Öffentliche Konsultation zum Thema: „Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche“

Sehr geehrte Damen und Herren,

Telefónica begrüßt die vom BfDI angestoßene öffentliche Konsultation zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche und bedankt sich für die Gelegenheit, zu diesem wichtigen und praxisrelevanten Thema Stellung zu nehmen.
Sowohl die Bundesregierung als auch die EU-Kommission treiben mit der Datenstrategie[1] und der KI-Strategie[2] die Nutzung von Daten unter anderem für gesellschaftlichen Wohlstand und Teilhabe, für eine prosperierende Wirtschaft oder den Schutz von Umwelt und Klima voran. Aktuelle Ereignisse zeigen, dass eine verantwortungsvolle Nutzung von Daten auch erforderlich sein kann, um gesundheitliche Bedrohungen zu bekämpfen. Auch die DSGVO

---

[1] Eckpunkte einer Datenstrategie der Bundesregierung, abrufbar unter: https://www.bundesregierung.de/resource/blob/997532/1693626/e617eb58f3464ed13b8ded65c7d3d5a1/2019-11-18-pdf-datenstrategie-data.pdf; Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Eine europäische Datenstrategie, 19.2.2020, COM(2020) 66 final, abrufbar unter: https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_de.pdf.

[2] Strategie Künstliche Intelligenz der Bundesregierung, November 2018, abrufbar unter: https://www.bmbf.de/files/Nationale_KI-Strategie.pdf; Europäische Kommission, Weissbuch „Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen“, 19.2.2020, COM(2020) 65 final, abrufbar unter: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_de.pdf.

selbst hat das erklärte Ziel, mit ihrem Rechtsrahmen einen Beitrag zum Wachstum der digitalen Wirtschaft im Binnenmarkt zu leisten (vgl. Erwägungsgrund 7 DSGVO). Dass dies selbstverständlich in einem verantwortungsvollen Rahmen und entsprechend den Regelungen der anwendbaren Datenschutzvorschriften erfolgen muss, ergibt sich für die Unternehmen schon aus ihrem Eigeninteresse, die Inanspruchnahme ihrer Produkte und Dienstleistungen für den Kunden vertrauenswürdig zu gestalten. Auch bei Telefónica ist ein vertrauensvoller Umgang mit unseren Kunden und damit auch ihren personenbezogenen Daten zentral und damit Teil der Geschäftsgrundsätze, die unser Handeln bestimmen.[3]

Immer mehr Anwendungen, die unser Leben vereinfachen, beruhen auf der Analyse von Daten: Internet-Suchen führen in Millisekunden zu passenden Ergebnissen, Pakete kommen zur Wunschzeit an und Spam-Filter blockieren unerwünschte E-Mails durch Erkennung von Textmustern. Die Grundlage dafür sind statistische Verfahren. Sie können Daten auf wiederkehrende Muster untersuchen und so wertvolle Informationen daraus ableiten. Dabei gilt ein einfacher Zusammenhang: Je umfangreicher die Datengrundlage ist, desto deutlicher sind die Muster und desto verlässlicher werden die abgeleiteten Erkenntnisse.

Intelligent verknüpft ergeben sich aus anonymisierten Daten wichtige Erkenntnisse, die für Unternehmen aus den unterschiedlichsten Branchen oder für wissenschaftliche Zwecke, ebenso wie für Kommunen, öffentliche Verkehrsbetriebe und die Gesellschaft insgesamt relevant sind.

Da durch die zunehmende Digitalisierung immer mehr Daten anfallen, werden auch die Einsatzmöglichkeiten für statistische Anwendungen immer vielseitiger. Doch gleichzeitig ergeben sich daraus auch neue Anforderungen: Es gilt, den verantwortungsvollen Umgang mit Daten sicherzustellen, damit der nachhaltige Schutz der Privatsphäre eines jeden Einzelnen gewährleistet ist. Telefónica arbeitet seit vielen Jahren an neuen Standards, um digitale Technologien sicherer und transparenter zu machen. Jeder soll seine Daten sicher wissen und sein digitales Leben selbst gestalten können.

Wir unterstützen daher das Anliegen des BfDI, durch die Konsultation im Dialog zu einem praxisgerechten Beurteilungsrahmen der Anonymisierung im Einklang mit den datenschutzrechtlichen Vorgaben zu gelangen. Nicht zuletzt sollte die Konsultation auch dazu beitragen, den Unternehmen mehr Rechtssicherheit hinsichtlich der anzuwendenden Rechtsvorschriften zu geben.

---

[3] https://www.telefonica.de/unternehmen/ueber-telefonica/geschaeftsgrundsaetze.html (Stand: 5.3.20).

Vor diesem Hintergrund erlauben wir uns, durch die nachfolgenden Anmerkungen auf Punkte hinzuweisen, die aus unserer Sicht weiterer Ausführungen bedürfen.

Anforderungen an eine Anonymisierung i. S. der DSGVO

Telefónica begrüßt, dass der BfDI von einem relativen Anonymitätsbegriff ausgeht. Diese Auslegung steht in völligem Einklang mit dem Begriffsverständnis, das der EuGH zur insoweit vergleichbaren Rechtslage nach der Richtlinie 95/46/EG entwickelt hat[4]. Sie entspricht im Übrigen schon dem Wortlaut von Erwägungsgrund 26 DSGVO, der klarstellt, dass die Identifizierbarkeit einer natürlichen Person nicht absolut zu bewerten ist, sondern vielmehr von einer Bewertung der Wahrscheinlichkeit abhängt, mit der Mittel zur Identifizierung (die grundsätzlich durchaus bestehen können) auch tatsächlich genutzt werden. Die Wahrscheinlichkeitsbewertung muss sich dabei an objektiven Faktoren wie den Kosten der Identifizierung und dem dafür erforderlichen Zeitaufwand unter Berücksichtigung der jeweils aktuell verfügbaren Technologie sowie technischen Entwicklungen orientieren.

Erwägungsgrund 26 DSGVO gibt somit Hinweise auf den Maßstab, der anzulegen ist, um zu ermitteln, wann unter der DSGVO von einer ausreichenden Anonymisierung auszugehen ist. Der BfDI weist zurecht darauf hin, dass Anonymisierung eine „fortwährende Aufgabe" ist und betont die Rolle des Verantwortlichen in diesem Zusammenhang. Allerdings bietet das Konsultationspapier dem Verantwortlichen keinerlei Hilfestellung, wie diese Aufgabe in der Praxis zu bewältigen ist, und schafft somit in einer entscheidenden Frage bisher keine Rechtssicherheit.

Das Konsultationspapier sollte daher um einen Handlungsspielraum ergänzt werden, die zur Erreichung einer wirksamen Anonymisierung entsprechend den Vorgaben der DSGVO umgesetzt werden können. Dazu sollten Kriterien und Vorgehensweisen definiert werden, die es erlauben, das Risiko der Reidentifizierung zu bestimmen und Maßnahmen festzulegen, mit denen dieses Risiko auf ein Maß reduziert werden kann, das es hinreichend unwahrscheinlich i. S. des Erwägungsgrunds 26 Satz 3 DSGVO erscheinen lässt, dass Mittel zur Identifizierung einer natürlichen Person genutzt werden. Gleichzeitig muss es den Unternehmen Handlungsspielräume für technische Entwicklungen und unternehmerisch Innovationen lassen.

Kriterien zur Bestimmung dieses Risikos bzw. geeigneter Abhilfemaßnahmen könnten aus unserer Sicht insbesondere sein:

---

[4] EuGH, Urt. v. 19.10.2016, Rs. C-582/14 – *Breyer*.

- Existenz von Zusatzwissen beim Verantwortlichen / Dritten, rechtliche Zulässigkeit einer Verknüpfung der Daten mit diesem Zusatzwissen und Geeignetheit des Zusatzwissens zur Re-identifizierung
- Ressourcen möglicher Tätergruppen:
  - Kosten einer Reidentifizierung
  - Zeitaufwand für eine Reidentifizierung
- Informationswert für die möglichen Tätergruppen / Interessenten
- Möglichkeiten zur alternativen Informationsbeschaffung und deren Aufwand
- Auswirkungen ergriffener technischer und/oder organisatorischer Maßnahmen zur Erschwerung einer Identifizierung, z. B.:
  - Stärke einer vorhandenen Verschlüsselung oder anderer technischer Maßnahmen zur Verhinderung der Verarbeitung der Daten
  - Differenzierte Verteilung von Zugriffsrechten auf verschiedene Stufen des Anonymisierungsverfahrens
  - Unumkehrbarkeit eines Hashings oder anderer Maßnahmen zur Entfernung/zum Ersatz identifizierender Merkmale
  - Vertragliche Vereinbarungen mit Empfängern der Daten/Verpflichtungen von Mitarbeitern bzgl. der Weiterverarbeitung

In diesem Zusammenhang sollte auch dargelegt werden, welche Verhaltensweisen in die Risikobetrachtung grundsätzlich einbezogen werden müssen. So hat der EuGH im Urteil in der Rechtssache *Breyer*[5] lediglich auf die rechtlichen Möglichkeiten für einen Zugriff auf Zusatzwissen abgestellt, mit dem die Inhaber einer IP-Adresse für einen Websitebetreiber identifiziert werden konnten. Rein technische Möglichkeiten, auf dieses Zusatzwissen rechtswidrig Zugriff zu erlangen, wie etwa Hackingszenarien, waren nicht Gegenstand der Betrachtung.

Anonymisierung als Verarbeitung: Erforderlichkeit einer Rechtsgrundlage zur Anonymisierung

Zur alten Rechtslage ging die BfDI in ihrem Tätigkeitsbericht für 2015 und 2016 vor Geltung der DGVO davon aus, dass die Anonymisierung – welche in § 3 Abs. 6 BDSG a. F. eigenständig und getrennt von den Begriffen des Erhebens, Verarbeitens und Nutzens definiert war – keine Verarbeitung darstellt und deshalb keiner Rechtsgrundlage bedarf.

Durch den Geltungsbeginn der DS-GVO haben sich an dieser datenschutzrechtlichen Bewertung nach unserem Verständnis keine grundlegenden Änderungen ergeben. Der

---

[5] EuGH (o. Fußn. 5).

Begriff der Verarbeitung gemäß Art. 4 Nr. 2 DS-GVO entspricht materiell den durch die Begriffe des Erhebens, Verarbeitens und Nutzens i. S. des § 3 Abs. 3 bis 5 BDSG a. F. beschriebenen Vorgängen im Zusammenhang mit personenbezogenen Daten. Das Anonymisieren unterfiel schon bisher nicht diesen Begriffen, sondern der gesonderten Definition in § 3 Abs. 6 BDSG a. F.

Auch in der Richtlinie 95/46/EG (Datenschutzrichtlinie), deren Umsetzung die Vorschriften des BDSG a. F. dienten, war die Anonymisierung weder in der Definition der Verarbeitung gemäß Art. 2 lit. b noch an anderer Stelle im regelnden Teil erwähnt. Ausschließlich in Erwägungsgrund 23 der Datenschutzrichtlinie fanden sich Hinweise, wann bei diesem rein technischen Vorgang der Entfernung des Personenbezugs von einer Anonymisierung und damit von einer Nichtanwendbarkeit der Richtlinie auszugehen ist. In gleicher Weise beschreibt dies nun Erwägungsgrund 26 DS-GVO. Mit Art. 4 Nr. 2 der DS-GVO hat der Verordnungsgeber die bisherige Definition und materiell-rechtliche Ausgestaltung des Begriffs der „Verarbeitung" der Datenschutzrichtlinie übernommen. Zwar hat der Verordnungsgeber weitere Regelbeispiele aufgezählt, jedoch keine wesentlichen Änderungen der Definition vorgenommen. Insbesondere hat der Verordnungsgeber nicht die Anonymisierung als Regelbeispiel aufgenommen.

Einer gesonderten Rechtsgrundlage für die Anonymisierung personenbezogener Daten im Sinne des Erwägungsgrundes 26 DS-GVO bedarf es somit auch unter Geltung der DS-GVO aus unserer Sicht nicht.

Zugleich halten wir jedoch die im Konsultationspapier geäußerte Rechtsauffassung nicht für grundsätzlich unvertretbar. Denn auch die Anonymisierung lässt sich im weiteren Sinne als Vorgang oder Vorgangsreihe „im Zusammenhang mit personenbezogenen Daten" begreifen, der als von der Definition der „Verarbeitung" gemäß Art. 4 Nr. 2 DSGVO umfasst sein kann. Folgte man dieser Auffassung, so bedürfte die Anonymisierung einer eigenständigen Rechtsgrundlage. Auf dieser Prämisse gründen die weiteren Ausführungen:

Mögliche Rechtsgrundlagen der Anonymisierung nach der DSGVO

Das Konsultationspapier legt in Abschnitt 3 dar, dass grundsätzlich jeder der in Art. 6 DSGVO genannten Erlaubnistatbestände als Rechtsgrundlage für die Anonymisierung von personenbezogenen Daten in Betracht kommt.[6] Die Klarstellung, dass jede Anonymisierung einer Rechtsgrundlage nach Art. 6 DSGVO bedarf, ist insbesondere aus Sicht des TK-Sektors

---

[6] BfDI, Öffentliches Konsultationsverfahren des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Thema: Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche, S. 6.

begrüßenswert, da sie Rechtssicherheit auch hinsichtlich der Voraussetzungen einer Anonymisierung von Telekommunikationsdaten schafft: Zwar grenzt Art. 95 DSGVO den Anwendungsbereich der DSGVO hinsichtlich der Datenverarbeitung im Bereich der Telekommunikation ein. Er bestimmt aber lediglich, dass Telekommunikationsunternehmen in Verbindung mit der Bereitstellung öffentlich zugänglicher Telekommunikationsdienste in öffentlichen Telekommunikationsnetzen durch die DSGVO keine zusätzlichen Pflichten auferlegt werden. Dagegen kann die DSGVO durchaus zusätzliche, in der ePrivacy-Richtlinie nicht vorgesehene Rechtsgrundlagen definieren, um die Verarbeitung (insbesondere die Anonymisierung) von Telekommunikationsdaten zu erleichtern.

Die im Konsultationspapier genannten Beispielsfälle bedürfen jedoch – mit Blick auf die gewünschte Auswahl nach ihrer praktischen Relevanz – aus unserer Sicht noch der Ergänzung.

Anonymisierung zur Erfüllung des Grundsatzes der Speicherbegrenzung, Art. 6 Abs. 1 lit. c, Art. 5 Abs. 1 lit. e, Abs. 2 DSGVO

Soweit in Abschnitt 3. 3) i) (3) auf Art. 6 Abs. 1 lit. c i. V. m. Art. 17 Abs. 1 DSGVO als Rechtsgrundlage Bezug genommen wird, sollte diese Überschrift – auch in Anbetracht der weiteren Ausführungen des BfDI in diesem Abschnitt – modifiziert werden: Die Rechtsgrundlage der Anonymisierung ergibt sich in dem hier beschriebenen Fall nicht aus einer gesetzlichen Pflicht zur Löschung gemäß Art. 17 Abs. 1 DSGVO, sondern vielmehr aus dem weitergehenden Grundsatz der Speicherbegrenzung gemäß Art. 5 Abs. 1 lit. e DSGVO, wie der BfDI im weiteren Verlauf zurecht ausführt.

Nach diesem Grundsatz sind personenbezogene Daten so zu speichern, dass die Identifizierung der betroffenen Personen nur so lange möglich ist, wie dies für die Verarbeitungszwecke erforderlich ist. Die Einhaltung dieses Grundsatzes muss gemäß Art. 5 Abs. 2 DSGVO der Verantwortliche gewährleisten. Die Anforderung stellt somit eine direkte rechtliche Verpflichtung des Verantwortlichen dar, die sich unmittelbar aus der DSGVO ergibt. Zu ihrer Erfüllung ist es erforderlich, die relevanten Daten zu anonymisieren. Der Grundsatz der Speicherbegrenzung fordert insbesondere sowohl vom Wortlaut als auch vom Sinn und Zweck keine Löschung der Daten, sondern eine Begrenzung der personenbezogenen Speicherung, die insbesondere durch eine Anonymisierung umgesetzt werden kann. Grundsätzlich ist damit der Verantwortliche direkt aus dem o.g. Grundsatz verpflichtet, und daher die Anonymisierung jedenfalls gemäß Art. 6 Abs. 1 lit. c i. V. m. Art. 5 Abs. 1 lit. e, Abs. 2 DSGVO zulässig.

Mit der rechtmäßigen Anonymisierung personenbezogener Daten im Einklang mit dieser Verpflichtung ist dem Grundsatz der Speicherbegrenzung gemäß Art. 5 Abs. 1 lit. e DSGVO Genüge getan. Soweit die Anonymisierung durch Löschen identifizierender Merkmale durchgeführt wird, kann damit zugleich einer Pflicht zur Löschung gemäß Art. 17 Abs. 1

DSGVO entsprochen werden. Telefónica stimmt in dieser Hinsicht der Auffassung der österreichischen Datenschutzbehörde[7] zu, dass eine Anonymisierung insoweit der Löschung personenbezogener Daten datenschutzrechtlich gleichsteht und begrüßt daher ausdrücklich, dass auch der BfDI dieser Ansicht im Ergebnis zu folgen scheint. Der Anwendungsbereich des Art. 17 Abs. 1 DS-GVO ist ansonsten schon gar nicht gegeben, wenn keine personenbezogene Daten mehr vorliegen, weil sie bereits entsprechend dem Grundsatz der Speicherbegrenzung anonymisiert wurden.

Aus unserer Sicht entspricht dieser Ansatz dem Geist der DSGVO voll und ganz. Denn Sinn und Zweck der datenschutzrechtlichen Vorschriften ist nicht, Daten grundsätzlich zu vernichten und sie so von jeder Nutzung auszuschließen, sondern die Rechte und Freiheiten der betroffenen Personen zu schützen, um so gerade die Vertrauensbasis zu schaffen, auf der sich die digitale Wirtschaft entfalten kann (vgl. zum Beispiel Art. 1 Abs. 2 DS-GVO „freier Verkehr von Daten“). Die Nutzbarmachung vormals personenbezogener Daten nach ihrer Anonymisierung setzt diesen Schutzgedanken vollständig um, soweit sichergestellt ist, dass das Anonymisierungsverfahren den Personenbezug dauerhaft und vollständig entfernt und dieser Personenbezug auch bei einer Weitergabe an Dritte nicht wiederhergestellt werden kann.[8]

Ein darüberhinausgehendes Recht der betroffenen Person auf bzw. eine Pflicht des Verantwortlichen zur Löschung gemäß Art. 17 Abs. 1 DSGVO besteht hinsichtlich dieser anonymisierten Daten nicht, da diese – wie im Konsultationspapier dargelegt– keinen Personenbezug mehr aufweisen und somit nicht den Vorschriften der DSGVO unterliegen.

Anonymisierung zur Wahrnehmung eines berechtigten Interesses, Art. 6 Abs. 1 lit. f DSGVO

Das Konsultationspapier lässt Ausführungen zu einer weiteren Rechtsgrundlage vermissen, die aus unserer Sicht in der Praxis von hoher Relevanz ist: Die Rechtmäßigkeit einer Anonymisierung kann sich auch daraus ergeben, dass sie gemäß Art. 6 Abs. 1 lit. f DSGVO zur Wahrnehmung eines berechtigten Interesses erforderlich ist. Insbesondere soweit personenbezogene Daten beim Verantwortlichen noch nicht einer gesetzlichen Pflicht zur Anonymisierung im Sinne des Grundsatzes der Speicherbegrenzung unterliegen, kann Art. 6 Abs. 1 lit. f DSGVO eine geeignete Rechtsgrundlage darstellen, wenn sich aus einer Interessensabwägung ergibt, dass es zur Wahrnehmung berechtigter Interessen erforderlich

---

[7] Datenschutzbehörde (Österreich), Bescheid v. 5.12.2018, Gz. DSB-D123.270/0009-DSB/2018, abrufbar unter: https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20181205_DSB_D123_270_0009_DSB_2018_00/DSBT_20181205_DSB_D123_270_0009_DSB_2018_00.html

[8] Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, WP216, S. 6.

ist, personenbezogene Daten in anonymisierter Form auszuwerten und nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen.

In diesen Fällen wird sich der Zweck der Anonymisierung oftmals nicht erst nachträglich ergeben, so dass die vom BfDI angeführte Legitimierung gemäß Art. 6 Abs. 4 i. V. m. der ursprünglichen Rechtsgrundlage nicht zur Verfügung steht. Vielmehr dürfte die vorgesehene Anonymisierung zur weiteren Auswertung der Daten – neben den sonstigen Zwecken der Verarbeitung, die sich z. B. aus einem Vertrag mit der betroffenen Person ergeben können – häufig bereits bei Erhebung als Zweck feststehen. Vorausgesetzt, dass die Verarbeitung zur Wahrnehmung des berechtigten Interesses erforderlich ist und die Interessen oder Grundrechte und -freiheiten der betroffenen Personen nicht überwiegen, können die Daten dann auf der Grundlage von Art. 6 Abs. 1 lit. f DSGVO für die weitere Verwendung anonymisiert werden, ohne dass es hierzu eines Kompatibilitätstests bedürfte. Eine Darstellung dieses Falls fehlt im Konsultationspapier bislang.

Spezialgesetzliche Datenschutzvorschriften des TKG

Wie das Konsultationspapier richtig feststellt, enthält das TKG weitere, spezialgesetzliche Erlaubnistatbestände für eine Anonymisierung. Es sollte allerdings klargestellt werden, dass daneben auch alle anderen sich aus Art. 6 Abs. 1 DSGVO ergebenden Rechtsgrundlagen weiter anwendbar bleiben.

Art. 6 Abs. 1 lit. c DSGVO i. V. m. § 96 Abs. 1 Satz 3 TKG

Der relevanteste Erlaubnistatbestand des TKG dürfte § 96 Abs. 1 Satz 3 TKG sein, der eine gesetzliche Pflicht zur Löschung von Verkehrsdaten enthält. Die Vorschrift dient der Umsetzung von Art. 6 Abs. 1 Richtlinie 2002/58/EG, in der allerdings eine Pflicht zur Löschung *oder Anonymisierung* normiert ist. Art. 6 Abs. 1 Richtlinie 2002/58/EG stellt damit eine spezialgesetzliche Ausprägung des Grundsatzes der Speicherbegrenzung gemäß Art. 5 Abs. 1 lit. e DSGVO dar.

Im Sinne des oben dargestellten Begriffsverständnisses, dass eine Löschung auch durch eine Anonymisierung erfolgen kann, genügt der Wortlaut von § 96 Abs. 1 Satz 3 TKG der Richtlinienvorgabe.

Allerdings sind daneben auch andere Formen der Anonymisierung denkbar, die nicht in der Löschung identifizierender Merkmale bestehen, sondern z. B. in der Aggregierung personenbezogener Daten zu einer – nicht mehr auf einzelne Personen beziehbare – Gruppenaussage (k-Anonymität). In diesen Fällen handelt es sich nicht um eine Löschung, sondern um eine Veränderung personenbezogener Daten, durch die gleichwohl der Personenbezug entfernt und damit eine Anonymisierung erreicht wird. Diese Fälle sind auch bei Zugrundelegung des dargelegten Begriffsverständnisses nicht vom Wortlaut des § 96 Abs. 1 Satz 3 TKG umfasst.

§ 96 Abs. 1 Satz 3 TKG ist daher richtlinienkonform dahingehend auszulegen, dass die in der Norm niedergelegte Pflicht in jedem Fall auch durch eine Anonymisierung der Verkehrsdaten erfüllt werden kann. Dies ergibt sich auch aus der Systematik der Richtlinie 2002/58/EG. Denn Art. 6 der Richtlinie benennt die Anonymisierung als gleichberechtigte Alternative zur Löschung von Verkehrsdaten, wenn diese zu den erlaubten Zwecken nicht mehr erforderlich sind.[9]

§ 96 Abs. 3 TKG und § 98 Abs. 1 TKG

Eine Anonymisierung ist selbstverständlich auch darüber hinaus in den Fällen zulässig, in denen das TKG die Verarbeitung erlaubt. Dies betrifft zum einen die Verarbeitung von teilnehmerbezogenen Verkehrsdaten für bestimmte werbliche Zwecke mit Einwilligung des Teilnehmers gemäß § 96 Abs. 3 TKG. Die Einwilligung sollte sich in diesen Fällen auch auf die Anonymisierung beziehen. Andernfalls kann eine Anonymisierung aber weiterhin auch auf Art. 6 Abs. 1 lit. c DSGVO i. V. m. § 96 Abs. 1 Satz 3 TKG gestützt werden, soweit die Voraussetzungen vorliegen.

Zum anderen dürfen auch Standortdaten, die in Bezug auf die Nutzer von öffentlichen Telekommunikationsnetzen oder öffentlich zugänglichen Telekommunikationsdiensten verwendet werden, gemäß § 98 Abs. 1 Satz 1 Alt. 1 TKG im zur Bereitstellung von Diensten mit Zusatznutzen erforderlichen Umfang anonymisiert werden. Selbstverständlich können auch Standortdaten, die bereits auf einer anderen Rechtsgrundlage anonymisiert worden sind, (unter anderem) für die Bereitstellung von Diensten mit Zusatznutzen verwendet werden.

Es sollte daher klargestellt werden, dass diese Vorschriften als zusätzliche, spezialgesetzliche Rechtsgrundlagen einer Anonymisierung zur Verfügung stehen, die weder zu anderen Rechtsgrundlagen in einem Vorrangverhältnis stehen noch diese sperren.

---

[9] In diesem Sinne auch Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, WP216, S. 8.