

# Stellungnahme: Konsultation des *BfDI* zu Anonymisierung

---

Stand: 09.03.2020

## Management Summary

---

Die Plattform Industrie 4.0 begrüßt die Konsultation des *BfDI* zur Anonymisierung, die für die Industrie 4.0 und die Digitalisierung kaum zu überschätzende Bedeutung hat.

Bei Zustimmung in weiten Teilen sieht die Plattform Industrie 4.0 erheblichen Bedarf nach Differenzierungen, Klarstellungen und Ergänzungen insbesondere in folgenden Aspekten:

- ▶ Ob ein Personenbezug von Daten vorliegt, beurteilt sich subjektiv aus der aktuellen Situation des konkreten Verarbeiters. Dieselben Daten können für verschiedene Verarbeiter personenbezogen, pseudonym oder anonym sein. Daher besteht auch keine objektive Abgrenzung zwischen pseudonymen und anonymen Daten.
- ▶ Eine Anonymisierung ist jedenfalls nicht stets, sondern nur im Einzelfall eine Verarbeitung personenbezogener Daten. Dies hängt auch von der konkreten Umsetzung ab. Eine Anonymisierung erfordert daher nicht stets eine Rechtsgrundlage.
- ▶ Eine im Einzelfall erforderliche Rechtsgrundlage kann bei einer Weiterverarbeitung (Art. 6 Abs. 4 DS-GVO) in der ursprünglichen Rechtsgrundlage bestehen oder bei einer Neuverarbeitung in jeder einschlägigen Rechtsgrundlage (Art. 6 Abs. 1 DS-GVO).
- ▶ Als im Einzelfall erforderliche Rechtsgrundlage kommt auch ein berechtigtes Interesse in Betracht (Art. 6 Abs. 1 lit. f DS-GVO). Die entsprechende Interessenabwägung ermöglicht regelmäßig eine Anonymisierung.
- ▶ Verarbeitungszweck der Anonymisierung personenbezogener Daten ist die Entfernung des Personenbezugs, nicht etwa eine bestimmte Nutzung anonymer Daten.
- ▶ Eine Anonymisierung nach aktueller Technologie führt zu anonymen Daten, die dann weder DS-GVO noch TKG und damit auch keiner Zweckbindung unterliegen. Die zukünftige Herstellung eines Personenbezugs von anonymen Daten bedürfte als neue Verarbeitung personenbezogener Daten einer Rechtsgrundlage.

### AG „Rechtliche Rahmenbedingungen“ der Plattform Industrie 4.0

Die Plattform Industrie 4.0 ist das zentrale deutsche Netzwerk, um die digitale Transformation in der Produktion voranzubringen. Über 350 Akteure aus über 150 Organisationen aus Politik, Wirtschaft, Wissenschaft, Gewerkschaften und Verbänden sind in der Plattform aktiv. Als eines der größten internationalen und nationalen Netzwerke unterstützt die Plattform deutsche Unternehmen bei der Implementierung von Industrie 4.0 in der Praxis mit konkreten Handlungsempfehlungen, Unterstützungsangeboten und Testumgebungen. Internationale Kooperationen unterstreichen die starke Rolle der Plattform über Deutschland hinaus.

In der Arbeitsgruppe „Rechtliche Rahmenbedingungen“ befassen sich rund 50 Expertinnen und Experten mit juristischen Themen für die Industrie 4.0, insbesondere für Datennutzung (mit Datenschutz) und Vertragsgestaltung sowie mit Haftungsfragen und kartellrechtlichen Aspekten. Diese Stellungnahme haben verfasst: RA Martin Schweinoch (SKW Schwarz),

RA Dr. Alexander Duisberg (Bird & Bird), Nils Hullen (IBM Deutschland), Dr. Gerd Kiparski (1&1) und Thomas Schauf (Telekom) sowie RA Dr. Stefan Peintinger (SKW Schwarz).

## Stellungnahme zur Konsultation

---

### Bedeutung der Anonymisierung

Die Nutzung von Daten, auch maschinengenerierter Daten, hat zentrale Bedeutung für die Industrie 4.0 und die gesamte Digitalisierung. Nur die Nutzung von Daten ermöglicht etwa die Entwicklung von Künstlicher Intelligenz oder autonomen Fahrens - um nur zwei Beispiele zu nennen. Die Bedeutung der Anonymisierung für eine zukunftsfähige Wirtschaft kann man kaum überschätzen. Gleichzeitig sind Auswirkungen nicht zwingend gebotener Restriktionen gerade im Vergleich zu Volkswirtschaften ohne solche Hemmnisse keinesfalls zu unterschätzen.

Ein Personenbezug von Daten ist in der Industrie 4.0 häufig ein unerwünschter, aber faktisch nicht vermeidbarer Nebeneffekt. Für die Nutzung der Daten ist dieser Personenbezug oft ebenso unnötig wie hinderlich. Daher ist es ein Kernanliegen der Plattform Industrie 4.0, für möglichst offene Nutzungsmöglichkeiten vorhandener und zukünftiger Daten einzutreten – ohne den Datenschutz von Betroffenen zu vernachlässigen.

Daher beteiligt sich die Arbeitsgruppe „Rechtliche Rahmenbedingungen“ der Plattform Industrie 4.0 neben dem Arbeitsprogramm an der Konsultation zu dem zentralen Thema der Anonymisierung und – damit verbunden – der Nutzungsmöglichkeiten für Daten.

### Zustimmung zu weiten Teilen der Konsultation

Die Plattform Industrie 4.0 begrüßt die Initiative des *BfDI* mit dem Ziel, eine Orientierung für datenschutzrechtliche Fragen der Anonymisierung zu bieten. Auch wegen der Sanktionsdrohungen der DS-GVO kann alleine die derzeit bestehende Verunsicherung zum Innovationshemmnis werden, selbst wenn geplante Umsetzungen im Ergebnis zulässig wären.

Die Plattform Industrie 4.0 stimmt Inhalten der Konsultation in weiten Bereichen zu. Dazu gehören der relative Ansatz für einen Personenbezug von Daten, praktikable Anforderungen für die Anonymisierung, die Alternativität von Löschung und Anonymisierung wie auch die stets mögliche Anonymisierung mit Einwilligung des Betroffenen.

### Inhalt und Aufbau dieser Stellungnahme

Viele Adressaten würden ein Positionspapier des *BfDI* zu datenschutzrechtlichen Aspekten der Anonymisierung voraussichtlich als umfassende Darstellung auffassen. Daher sieht die Plattform Industrie 4.0 Bedarf nach Differenzierungen, Klarstellungen und Ergänzungen. Einige Kernpunkte dafür spricht das Management Summary knapp an.

Im Folgenden werden diese Kernpunkte aufgegriffen und zusammen mit weiteren Aspekten jeweils näher begründet. Die Darstellung beginnt mit übergreifenden Aspekten, es folgen

Fragen materieller Berechtigung zur Anonymisierung und dann formelle Themen sowie TK-spezifische Aspekte.

## A. Übergreifende Aspekte

---

### 1. Personenbezogene, anonyme, pseudonyme Daten

- 1 Wir begrüßen die Klarstellung der Konsultation (S. 5), wann abstrakt eine ausreichende Anonymisierung vorliegt. Für diese zentrale Frage ist eine klare Darstellung wesentlich.
- 2 Ob ein anonymes oder personenbezogenes Datum vorliegt, beurteilt sich anhand der Definition von Art. 4 Nr. 1 DS-GVO unter Beachtung der Breyer-Entscheidung des EuGH.<sup>1</sup> Dabei ist auf den konkreten Verarbeiter in seiner aktuellen subjektiven Situation abzustellen (relativer Personenbezug). Dasselbe Datum kann für einen Verarbeiter personenbezogen, für einen anderen Verarbeiter pseudonym oder für einen weiteren Verarbeiter anonym sein. Die Konsultation (S. 5 ff.) unterscheidet indes nicht zwischen Anonymisierung und Pseudonymisierung von Daten, insbesondere nicht für etwa unterschiedliche Anforderungen an die jeweilige Art und Weise des Vorgehens.
- 3 Wir verweisen in diesem Zusammenhang auf unser Ergebnispapier „*Wie das Recht Schritt hält*“, das beschreibt, dass die Regelungen zur Verarbeitung pseudonymisierter Daten im derzeitigen Recht unterentwickelt sind.<sup>2</sup> Aus den Erwägungsgründen („EG“) 26 und 28 DS-GVO sowie Art. 6 Abs. 4 lit. e DS-GVO wird deutlich, dass der europäische Gesetzgeber die Verarbeitung pseudonymer Daten (insbesondere auch in Big-Data-Lösungen) klar privilegieren und incentivieren möchte. Die Grenze zwischen Anonymisierung und Pseudonymisierung ist für die Nutzer solcher Daten von hoher Relevanz.
- 4 Für die Industrie 4.0 ist diese Abgrenzung von gesteigerter Bedeutung: Häufig fallen in vernetzten Produktionsabläufen personenbeziehbare Daten eher als „Beifang“ an, etwa im Rahmen einer „Mensch-Maschine-Interaktion“. Diese Daten stehen aber – im Gegensatz zu vielen Verbraucher-orientierten Geschäftsmodellen – keineswegs im Zentrum der Betrachtungen. Umso wichtiger ist daher, verlässliche Kriterien für die Anonymisierung – wie auch für die Verarbeitung pseudonymisierter Daten – an die Hand zu bekommen.
- 5 Die Bedeutung der Anonymisierung und die Relevanz des Umgangs mit anonymen Daten können gar nicht überschätzt werden. Die Signalwirkung eines finalen Papiers des *BfDI* ist auf keinen Fall zu unterschätzen. Der *BfDI* sollte dazu weitere Klarstellungen aufnehmen, auch wenn aufgrund der maßgeblichen relativen Beurteilung eines Personenbezugs nach der aktuellen subjektiven Situation des konkreten Verarbeiters keine objektive Abgrenzung zwischen anonymen und pseudonymen Daten möglich ist.

---

<sup>1</sup> EuGH, Urteil vom 19.10.2016, Az. C-582/14 = BeckRS 2016, 82520.

<sup>2</sup> Plattform Industrie 4.0, Ergebnispapier, Oktober 2016, S. 13; abrufbar unter: <https://www.bmwi.de/Redaktion/DE/Publikationen/Industrie/industrie-4-0-wie-das-recht-schritt-haelt.html>.

## 2. Anonymisierung nur im Einzelfall als Verarbeitung

- 6 Der *BfDI* sollte bereits diskutieren, ob eine Anonymisierung stets eine Verarbeitung personenbezogener Daten darstellt.<sup>3</sup> Zwar könnte der weite Begriff der „Verarbeitung“ dafür sprechen, aber systematisch hat die DS-GVO die Anonymisierung nicht geregelt. EG 26 Sätze 5 und 6 DS-GVO zeigen, dass die Grundsätze des Datenschutzes nicht für anonyme Daten gelten. Die Konsultation berücksichtigt EG 26 Satz 6 nicht hinreichend.
- 7 Nicht nur im Bereich Industrie 4.0 gibt es eine Vielzahl praktischer Fälle eines Datenumgangs, die jedenfalls keine „Verarbeitung“ im Sinne von Art. 4 Nr. 2 DS-GVO darstellen. Wenn etwa in einer verteilten Datenhaltung die Daten in einem Silo für sich alleine keinen Personenbezug aufweisen, können diese Daten auch von einem Dritten ohne Verarbeitung nach Art. 4 Nr. 2 DS-GVO anonym genutzt werden. Eine Anonymisierung im Sinne einer Verarbeitung ist dafür nicht erforderlich. Es wäre kontraproduktiv und innovationshemmend, jede Anonymisierung stets als Verarbeitung anzusehen. Vielmehr ist die konkrete technische Gestaltung und Umsetzung im Einzelfall maßgeblich.
- 8 Dabei sind als grundlegende Weichenstellungen entscheidend: Bei der Anonymisierung handelt es sich um eine Ausprägung der datenschutzrechtlichen Grundprinzipien der Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO) und Speicherbegrenzung (Art. 5 Abs. 1 lit. e DS-GVO). Deswegen wäre die Kernfrage, ob die Entfernung des Personenbezugs stets einer Rechtsgrundlage bedarf. Dies ist abzulehnen. Die Umsetzung der genannten Grundprinzipien bedarf keiner weiteren Rechtsgrundlage aus der DS-GVO oder spezialgesetzlicher Regelungen. Der *BfDI* hat bereits selbst explizit ausgeführt, dass eine Anonymisierung von Daten nicht als Verarbeitung anzusehen und somit zulässig sei.<sup>4</sup> Dieser Feststellung lag der Verarbeitungsbegriff im BDSG a.F. auf Basis der Richtlinie 95/46/EG zugrunde. Den Verarbeitungsbegriff der Richtlinie 95/46/EG hat die DS-GVO fast wortgleich übernommen. Woraus sich eine Änderung der Rechtslage ergeben soll, die nun (stets) eine Rechtsgrundlage für die Anonymisierung erfordern würde, ist nicht erkennbar.
- 9 Sinn und Zweck der Datenschutzgesetze ist primär der Schutz des Grundrechts auf informationelle Selbstbestimmung, wozu auch die zweckgebundene Verarbeitung personenbezogener Daten gehört. Werden diese Daten anonymisiert, entfällt das Schutzbedürfnis. Anonymisierung ist somit zum einen ein rechtlich legitimes Mittel zum Schutz des (zuvor) Betroffenen und greift zum anderen den politischen Willen des Gesetzgebers auf.
- 10 Dass eine Anonymisierung auch ohne Rechtsgrundlage möglich sein muss, zeigt auch die Richtlinie (2002/58/EG; „ePrivacy-Richtlinie“). Art. 6 und 9 der ePrivacy-Richtlinie (Verkehrs- und Standortdaten) legen jeweils fest, dass personenbeziehbare Daten zu löschen

---

<sup>3</sup> Differenzierend etwa *Gola*, in: *Gola, Datenschutz-Grundverordnung*, 2. Aufl. 2018, Art. 4 RdNr. 41; wohl ohne konkrete Festlegung etwa *Ziebarth*, in: *Sydow, Europäische Datenschutzgrundverordnung*, 2. Aufl. 2018, Art. 4 RdNr. 28; *Spyra*, in *Münchener Anwaltshandbuch Medizinrecht*, Clausen/Schroeder-Printzen, 3. Aufl. 2020, § 23, RdNr. 20 ff; bejahend etwa: *Hansen*, in: *Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht*, 1. Aufl. 2019, Art. 4 Nr. 5 DS-GVO RdNr. 23.

<sup>4</sup> Vgl. *BfDI*, 26. Tätigkeitsbericht 2015-2016, Ziffer 17.2.4.4 „Big Data im TK-Bereich“, S. 170.

oder zu anonymisieren sind, sobald sie nicht mehr benötigt werden. Eine Rechtsgrundlage dafür wird aber neben den engen Verarbeitungstatbeständen gerade nicht aufgeführt.

- 11 Aus Art. 6 Abs. 1 lit. e der Richtlinie 95/46/EG<sup>5</sup> und der ePrivacy-Richtlinie hat die Art. 29-Gruppe in WP 216 geschlossen, dass personenbezogene Daten zumindest „standardmäßig“ anonymisiert werden sollten.<sup>6</sup>
- 12 Würde für den Anonymisierungsvorgang<sup>7</sup> selbst jeweils stets eine Rechtsgrundlage wie etwa die Weiterverarbeitung zu kompatiblen Zwecken oder das Vorliegen eines berechtigten Interesses gefordert, wäre dies eine rein formalistische Betrachtung. Die Umsetzung der Datenschutzgrundprinzipien ist stets vereinbar mit dem ursprünglichen Zweck und eine Vereinbarkeitsprüfung inhaltlich obsolet. Entsprechendes gilt bei der Prüfung eines berechtigten Interesses. Dennoch müsste formalistisch etwa den Dokumentationsanforderungen gemäß Art. 5 Abs. 2 DS-GVO Rechnung getragen werden.
- 13 Der *BfDI* sollte auch anhand der praktischen Vielgestaltigkeit und der aufgezeigten systematischen Aspekte nochmals prüfen, ob und, wenn ja, in welchen Einzelfällen eine Rechtsgrundlage für die jeweilige Anonymisierung erforderlich sein kann.

### 3. Weiterverarbeitung und Neuverarbeitung

- 14 Als mögliche Rechtsgrundlagen für eine Anonymisierung stellt die Konsultation (S. 6 – 8) nur dar, wann eine Anonymisierung (verstanden als Vorgang) als Weiterverarbeitung nach Art. 6 Abs. 4 DS-GVO möglich wäre. Die weitere Möglichkeit einer Anonymisierung als neue Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO bleibt völlig unerwähnt.<sup>8</sup>
- 15 Die Rechtsnatur von Art. 6 Abs. 4 DS-GVO ist in mehrfacher Hinsicht unklar.<sup>9</sup> Jedenfalls entfaltet Art. 6 Abs. 4 DS-GVO aber keine Sperrwirkung für andere Rechtfertigungsgründe.<sup>10</sup> Aus EG 50 Abs. 1 S. 2, Abs. 2 S. 9 und S. 10 DS-GVO ergibt sich, dass eine Verarbeitung zu „inkompatiblen“ Zwecken zulässig ist, wenn dafür eine „andere gesonderte Rechtsgrundlage“ greift, zum Beispiel Art. 6 Abs. 1 lit. f DS-GVO.<sup>11</sup>
- 16 Der *BfDI* sollte die Gleichwertigkeit und einander nicht ausschließende Alternativität verschiedener Rechtsgrundlagen herausstellen, wenn für einen Anonymisierungsvorgang im Einzelfall eine Rechtsgrundlage erforderlich sein sollte. Der *BfDI* sollte nicht den Eindruck zulassen, mögliche Rechtsgrundlagen wären ausgeschlossen oder nicht relevant.

---

<sup>5</sup> Entspricht Art. 5 Abs. 1 lit. e DS-GVO.

<sup>6</sup> Artikel-29-Datenschutzgruppe, Stellungnahme 5/2014 zu Anonymisierungstechniken vom 10.04.2014, WP216, S. 8; abrufbar unter [https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216\\_de.pdf](https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf) („WP216“).

<sup>7</sup> Diese Stellungnahme geht nur von Anonymisierungsvorgängen aus, die zu echter Anonymisierung führen.

<sup>8</sup> Siehe EG 50 Abs. 2 S. 9 und S. 10 DS-GVO; *Heberlein*, in: Ehmann/Selmayr, DS-GVO, 2. Aufl. 2018, Art. 6 RdNr. 55.

<sup>9</sup> *Albers/Veit*, in: BeckOK Datenschutzrecht, Wolff/Brink, 30. Edition, Stand: 01.11.2019, Art. 6 DS-GVO, RdNr. 71ff; *Schulz*, in: Gola, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 6 RdNr. 202ff; *Assion/Nolte/Veil*, in: Gierschmann/Schlender/Stentzel/Veil, DS-GVO, 2017, Art. 6 RdNr. 200.

<sup>10</sup> *Assion/Nolte/Veil*, in: Gierschmann/Schlender/Stentzel/Veil, DS-GVO, 2017, Art. 6 RdNr. 201 ff.

<sup>11</sup> Vgl. *Schulz*, in: Gola, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 6 RdNr. 212; *Roßnagel/Nebel/Richter*, Was bleibt vom Europäischen Datenschutzrecht? - Überlegungen zum Ratsentwurf der DS-GVO, ZD 2015, 455, 457.

## B. Materielle Aspekte

---

Nur soweit ein Anonymisierungsvorgang im Einzelfall eine Verarbeitung im datenschutzrechtlichen Sinne darstellt, käme es auf eine Rechtsgrundlage und weitere Anforderungen der DS-GVO an. Vor diesem Hintergrund werden auch DS-GVO-Anforderungen im Kontext eines Anonymisierungsvorgangs angesprochen.

### 1. Kein uneingeschränkter Datenschutz

- 17 Art. 8 Charta der Grundrechte der Europäischen Union („Charta“) schützt personenbezogene Daten. Art. 16 Charta schützt gleichzeitig die unternehmerische Freiheit. Diesem Spannungsverhältnis trägt EG 4 S. 4 DS-GVO auch Rechnung.
- 18 Um einen praktischen Ausgleich zwischen diesen Grundrechtspositionen zu erreichen, sollte der *BfDI* dieses Spannungsverhältnis berücksichtigen. Unternehmen benötigen anonyme Daten zum Schutz von (ex-)betroffenen Personen und aus wirtschaftlichen Gründen. Eine betroffene Person kann in ihrem Grundrecht aus Art. 8 Charta nicht besser geschützt werden, als gar nicht mehr betroffen zu sein.
- 19 Der *BfDI* sollte daher in diesem Spannungsfeld für einen Anonymisierungsvorgang keine Hürden formulieren, die der Grundrechtsschutz von Betroffenen nicht zwingend erfordert.

### 2. Anonymisierung stets „kompatibel“ (6 IV DS-GVO)

- 20 Die Konsultation vergleicht im Beispiel für Art. 6 Abs. 4 DS-GVO unzutreffend den ursprünglichen Verarbeitungszweck personenbezogener Daten (Begründung und Ausgestaltung des Vertragsverhältnisses) mit dem Zweck künftigen Umgangs mit anonymisierten Daten.
- 21 Wenn für die konkrete Anonymisierung eine Verarbeitung zugrunde gelegt wird, wäre die Weiterverarbeitung nach Art. 6 Abs. 4 DS-GVO (nur) die Anonymisierung der Daten selbst. Der Zweck der Anonymisierung als (Weiter-)Verarbeitung ist die Entfernung des Personenbezugs. Ein mit dem späteren Umgang mit den anonymen Daten verfolgter Zweck ist für die (ex ante) datenschutzrechtliche Beurteilung zwingend irrelevant, da auf diesen späteren Umgang die DS-GVO unanwendbar ist. Dies entspricht auch dem Schutzgedanken der DS-GVO, der auf anonyme Daten gerade nicht anwendbar ist.
- 22 Würde bei der Anonymisierung von Daten (auch) der Zweck eines späteren Umgangs mit den anonymen Daten geprüft, würde damit die Geltung der DS-GVO entgegen ihres klaren Wortlauts auch auf anonyme Daten erstreckt. Dann würde sich zudem die Frage stellen, ob der Umgang mit anonymen Daten auf den im Rahmen der Anonymisierung geprüften Zweck begrenzt sein soll. Das würde die durch Art. 16 Charta geschützten Rechte ohne erforderliche Legitimation beeinträchtigen und verbietet sich auch deswegen klar.
- 23 Die Konsultation (S. 7/8) stellt einen beispielhaften Kompatibilitätstest dar. Dessen Ergebnis ist zu verallgemeinern: Einer betroffenen Person kann bei einer Anonymisierung nichts passieren; sie kann nicht besser geschützt werden, als gar nicht mehr betroffen zu sein.

- 24 Der *BfDI* sollte daher klarstellen, dass eine Anonymisierung – selbst wenn sie als datenschutzrechtliche Verarbeitung angesehen werden würde – regelmäßig nach Art. 6 Abs. 4 DS-GVO zulässig sein muss, insbesondere unter Berücksichtigung von Abs. 4 lit. d DS-GVO (Folgen) und erst recht Abs. 4 lit. e DS-GVO (Garantien).

### 3. „Berechtigte Interessen“ fehlen (6 I lit. f DS-GVO)

- 25 Die Konsultation entbehrt jeglicher Darstellung, dass und wann eine Anonymisierung als Verarbeitung nach Art. 6 Abs. 1 lit. f DS-GVO zulässig ist. Zumindest für am Wettbewerb teilnehmende öffentlich-rechtliche Unternehmen und für TK-Unternehmen ist Art. 6 Abs. 1 lit. f) DS-GVO durchaus relevant.
- 26 Art. 6 Abs. 1 lit. f DS-GVO kann als Rechtsgrundlage für eine Weiterverarbeitung ebenso wie für eine neue Verarbeitung herangezogen werden<sup>12</sup>. Eine Abwägung gemäß Art. 6 Abs. 1 lit. f DS-GVO führt regelmäßig zu einem zulässigen Anonymisierungsvorgang. Es ist gleichzeitig zu betonen, dass nicht jede Anonymisierung auch eine Verarbeitung ist.
- 27 Der *BfDI* sollte die Anwendbarkeit von Art. 6 Abs. 1 lit. f DS-GVO klar zum Ausdruck bringen, auch wegen der Signalwirkung eines geplanten Positionspapiers.

### 4. Keine weitere Zweckbindung

- 28 Die Konsultation suggeriert eine fortgesetzte oder absolute Zweckbindung anonymisierter Daten. Indes kann es unter keinem Gesichtspunkt eine direkte oder indirekte „Fortsetzung“ einer Zweckbindung für anonyme Daten geben. Für anonyme Daten gilt die DS-GVO nicht.<sup>13</sup> Daher ist auch Art. 5 DS-GVO auf solche Daten unanwendbar. Anonymisierte Daten sind anonym und stehen originär nicht-personenbezogenen Daten in jeder Hinsicht gleich.
- 29 Datenschutzrechtlich kommt es bei der Anonymisierung nicht auf einen später mit anonymen Daten verfolgten Zweck an, für den die DS-GVO unanwendbar ist. Gleiches gilt bei einer Anonymisierung als Löschung. Auch in diesem Fall ist der Verarbeitungszweck die Beseitigung des Personenbezugs. Rechtmäßige personenbezogene Daten können jederzeit auch vor einer gesetzlichen Löscho- oder Anonymisierungspflicht auch für eine weitere, anonyme Verarbeitung anonymisiert werden.
- 30 Der *BfDI* sollte daher klar zum Ausdruck bringen, dass mit einer Anonymisierung eine vorherige Zweckbindung endgültig beendet ist, welche für ursprünglich personenbezogene Daten gegolten hat und für diese personenbezogenen Daten weiterhin gilt.

### 5. (Re-)Identifizierung als neue Verarbeitung

- 31 Die Konsultation führt aus (S. 9, letzter Absatz), bei einer Anonymisierung verbleibe ein Restrisiko der Re-Identifizierung. Wenn nach aktuellem Stand verfügbarer Technologien eine Anonymisierung erfolgt, ist auch eine Re-Identifizierung anhand dieses Stands der Technik zu beurteilen. So anonymisierte Daten sind mit *Status Quo* anonym.

---

<sup>12</sup> Siehe oben Teil A Ziffer 3

<sup>13</sup> Vgl. EG. 26 Sätze 5 und 6 DS-GVO.



- 32 Eine zukünftige Re-Identifizierung wäre stets eine eigenständige neue Verarbeitung, die gemäß DS-GVO eine neue Rechtsgrundlage erfordert. Die abstrakt stets gegebene Möglichkeit einer künftigen Re-Identifizierung kann daher einer Anonymisierung nicht entgegenstehen. Will ein Verantwortlicher eine Re-Identifizierung durchführen, sind datenschutzrechtliche Anforderungen natürlich wieder zu beachten. Eine Re-Identifizierung kann schon denkllogisch nicht für alle Zukunft unwiderruflich unmöglich gemacht werden.<sup>14</sup>
- 33 Eine Anonymisierung nach „state of the art“ (Konsultation S. 5 oben) verpflichtet daher auch nicht zur ständigen Überwachung etwaiger (Rest-)Risiken.<sup>15</sup> So gibt es etwa im Bereich des maschinellen Lernens erste praktikable Ansätze für kryptografische Verfahren für kollaboratives Lernen, wie die „sichere Mehrparteienberechnung“ (engl. „secure multi-party computation“).<sup>16</sup> Die Logik auf S. 5 der Konsultation ist daher zwingend unzutreffend.
- 34 Der *BfDI* sollte klarstellen, dass (a) keine „Datenbeobachtungspflicht“ für anonyme Daten besteht und dass (b) eine Anonymisierung und die Möglichkeit einer Re-Identifizierung zum Zeitpunkt der Anonymisierung mit demselben Stand der Technik zu beurteilen sind.

## 6. Technische Aspekte einer Anonymisierung

- 35 Die Konsultation nimmt keine Stellung zur praxisrelevanten technischen Seite der Anonymisierung. Wir regen an, im weiteren Verfahren die Ergebnisse der entsprechenden *BMW*-Studie zu berücksichtigen.<sup>17</sup> Weitere Ausführungen dazu enthält auch der Technical Report des *BMW*-Technologieprogramms Smart Data – Innovationen aus Daten: „Smart Data – Smart Privacy?“.<sup>18</sup>
- 36 Der *BfDI* sollte keine Empfehlung für eine technische Ausführung abgeben. Indes sollte auf neuere Untersuchungen verwiesen werden, insbesondere da das WP 216 aus dem Jahr 2014 naturgemäß nicht mehr auf dem aktuellsten Stand der Technik sein kann.

## C. Formelle Aspekte

### Vorab-Information bei Weiter- und Neuverarbeitung

- 37 Wenn eine Anonymisierung im Einzelfall eine Weiter- oder Neuverarbeitung darstellt, gelten dafür auch Art. 13, 14 DS-GVO. Im Fall von Art. 14 DS-GVO wäre auch Art. 14 Abs. 5 lit. b DS-GVO anzuwenden. Nach einer Anonymisierung ist es entweder unmöglich oder nur mit unverhältnismäßigem Aufwand möglich, ex-betroffene Personen zu informieren. Ein solcher Datenschutzhinweis unterbleibt daher in der Regel. Daneben ist es jedenfalls

---

<sup>14</sup> Möglicherweise anders interpretierbar WP 216, S. 3.

<sup>15</sup> Möglicherweise anders interpretierbar WP 216, S. 29f.

<sup>16</sup> Vgl. *Winter/ Battis/ Halvani*, Herausforderungen für die Anonymisierung von Daten, ZD 2019, 489, 492.

<sup>17</sup> Vgl. Ergebnisbroschüre der Smart Data Group von 11/2017, herausgegeben vom *BMW*, S. 33; abrufbar unter: <https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/smart-data-innovationen-aus-daten.html>.

<sup>18</sup> Vgl. Technical Report des *BMW*-Technologieprogramms „Smart Data – Innovationen aus Daten“, Smart Data – Smart Privacy?, 11/2015, S. 7ff.; abrufbar unter: [https://www.hiig.de/wp-content/uploads/2015/12/SmartData\\_Thesenpapier\\_smart\\_Privacy.pdf](https://www.hiig.de/wp-content/uploads/2015/12/SmartData_Thesenpapier_smart_Privacy.pdf).

nach Art. 13, 14 DS-GVO zulässig, Informationspflichten für eine Anonymisierung als Verarbeitung auch vorweg einzulösen. Dies folgt aus dem Wortlaut der DS-GVO.<sup>19</sup>

- 38 Nur wenn eine Anonymisierung im Einzelfall eine Verarbeitung (Art. 4 Nr. 2 DS-GVO) darstellt, wäre diese Verarbeitungstätigkeit nach Art. 30 DS-GVO zu dokumentieren. Dafür wäre eine praktische Handreichung des *BfDI* (etwa als Muster) hilfreich.
- 39 Der *BfDI* sollte diese formalen Aspekte eines Anonymisierungsvorgangs darstellen als Beitrag zur Rechtssicherheit bei den verschiedenen Stakeholdern.

## D. TK-spezifische Aspekte

### 1. Anonymisierung bei §§ 96 III und 98 I TKG

- 40 Die Konsultation nimmt Bezug zu datenschutzrechtlichen Spezialvorschriften. § 96 Abs. 3 TKG ermöglicht eine Verarbeitung teilnehmerbezogener Verkehrsdaten für Zwecke der Vermarktung, zur bedarfsgerechten Gestaltung von TK-Diensten oder zur Bereitstellung von Diensten mit Zusatznutzen. Anders als in der Konsultation dargestellt, dürfen in diesem Fall personenbezogene Daten verarbeitet werden, sofern eine Einwilligung des Betroffenen vorliegt. Eine Anonymisierung ist hier 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 bezweifelt werden.
- 41 Bei § 98 TKG ist zu beachten, dass es sich dabei um andere Standortdaten als Verkehrsdaten handelt.<sup>20</sup> Diese dürfen nicht gleichgesetzt werden. Zudem würde eine zu enge Wortlautauslegung, wonach anonymisierte Daten für einen „Dienst mit Zusatznutzen“ zu verwenden wären, die Nutzung anonymisierter – also anonymer – Daten enorm einschränken.
- 42 Der *BfDI* sollte diese Punkte im weiteren Verfahren nochmals prüfen.

### 2. Anonymisierung von TK-Verkehrsdaten (6 DSGVO)

- 43 Die Konsultation führt aus, nach § 96 Abs. 2 S. 2 Alt. 2 TKG dürften Verkehrsdaten nur verwendet werden, soweit dies für durch andere gesetzliche Vorschriften begründete Zwecke erforderlich sei. Hierzu gehöre auch eine Löschung gemäß § 96 Abs. 1 S. 2 Alt. 2 TKG oder Art. 6 Abs. 1 lit. c DS-GVO.
- 44 Wir begrüßen grundsätzlich, dass auch eine Löschung durch Anonymisierung als möglich erachtet wird. Dies entspricht der zugrundeliegenden ePrivacy-Richtlinie, die in Art. 6 DS-GVO eine Löschung oder Anonymisierung alternativ ermöglicht. Insofern besteht in § 96

<sup>19</sup> Vgl. Art. 13 Abs. 3 i.V.m. Abs. 4 DS-GVO und Art. 14 Abs. 4, Abs. 5 lit. a DS-GVO sowie die Logik von Art. 13 Abs. 2 lit. b DS-GVO und Art. 14 Abs. 2 lit. c DS-GVO jeweils i.V.m. Art. 21 Abs. 4 DS-GVO.

<sup>20</sup> Vgl. Art. 9 ePrivacy-Richtlinie.

Abs. 1 TKG, der lediglich die Löschung nennt, ein Umsetzungsdefizit der ePrivacy-Richtlinie im nationalen Recht. Die erforderliche richtlinienkonforme Auslegung von § 96 Abs. 1 TKG ergibt, dass eine Löschung durch Anonymisierung möglich ist. Da es sich bei Löschung wie Anonymisierung um die Umsetzung der Datenschutzgrundprinzipien handelt, bedeutet das allerdings nicht gleichzeitig, dass es sich auch um eine Verarbeitung handelt.<sup>21</sup>

- 45 Wenn die Anonymisierung im Einzelfall eine Verarbeitung darstellen würde, stünden als Rechtsgrundlagen dafür nicht nur § 96 Abs. 1 S. 2 Alt. 2 TKG, Art. 6 Abs. 1 lit. c DS-GVO in Verbindung mit § 96 Abs. 1 S. 3 TKG zur Verfügung. Eine Anonymisierung der Verkehrsdaten ist auch auf Basis eines berechtigten Interesses gemäß § 96 Abs. 1 S. 3 TKG in Verbindung mit Art. 6 Abs. 1 lit. f DS-GVO oder als Weiterverarbeitung im Sinne von Art. 6 Abs. 4 DS-GVO möglich.<sup>22</sup>
- 46 Die Artikel 29-Gruppe hat schon im WP 216 festgestellt, dass eine Anonymisierung in Art. 6 Abs. 1 der ePrivacy-Richtlinie ausdrücklich zulässig ist.<sup>23</sup> In diesem Fall ist laut WP 216 „eine entsprechende Rechtsgrundlage nach Artikel 7 der Datenschutzrichtlinie gegeben.“ Daher konnte im dort beschriebenen Fall auf Art. 7 lit. f Richtlinie 95/46/EG für eine Anonymisierung aufgrund berechtigten Interesses zurückgegriffen werden. Dieser Gedanke ist ohne weiteres auf das Verhältnis der ePrivacy-Richtlinie zur DS-GVO zu übertragen. Zusätzliche Beschränkungen im TKG für einen Rückgriff auf allgemeine Rechtsgrundlagen des Art. 6 DS-GVO, die keine Grundlage in der ePrivacy-Richtlinie finden, können keine Berücksichtigung finden.<sup>24</sup>
- 47 Der *BfDI* sollte diese Systematik zur Klarstellung ausdrücklich darstellen.

## Fazit

---

Die Plattform Industrie 4.0 begrüßt durch die Arbeitsgruppe „Rechtliche Rahmenbedingungen“ die Konsultation des *BfDI* zu der für die Industrie 4.0 und die gesamte Digitalisierung zentralen Frage der Anonymisierung ausdrücklich und stimmt deren Inhalten in weiten Bereichen zu. Gleichzeitig besteht für das Positionspapier des *BfDI* erheblicher Bedarf nach Differenzierungen, Klarstellung und Ergänzungen für wesentliche Aspekte, die oben näher dargestellt und begründet sind.

Die Arbeitsgruppe „Rechtliche Rahmenbedingungen“ der Plattform Industrie 4.0 würde vor diesem Hintergrund eine Beteiligung im weiteren Verfahren sehr befürworten und steht für einen konstruktiven Dialog bereit.

---

<sup>21</sup> Siehe oben Teil A Ziffer 2.

<sup>22</sup> Siehe dazu jeweils näher oben Teil B Ziffern 2 und 3

<sup>23</sup> WP216, S. 9.

<sup>24</sup> Siehe EuGH, Urteil vom 19.10.2016, Az. C-582/14, RdNr. 57 f. = BeckRS 2016, 82520.