Sehr geehrte Damen und Herren,

bitte entnehmen Sie meine Stellungnahme und rechtlichen Bedenken - insbesondere zu einzelnen Interpretationen in dem vorgelegten Papier - aus meinen Anmerkungen, die ich direkt in Ihr Dokument eingefügt habe, rot und gelb markiert.

Zusammenfassend möchte ich festhalten:
Wenn anonymisierte Daten in einer Krise, so wie durch Covid19, hilfreich sein könnten und im Sinne einer Verarbeitung und Nutzung nach Art. 6 Abs. 1 S. 1 lit. e) DSGVO im öffentlichen Interesse liegt, so ist das grundsätzlich absolut sinnvoll. Wir sollten ja eh jedwede Technik bestenfalls für eine gesunde und starke Gemeinschaft einsetzen. Dafür bedarf es einer hochentwickelten Gesellschaft. Der gute alte Missbrauch zählt aber leider nicht dazu, und Wirtschaftskriminalität inkl. Datenmissbrauch ist leider immer noch nachhaltig einer der größten Wachstumsmärkte überhaupt. Faktisch leben wir in einer Zeit, in der die Wirtschaft bei weitem nicht ihre Vertrauenswürdigkeit bewiesen hat. Die bräuchte es aber für umfänglichen technischen Nutzen.

Der Nutzen von personenbezogenem Datenschutz muss mit größtmöglicher Achtsamkeit dem Nutzen von anonymisierten Nutzung gegenübergestellt werden. Bestenfalls unter Berücksichtigung folgender Punkte:

1. Anonymisierte Nutzung ohne nachweisbare zwanglose Einwilligung der Grundrechtsträger darf meines Erachtens nach nur in begründeten Ausnahmefällen rechtmäßig sein. Bevor also über die Verlässlichkeit von Anonymisierung entschieden wird, ist über die gesonderte Ausnahme zu entscheiden.
Die Corona-Krise zu bewältigen, liegt definitiv im öffentlichen Interesse. Mit allen Mitteln, aber nicht um jeden Preis.

2. Da der Nutzen der Anonymisierung unserer Daten für die Summe aller Grundrechtsträger deutlich überwiegend sein muss, dürfen die Risiken der Freigabe zur Verarbeitung von personenbezogenen Daten zwecks Anonymisierung nicht leichtfertig vernachlässigt werden. Außer in Krisen z.B., in denen sich ein für alle infizierten Personen tödliches Virus derart verbreiten würde, dann -aber auch nur dann- muss auch das gesetzliche Handeln radikal sein können. Ich denke, in Deutschland haben wir entsprechende Notstandsregelungen, die ausreichend Basis bieten. Eine andere schwere Krise könnte ein Krieg oder Angriff mit verschiedensten technischen, chemischen und/oder digitalen Mitteln sein. Spätestens da möchte man doch meinen: Feuer frei für staatliche Datennutzung. Wenn man nicht wüsste, dass in den schwersten Zeiten sich gerne auch der schwerste Missbrauch ausbreitet.

3. In allen nicht derart radikalen Fällen ist die Sicherheit von Anonymisierung vs. Pseudoanonymisierung mit Achtsamkeit und Konsequenz zu verfolgen. Die größte technische Herausforderung liegt aber gar nicht darin, ein geeignetes technisches Mittel zu finden, sondern in der Nachhaltigkeit und damit zwangsläufig Anpassungsfähigkeit technischer Sicherstellung.
Achtsamkeit: Die technischen Sicherstellungsmittel müssen konstant überprüft und angepasst werden, auch für abgeschlossene Verfahren.
Konsequenz: Die Aufsichtsbehörden müssen das Ausnutzen von Unternehmen solcher Freigaben, den Missbrauch und auch bereits Verstöße mit Geldbußen, Sanktionen und insbesondere persönlichen strafrechtlichen Klageverfahren nach Art. 42 Abs. 1 und 2 BDSG gegen die hauptverantwortlichen Personen, primär Vorstandsvorsitzende und Geschäftsführung - das Gesetz bietet die Möglichkeit dazu - derart abschreckend ahnden, dass es tatsächlich abschreckt.
Hier sehe ich die aktuell größte Gefahr: Deutsche Datenschutzaufsichtsbehörden sind weit entfernt von wirksamem Datenschutz, wie ich in Kürze beweisen werde. Leider, denn anders wär es mir lieber.

Ob Corona oder Krieg - und Wirtschaftsmissbrauch ist für beides fast immer ursächlich: Ohne die Gemeinschaft ist die Wirtschaft nichts. Ist die Gemeinschaft krank, ist es die Wirtschaft auch. Vernachlässigung von Ahndung und Konsequenz: Die DSGVO richtet sich nicht nach schlechten Gewohnheiten. Sie ist eine Folge davon.

Fazit und Vorschlag:

Bitte überdenken Sie einige Ihrer Ausführungen, s.a. meine Anmerkungen im Dokument.

Machen Sie, die Datenschutzaufsichtsbehörde, in Sonderfällen nach Art. 6 Abs. 1 S. 1 lit. e) DSGVO die Unternehmen, die jeweils je nach Krise notwendige personenbezogenen Daten verarbeiten und nutzen, zu Ihren Auftragsverarbeitern. Und/oder implementieren Sie eine staatliche aber von der Politik unabhängige Stelle, an die als einzige und alleinig für solche Fälle personenbezogene Daten der öffentlichen und nicht-öffentlichen Institutionen zwecks Anonymisierung und sodann Nutzung der anonymisierten Daten übermittelt werden; ggfs. unter der verpflichtenden Bedingung, sich dafür in jedem Fall eine judikative Entscheidung einholen zu müssen (ähnlich wie Staatsanwaltschaften bei internationalen Haftbefehlen).

So und/oder so: Stellen Sie die staatliche unpolitische Obhut und Verantwortlichkeit sicher und überlassen sie (die Verarbeitung für) anonymisierte Nutzung von Daten ohne freiwillige Einwilligung der Grundrechtsträger in keinem Fall der Wirtschaft.

Beste Grüße
Susanne Fritz

www.impact-one.de <http://www.impact-one.de>

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Bonn, den 10. Februar 2020

Öffentliches Konsultationsverfahren

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zum Thema:

Anonymisierung unter der DSGVO

unter besonderer Berücksichtigung der TK-Branche

Stellungnahme dazu von Susanne Fritz vom 23.3.2020 im Text markiert

Das Konsultationsverfahren richtet sich insbesondere an Akteure aus Politik, Wirtschaft, Gesellschaft und Verwaltung, die sich diesem Thema befassen.

Kommentare und Stellungnahmen können bis
einschließlich **~~09. März 2020~~** *23.3.2020* an die an E-Mail-Adresse

konsultation@bfdi.bund.de

geschickt werden.

Inhalt

Zusammenfassung

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, 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.
Nicht, wenn man die deutsche Sprache ernst nimmt. So wie der EuGH.

Der EuGH hat in der Rs. Nowak entschieden, dass das Recht auf Löschung einer Prüfungsarbeit beinhaltet, dass die Arbeit "zerstört" wird.

s.a.w.u.

1. Einleitung

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 Absatz 1 Buchstabe c) DSGVO, die personenbezogenen Daten nur in anonymisierter Form zu verarbeiten. Die Anonymisierung kann auch als ein Mittel angesehen werden, im

Immerhin stellt auch mein anonymer Datensatz einen Wert dar, und jeder Wert wird und/oder kann der Bereicherung der Verantwortlichen dienen; jede Bereicherung kann eine etwaig rechtswidrige Bereicherung sein.
Die tatsächlichen Fragen sollten dementsprechend lauten:
1. Wenn 6/1/1 a nicht gilt - warum sollte ich den Wert meines Datensatzes einem verantwortlichen kostenlos schenken müssen? Bereits das wäre ein Schaden nach Art. 82 DSGVO
2. Wie soll ich im Fall der Fälle § 42 Abs. 2 BDSG geltend machen? ...
Ergo: Ob die Verwertung eine Bereichung für die Betroffenen ist, müssen die Betroffenen selbst bestimmen können. 6/1/1 a

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.

Dementgegen: siehe Urteil des EuGH C-673/17 vom 01.10.19, s. Ziff. 2 der Rechtsanerkennung !

'Aus diesen Gründen hat der Gerichtshof für Recht erkannt, dass es für jedes Cookie eine aktive und freiwillige Einwilligung braucht, unabhängig davon, ob es sich bei den im Endgerät des Nutzers einer Website gespeicherten oder abgerufenen Informationen um personenbezogene Daten im Sinne der DSGVO handelt oder nicht.'

Et voilà. Das und auch Art. 21 Abs. 5 (kennt und berücksichtigt kaum jemand) dürfte dem Wunsch der überwiegenden Grundrechtsträger entsprechen. Who cares?

2. Ziel und Gegenstand der Konsultation

Die Rechtslage ist in Bezug auf die Anonymisierung unklar und umstritten. Uneinheitlich beurteilt wird vor allem die Frage, ob die Anonymisierung personenbezogener Daten eine Verarbeitung darstellt, die einer Rechtsgrundlage bedarf. Fraglich ist ferner, auf welche Rechtsgrundlage die Anonymisierung gegebenenfalls gestützt werden kann.

6/1/1 a !

Warum ist das fraglich? Wenn die Anonymisierung keiner Rechtsgrundlage bedürfte, wäre das ein Freibrief für alle - die Risiken wären enorm, da die Kontrolle zwar rechtlich, aber nicht praktisch sicherzustellen wäre

Das Ziel der Konsultation ist es, den geltenden Rechtsrahmen für die Anonymisierung personenbezogener Daten durch Verantwortliche aus Sicht des BfDI aufzuzeigen und eine öffentliche Diskussion darüber anzustoßen. Nach Auswertung der im Rahmen der Konsultation eingehenden Stellungnahmen wird der BfDI ein Positionspapier veröffentlichen. Ziel ist es, allen Verantwortlichen, insb. aus dem Telekommunikationssektor, Orientierung zur Anonymisierung zu geben.

3. Position des BfDI

1) Anforderungen an 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.[1] Wann eine Anonymisierung als hinreichend angesehen werden kann, darüber gibt die DSGVO keine Auskunft. Erwägungsgrund 26 Satz 3 und 4 enthält lediglich folgende

Eine Anonymisierung ist zwangsläufig nur dann hinreichend, wenn die Verarbeitungsanforderungen nach DSGVO erfüllt und sichergestellt sind, denn die Umwandlung von personenbezogengen zu anonymisierten Daten bedarf der Verarbeitung

[1] Vgl. auch § 27 Abs. 3 BDSG.

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 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“.

absolute Sicherheit gibt es nie

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.[2] 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 Arbeitskräften wiederhergestellt werden kann. [3]

Die Überprüfung der Anonymisierung auf ihre Validität ist eine fortwährende Aufgabe des Verantwortlichen[4], die der Kontrolle durch die Datenschutzbehörden unterliegt.

2) 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.[5]

Eine Anonymisierung setzt voraus, dass der Personenbezug der Daten aufgehoben wird. Dafür müssen die Daten durch Entfernen einzelner Elemente verändert werden. Die

---

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

[3] 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.

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

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

Anonymisierung ist damit das Ergebnis der Verarbeitung personenbezogener Daten.[6] Auch das Zusammenfassen von personenbezogenen Daten (Aggregieren) – eine Anonymisierungsmethode – stellt eine Veränderung i.S.d. Art. 4 Nr. 1 DSGVO dar, da die einzelne Information einen anderen Inhalt bekommt.

Wenn schon das Löschen personenbezogener Daten gemäß Art. 4 Nr. 2 DSGVO eine Verarbeitung darstellt, dann muss dies auch für die Anonymisierung gelten.

Die Anonymisierung unterfällt damit dem Begriff der Verarbeitung und bedarf als solche einer Rechtsgrundlage.

3) Mögliche Rechtsgrundlage

i) Datenschutz-Grundverordnung

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:

(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

(2) Art. 6 Abs. 4 DSGVO i.V.m. der ursprünglichen Rechtsgrundlage *Nein!*

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 [7], 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

[6] Vgl. Stellungnahme 5/2014 der Artikel 29-Gruppe zu Anonymisierungstechniken, WP 216, S. 3.

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

Weiterverarbeitung weiterhin die Rechtsgrundlage, die die ursprüngliche Verarbeitung legitimiert hat, vgl. Erwägungsgrund 50 Satz 2 DSGVO.

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.

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 an-

schließende 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.

(3) Art. 6 Abs. 1 Buchst. c) i.V.m. Art. 17 Abs. 1 DSGVO

Soweit die personenbezogenen Daten der Pflicht zur unverzüglichen Löschung gemäß Art. 17 Abs. 1 DSGVO unterfallen, können diese ggf. auch gemäß Art. 6 Abs. 1 Buchst. c) DSGVO anonymisiert werden. Dies ist unter der Prämisse möglich, dass die Anonymisierung dem Löschen gleichgesetzt werden kann.[8] Dafür sprechen folgende Erwägungen:

Anonymisierung = Löschung? Ganz schlechte Prämisse

Zunächst muss hinsichtlich der Fragestellung zwischen der Verpflichtung zur Speicherbegrenzung nach Art. 5 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 (personen-bezogenen) Daten. Dies ergibt sich bereits aus dem Wortlaut, wonach die geforderte

---

[8] 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

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.[9]

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 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. ***Wesentlicher ist: "Bis zu diesem Zeitpunkt"***

Gegen die Gleichsetzung von Löschung und 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 ***Unsinn!***

Nicht? Dann ist das "Recht auf Vergessen werden" nicht erfüllt.

Grade die Zwangsläufigkeit ist Voraussetzung und Erfüllungspfliocht gleichermaßen!

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

*** Aber doch nur, weil man bei digitalen Daten von Löschung und bei Printspeicherung von Vernichtung spricht.

Oder haben Sie schonmal jemanden sagen hören "Kannst du diese Papiere bitte mal löschen"
Oder: "Kannst du mal die eMails bitte vernichten"

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. ***

ii) 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.

(1) § 96 Abs. 3 TKG

Die teilnehmerbezogenen Verkehrsdaten dürften unter den Voraussetzungen des § 96 Abs. 3 S. 1 TKG zum Zwecke der Vermarktung von Telekommunikationsdiensten, zur bedarfsgerechten Gestaltung von Telekommunikationsdiensten oder zur Bereitstellung von Diensten mit Zusatznutzen anonymisiert werden, sofern der Betroffene in diese Verwendung eingewilligt hat.

(2) § 98 Abs. 1 TKG

Standortdaten dürfen nach § 98 Abs. 1 S. 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 S. 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 Ortungsdienste.

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

Nach § 96 Abs. 2 S. 2 Alt. 2 TKG dürfen die Verkehrsdaten nur verwendet werden, soweit dies durch andere gesetzliche Vorschriften begründete Zwecke erforderlich ist. Art. 6 Abs. 1 Buchst. c) DSGVO erlaubt eine Datenverarbeitung, die zur Erfüllung einer rechtlichen

Verpflichtung, der der Verantwortliche unterliegt, erforderlich ist. Insofern verpflichtet § 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 können[10], ist die Anonymisierung von Verkehrsdaten gemäß § 96 Abs. 1 S. 2 Alt. 2 bzw. Art. 6 Abs. 1 Buchst. c) DSGVO möglich.

Falsch. Da ist der Wunsch Vater des Gedankens. Sollte diese eigenwillige Interpretation durch den BfDI (weiter) verbreitet werden, werden in Bälde Unternehmen Daten nach Art. 17 DSGVO nicht mehr löschen/ vernichten, sondern nur noch anonymisieren. Und das wird nicht die einzige negative Folge sein.

4. Ausblick auf die E-Privacy-Verordnung

Der Schaden wäre enorm.

Soweit ersichtlich sehen alle bislang bekannten Entwürfe der E-Privacy-Verordnung – mit redaktionellen Abweichungen – vor, dass die elektronischen Kommunikationsinhalte zu löschen oder zu anonymisieren sind, sobald die vorgesehenen Empfänger die elektronischen Kommunikationsinhalte erhalten haben. Das Gleiche soll für die elektronischen Kommunikationsmetadaten gelten, sobald sie für die Übermittlung einer Kommunikation nicht mehr benötigt werden.[11] Anonymisierung und Löschung werden im Einklang mit den obigen Ausführungen als alternativ eingestuft.

Nicht von mir!

So heisst es in Art. 17 DSGVO auch, dass die Daten gelöscht werden und nicht nur der Personenbezug. Bereits vom Wortlaut her wird die weit überwiegende Anzahl von Grundrechtsträgern unter Löschung eine absolute und unwiederrufbare Vernichtung verstehen, so wie beim Schreddern von Printdokumenten mit anschließendem Verbrennen resp. Entsorgen über das Altpapier.
Das Recht auf Löschung beinhaltet das Recht auf Zerstörung, wie schon der EuGH festgestellt hat.

5. Ergebnis

Die Anonymisierung personenbezogener Daten ist – auch im Telekommunikationssektor – 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.

Fazit:

1. Fragen Sie doch die Grundrechtsträger! Z.B., was sie unter Löschung verstehen.
Einfache Fragen mit einfachen Antwortmöglichekiten mit grosser Wirkkraft über eine online-Umfrage auf der Website des BfDI, konstant über die Medien beworben - das ist alles andere als ein Hexenwerk.
Holen Sie die Grundrechtsträger ab!

2. In der Covid19-Krise sehe ich die Rechtsgrundlage zur Anonymisierung in Art. 6 Abs. 1 S. 1 lit. e) DSGVO.
Die Pandemie wirksam zu bekämpfen, liegt im öffentlichen Interesse.
Komma aber - siehe eMail

---

[10] 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 C., II., 1., c); 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.

[11] Vgl. u.a. Art. 7 Abs. 1 S. 1 und Abs. 2 des Entwurfs der Europäischen Kommission vom 10.01.2017 (COM(2017) 10 final).