. Erwägungsgrund 26, Satz 4 und 5 DSGVO).

2. Anforderungen an die Anonymisierung

Durch die Verwendung des Begriffs der anonymisierten Daten in Erwägungsgrund 26 Satz 5 bringt der Verordnungsgeber zum Ausdruck, dass eine Anonymisierung rechtlich möglich ist[3]. Wann eine Anonymisierung als hinreichend angesehen werden kann, darüber gibt die DSGVO keine Auskunft. Erwägungsgrund 26 Satz 3 und 4 enthält lediglich folgende Hinweise: „Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern. Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen

[1] Vgl. ISO 29100:2011; Petrlic/Sorge, Datenschutz: Einführung in technischen Datenschutz, Datenschutzrecht und angewandte Kryptographie, 2017, S. 13; Paal/Pauly/Ernst, DS-GVO, Art. 4 Rn. 48.

[2] Vgl. § 3 BbgDSG; § 2 Abs. 4 BremDSG; § 11 Abs. 2 HmbDSG und LT-Drucks. 21/11987, S. 10; § 4 DSG NRW; § 24 Nr. 18 DSG Nds; § 3 Abs. 2 S. 2 Nr. 4 Sächs. DSG; § 2 Abs. 7 DSG LSA; § 13 Abs. 2 Schleswig-Holsteinisches DSG; § 28 Abs. 3 ThürDSG.

[3] Vgl. auch § 27 Abs. 3 BDSG.

Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind“.

Eine absolute Anonymisierung derart, dass die Wiederherstellung des Personenbezugs für niemanden möglich ist, dürfte häufig nicht möglich sein und ist im Regelfall datenschutzrechtlich auch nicht gefordert[4]. Ausreichend ist in der Regel, dass 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 Arbeitskraft wiederhergestellt werden kann[5].

Besonders hervorzuheben ist dabei, dass eine valide Anonymisierung – je nach Art der zu anonymisierenden Daten und Kontext der Verarbeitung – eine Herausforderung für den jeweiligen Verantwortlichen bedeuten kann und dass nicht vorschnell von einer hinreichenden Anonymisierung ausgegangen werden darf.
Von anonymisierten Daten abzugrenzen sind insbesondere pseudonymisierte Daten. Darunter versteht die DSGVO gemäß Art. 4 Nr. 5 „die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden“. Während bei den pseudonymisierten Daten der berechtigte Inhaber der zusätzlichen Informationen mittels dieser den Personenbezug wiederherstellen kann, ist die Wiederherstellung des Personenbezugs bei den anonymen Daten für jedermann zumindest praktisch unmöglich ist. Bei den pseudonymisierten Daten handelt es sich um personenbezogene Daten, auf die das Datenschutzrecht anwendbar ist (vgl. Erwägungsgrund 26 Satz 2 DSGVO).

Die Überprüfung der Anonymisierung auf ihre Validität ist eine fortwährende Aufgabe des Verantwortlichen[6], die der Kontrolle durch die Datenschutzbehörden unterliegt.

---

[4] Ziebarth, in: Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 4 Rn. 29 f.

[5] Vgl. EuGH, Urt. v. 19.10.2016 – C-582/14 – Breyer, ZD 2017, 24 (26) = MMR 2016, 842 (843); Eckhardt, in: Spindler/Schuster, Recht der elektronischen Medien, 4. Aufl. 2019, § 98 TKG, Rn. 13.

[6] Stellungnahme 5/2014 der Artikel 29-Gruppe zu Anonymisierungstechniken, WP 216, S. 4.

3. Anonymisierung als Verarbeitung

Art. 4 Nr. 2 DSGVO definiert den Begriff der Verarbeitung als „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten“ und führt einige nicht abschließende Regelbeispiele für Verarbeitungsvorgänge auf. Der Begriff wird weit verstanden und umfasst letztlich jeglichen Umgang mit personenbezogenen Daten[7].

Bei der Anonymisierung handelt es sich um einen Vorgang, der darauf gerichtet ist, dass die personenbezogenen Daten ihren Personenbezug verlieren. Dies legt den Schluss nahe, dass die personenbezogenen Daten durch die Anonymisierung – in ihrer Personenbezogenheit – verändert werden im Sinne von Art. 4 Nr. 2 Alt. 7 DSGVO.

Sollte eine „Veränderung“ im Einzelfall nicht vorliegen, würde in jedem Fall entweder der Auffangtatbestand der Verwendung (Art. 4 Nr. 2 At. 10 DSGVO) oder ein in Art. 4 Nr. 2 nicht ausdrücklich genanntes Beispiel greifen[8].
Die Anonymisierung stellt eine Verarbeitung dar und bedarf als solche einer Rechtsgrundlage[9].

4. Mögliche Rechtsgrundlagen

4.1. DSGVO

Prinzipiell kann jeder der in Art. 6 DSGVO genannten Erlaubnistatbestände in Frage kommen. Die Antwort auf die Frage, welche Rechtsnorm als Rechtsgrundlage für eine Anonymisierung konkret herangezogen werden kann, hängt von den jeweiligen Umständen des Einzelfalls ab.
Praktische Relevanz kommt jedoch vor allem folgenden Normen zu:

4.1.1. Art. 6 Abs. 1 Buchst. a) DSGVO

Mit einer wirksamen Einwilligung der betroffenen Person ist die Anonymisierung von personenbezogenen Daten gemäß Art. 6 Abs. 1 Buchst. a) DSGVO möglich.

---

[7] BeckOK DatenschutzR/Schild, 30. Ed. 1.11.2019, DS-GVO, Art. 4 Rn. 32.

[8] Hornung/Wagner, ZD 2020, 223 (224).

[9] Vgl. NRW LT-Drucks. 17/1981, S. 134; Nieders. LT-Drucks. 18/548, S. 51; Leitfaden der irischen DPC zur Anonymisierung und Pseudonymisierung (Stand: Juni 2019), S. 2 und 13, abrufbar unter: https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190614%20Anonymisation%20and%20Pseudonymisation.pdf (zuletzt abgerufen am 24.06.2020); Hansen, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Aufl. 2019, Art. 4 Nr. 5 DSGVO, Rn. 23; Roßnagel, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Aufl. 2019, Art. 4 Nr. 2 DSGVO, Rn. 12, 14.

4.1.2. Art. 6 Abs. 4 DSGVO in Verbindung mit der ursprünglichen Rechtsgrundlage

Im Regelfall werden die personenbezogenen Daten, die anonymisiert werden sollen, zu einem bestimmten anderen Zweck erhoben. Eine anschließende Anonymisierung stellt deshalb in diesen Fällen eine Weiterverarbeitung dar[10], deren Zweck mit dem ursprünglichen Erhebungszweck vereinbar sein muss, 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[11]. Erwägungsgrund 50 Satz 2 DSGVO bringt den entsprechenden Willen des Verordnungsgebers deutlich zum Ausdruck.

Für die Beurteilung der Vereinbarkeit mit dem Erhebungszweck nennt Art. 6 Abs. 4 DSGVO fünf Kriterien, die im Einzelfall einer Abwägung zugeführt und wertend zueinander in Beziehung gesetzt werden müssen. So hat der Verantwortliche zu berücksichtigen:

- jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung,
- den Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen,
- die Art der personenbezogenen Daten, insbes. ob besondere Kategorien personenbezogener Daten gemäß Art. 9 verarbeitet werden oder ob personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 verarbeitet werden,
- die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen,
- das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören können.

Hinzuweisen ist darauf, dass der datenschutzrechtlich relevante Zweck der Anonymisierung nicht die Aufhebung des Personenbezugs ist, sondern das dahinter

---

[10] Stellungnahme 5/2014 der Artikel 29-Gruppe zu Anonymisierungstechniken, WP 216, S. 8.

[11] Vgl. Kühling/Martini, EuZW 2016, 448 (451); Roßnagel, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Aufl. 2019, DSGVO, Art. 6 Abs. 4, Rn. 1; Taeger, in: Taeger/Gaben (Hrsg.), DSGVO/BDSG, 3. Aufl. 2019, Art. 6 DSGVO, Rn. 151.

stehende tatsächliche Interesse des Verantwortlichen. Sind weitgehende Verwendungen der anonymisierten Daten vorgesehen, beispielsweise im Zeitpunkt der Anonymisierung noch nicht abschließende Nutzungen im Big Data-Kontext, ist dies als Zweck anzusehen und der Abwägung zugrunde zu legen.
Erhebt ein Unternehmen beispielsweise auf Grundlage des Art. 6 Abs. 1 Buchst. b) DSGVO von seinen Kunden personenbezogene Daten zwecks der Begründung und der inhaltlichen Ausgestaltung des Vertragsverhältnisses und werden bestimmte Daten – wie Alter, Wohnort und die nachgefragte Dienstleistung – anonymisiert, um diese einer Auswertung im Hinblick auf die Verteilung der Dienstleistungen nach Alterskohorten in einer bestimmten Region zuzuführen, könnte die Abwägung wie folgt aussehen:

- Zwischen der Anonymisierung der Daten und der letztlich bezweckten Optimierung der Dienstleistungen dürfte eine hinreichende Verbindung mit dem ursprünglichen Zweck der Begründung und der inhaltlichen Ausgestaltung des Vertragsverhältnisses im Sinne des Art. 6 Abs. 4 Buchst. a) DSGVO bestehen.
- Für den nach Art. 6 Abs. 4 Buchst. b) DSGVO erforderlichen Zusammenhang spricht, dass sowohl die Erhebung der Daten als auch deren Anonymisierung bzw. die anschließende Analyse zum Zweck der Optimierung der Dienstleistungen das Vertragsverhältnis zwischen dem Unternehmen und seinen Kunden betrifft.
- Mit Blick auf die Art der personenbezogenen Daten ist gemäß Art. 6 Abs. 4 Buchst. c) DSGVO der Umstand in die Abwägung einzubeziehen, dass es sich bei den hier relevanten Bestandsdaten nicht um besonders sensible Daten handelt.
- Etwaige Folgen der mit der Anonymisierung verbundenen Weiterverarbeitung für die betroffenen Personen (Art. 6 Abs. 4 Buchst. d) DSGVO), die die Annahme einer Inkompatibilität der Weiterverarbeitung nahelegen würden, sind nicht ersichtlich.
- Angesichts der Tatsache, dass Verschlüsselung und Pseudonymisierung ausreichende Garantien i.S.d. Art. 6 Abs. 4 Buchst. e) DSGVO sein können, muss dies ebenso für die Anonymisierung gelten.

Unter Vorbehalt der Besonderheiten des Einzelfalls dürfte die Abwägung im Beispielsfall zugunsten der Zulässigkeit der Anonymisierung ausfallen.

4.1.3. Art. 6 Abs. 1 Buchst. c) i.V.m. Art. 17 Abs. 1 Buchst. a) DSGVO

Soweit die personenbezogenen Daten der Pflicht zur unverzüglichen Löschung gemäß Art. 17 Abs. 1 Buchst. a) DSGVO unterfallen, können diese ggf. auch gemäß Art. 6 Abs. 1 Buchst. c) DSGVO anonymisiert werden. Dies ist unter der Prämisse möglich, dass die Löschverpflichtung auch durch die Anonymisierung erfüllt werden kann[12].

Dafür sprechen folgende Erwägungen:

Zunächst muss hinsichtlich der Fragestellung zwischen der Verpflichtung zur Speicherbegrenzung nach Art. 5 Abs. 1 Buchst. e) DSGVO und dem Recht auf Löschung nach Art. 17 Abs. 1 DSGVO unterschieden werden.
Art. 5 Abs. 1 Buchst. e) DSGVO verlangt nicht ausdrücklich die Löschung der (personenbezogenen) Daten. Dies ergibt sich bereits aus dem Wortlaut, wonach die geforderte Speicherbegrenzung nicht auf das Speichern von Daten, sondern vielmehr nur auf die Bestimmbarkeit von personenbezogenen Daten bezogen ist. Das Löschen der Daten ist nach der Systematik der DSGVO also offenbar nur eine von mehreren Möglichkeiten, die Anforderungen des Art. 5 Abs. 1 Buchst. e) DSGVO zu erfüllen. Es ist dann nicht notwendig, wenn der Personenbezug durch Anonymisierung wirksam beseitigt werden kann[13].
Davon zu unterscheiden ist das Recht auf Löschung nach Art. 17 Abs. 1 DSGVO. Diese Vorschrift bestimmt, dass personenbezogene Daten durch den Verantwortlichen unverzüglich gelöscht werden müssen, wenn die personenbezogenen Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig 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.
Anonyme Informationen sind gemäß Erwägungsgrund 26 zur DSGVO als Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert

---

[12] Vgl. Entscheidung der österreichischen Datenschutzbehörde vom 5. 12.2018, Az.: DSB-D123.270/0009-DSB/2018, abrufbar unter: https://www.ris.bka.gv.at/Dokument.wxe?ResultFunctionToken=65180dcc-32f0-4f9a-8c2d-0c31986085b1&Position=1&Abfrage=Dsk&Entscheidungsart=Undefined&Organ=Undefined&SucheNachRechtssatz=True&SucheNachText=True&GZ=&VonDatum=01.01.1990&BisDatum=03.02.2019&Norm=&ImRisSeitVonDatum=&ImRisSeitBisDatum=&ImRisSeit=EinerWoche&ResultPageSize=100&Suchworte=&Dokumentnummer=DSBT_20181205_DSB_D123_270_0009_DSB_2018_00 (zuletzt abgerufen am 24.06.2020).

[13] S. u.a. Roßnagel, in: Simitis/Hornung/Spiecker, DSGVO, Art. 5 Rn. 155; Reimer, in: Sydow, DSGVO, Art. 5 Rn. 40

werden, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann, definiert. Für diese sollen die Grundsätze des Datenschutzes nicht gelten. Daraus folgt, dass in dem Fall, in dem nur noch anonymisierte Informationen, d.h. Informationen ohne Personenbezug, vorliegen, die Verpflichtungen aus der DSGVO und damit auch die Verpflichtung zu einer etwaigen weitergehenden Speicherbegrenzung aus Art. 5 Abs. 1 Buchst. e) DSGVO nicht greifen. Ungeachtet der Ausführungen in Erwägungsgrund 26 bestünde nach vorgenommener wirksamer Anonymisierung eine weitergehende Verpflichtung aus Art. 5 Abs. 1 Buchst. e) DSGVO mangels Vorliegens des Tatbestandsmerkmals der personenbezogenen Daten nicht. Ab diesem Zeitpunkt werden keine personenbezogenen Daten im Sinne des Art. 2 Abs. 1 DSGVO mehr verarbeitet.
Gegen die Möglichkeit der Erfüllung der Löschverpflichtung durch die Anonymisierung könnte argumentiert werden, dass bei der Anonymisierung im Vergleich zur Löschung ein Restrisiko der Re-Identifizierung verbleibe. Demgegenüber lässt sich jedoch anführen, 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. Diese Argumentation lässt sich auch auf den Anspruch auf Löschung nach Art. 17 DSGVO übertragen.
Aus Sicht des BfDI kann die Verpflichtung zur Löschung personenbezogener Daten nur dann durch die Anonymisierung erfüllt werden, wenn die personenbezogenen Daten rechtmäßig erhoben wurden (vgl. Art. 17 Abs. 1 Buchst. a) DSGVO).

4.2. Spezialgesetzliche Datenschutzvorschriften am Beispiel des TKG

Die Anonymisierung kann sich – soweit einschlägig – nach den spezialgesetzlichen Normen richten. Beispielsweise sind für die Verarbeitung von Verkehrsdaten im Sinne des § 3 Nr. 30 TKG, also Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden, die §§ 91 ff. TKG maßgeblich.

4.2.1. § 96 Abs. 3 TKG

Die teilnehmerbezogenen Verkehrsdaten dürften unter den Voraussetzungen des § 96 Abs. 3 Satz 1 TKG zum Zwecke der Vermarktung von Telekommunikations-

diensten, zur bedarfsgerechten Gestaltung von Telekommunikationsdiensten oder zur Bereitstellung von Diensten mit Zusatznutzen anonymisiert werden, sofern der Betroffene in diese Verwendung eingewilligt hat.

4.2.2. § 98 Abs. 1 TKG

Standortdaten dürfen nach § 98 Abs. 1 Satz 1 TKG im zur Bereitstellung von Diensten mit Zusatznutzen erforderlichen Umfang und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden, wenn sie anonymisiert wurden oder wenn der Teilnehmer dem Anbieter des Dienstes mit Zusatznutzen seine Einwilligung erteilt hat. Im Umkehrschluss aus § 98 Abs. 1 Satz 1 Alt. 1 TKG bedeutet dies, dass Standortdaten der Verarbeitung in Form einer Anonymisierung zugeführt werden dürfen, wenn und soweit dies zur Bereitstellung von Diensten mit Zusatznutzen erforderlich ist. Nach § 3 Nr. 5 TKG sind dies Dienste, die die Erhebung und Verwendung von Standortdaten in einem Maße erfordern, das über die Übermittlung einer Nachricht hinausgeht. Es handelt sich um Dienste, die mit einem Zusatznutzen für Nutzer verbunden sind. Ein klassisches Beispiel hierfür sind die Ortungs-Dienste.

4.2.3. § 96 Abs. 1 Satz 2 Alt. 2 i.V.m. § 96 Abs. 1 Satz 3 TKG

Nach § 96 Abs. 2 Satz 2 Alt. 2 TKG dürfen die Verkehrsdaten nur verwendet werden, soweit dies für die durch andere gesetzliche Vorschriften begründeten Zwecke erforderlich ist. Insofern verpflichtet § 96 Abs. 1 Satz 3 TKG den Diensteanbieter die Verkehrsdaten nach Beendigung der Verbindung unverzüglich zu löschen. Da die personenbezogenen Daten auch durch deren Anonymisierung gelöscht werden können[14], ist die Anonymisierung von Verkehrsdaten gemäß § 96 Abs. 1 Satz 2 Alt. 2 TKG möglich.

5. Transparenz

Die Transparenz der Verarbeitung personenbezogener Daten zum Zweck ihrer Anonymisierung ist entsprechend den einschlägigen Vorschriften zu gewährleisten. Dies bedeutet vor allem, dass der Verantwortliche gemäß Art. 13 Abs. 1 Buchst. c) und Art. 14 Abs. 1 Buchst. c) DSGVO der betroffenen Person die Zwecke, für die die personenbezogenen Daten anonymisiert werden sollen, sowie die Rechtsgrundlage für die Anonymisierung mitzuteilen hat. Gemäß Art. 13 Abs. 3

[14] Da das TKG weder den Begriff der Löschung noch den der Anonymisierung definiert, kann an dieser Stelle auf die Ausführungen zur DSGVO verwiesen werden, vgl. oben unter 4.1.3.; die Richtlinie 2002/58/EG (E-Privacy-RL) enthält diesbezüglich ebenfalls keine begrifflichen Festlegungen, sodass die Begriffsbestimmungen der DSGVO gelten, vgl. Art. 2 Abs. 1 E-Privacy-RL i.V.m. Art. 94 Abs. 2 S. 1 DSGVO.

DSGVO gilt dies auch in den Fällen, in denen die Anonymisierung eine Weiterverarbeitung darstellt.

6. Datenschutz-Folgenabschätzung

Gemäß Art. 35 Abs. 1 DSGVO ist eine Datenschutz-Folgenabschätzung durchzuführen, wenn eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Bei einer Anonymisierung muss der Verantwortliche in der Regel davon ausgehen, dass ein hohes Risiko besteht, weil bei der Anonymisierung eben regelmäßig das Kriterium "Verarbeitung in großem Umfang" und zumindest aktuell immer noch das Kriterium "neue Technologien" zutreffen.
Die Notwendigkeit der Durchführung einer Datenschutz-Folgenabschätzung ist insbesondere deshalb begründet, weil die Generierung eines anonymen Datenbestandes eine komplexe Aufgabe des Verantwortlichen darstellt und viele Fehlerquellen birgt. Dabei hat der Verantwortliche darüber hinaus die Folgen einer möglichen De-Anonymisierung in die Betrachtung einzubeziehen.

Vor einer Anonymisierung ist in der Regel eine Datenschutz-Folgenabschätzung durchzuführen.

7. Zusammenfassung

Die Anonymisierung personenbezogener Daten ist – auch im TK-Sektor – grundsätzlich möglich, sofern sie sich auf eine Rechtsgrundlage stützen lässt. Ob dies der Fall ist, ist unter Berücksichtigung aller Umstände im Einzelfall zu beurteilen. Besonderes Augenmerk verdient dabei die Validität des eingesetzten Anonymisierungsverfahrens. Die Validität der Anonymisierung bedarf einer kontinuierlichen Überprüfung durch den Verantwortlichen.

Eine Anonymisierung …

- liegt vor, wenn der Personenbezug von Daten derart aufgehoben ist, dass er nicht oder nur unter unverhältnismäßigem Aufwand an Zeit, Kosten und Arbeitskräften wiederhergestellt werden kann.
- stellt eine Verarbeitung personenbezogener Daten dar und bedarf als solche einer Rechtsgrundlage.

Je nach Kontext und Zweck der Anonymisierung kommen mehrere Rechtsgrundlagen in Betracht, im Bereich der DSGVO insbesondere der Tatbestand der kompatiblen Weiterverarbeitung (Art. 6 Abs. 4 DSG-VO i.V.m. der ursprünglichen Rechtsgrundlage) und die Erfüllung einer rechtlichen Verpflichtung (Art. 6 Abs. 1 Buchst. c) DSGVO).

Eine Verpflichtung zur unverzüglichen Löschung ist durch eine Anonymisierung erfüllbar.