Stellungnahme

des Gesamtverbandes der Deutschen Versicherungswirtschaft

zum

Öffentlichen Konsultationsverfahren des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zum Thema:

Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche

Gesamtverband der Deutschen Versicherungswirtschaft e. V.

Wilhelmstraße 43 / 43 G, 10117 Berlin
Postfach 08 02 64, 10002 Berlin
Tel.: +49 30 2020-5000
Fax: +49 30 2020-6000

51, rue Montoyer
B - 1000 Brüssel
Tel.: +32 2 28247-30
Fax: +49 30 2020-6140
ID-Nummer 6437280268-55

Ansprechpartner:
Datenschutz/Grundsatzfragen

E-Mail: **data-protection@gdv.de**

www.gdv.de

Zusammenfassung

Die Anonymisierung personenbezogener Daten kann ein wirksames Mittel sein, um Betroffene zu schützen und gleichzeitig den wirtschaftlichen Wert von Daten auszuschöpfen. Dieses Ziel verfolgen auch die Digitalstrategie der EU-Kommission und die Datenstrategie der Bundesregierung.

Die Konsultation des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit bietet die Möglichkeit, dies zu verwirklichen. Um einen praktikablen Umgang mit der Anonymisierung sicherzustellen und die bestehende Rechtsunsicherheit zu beseitigen, adressiert die deutsche Versicherungswirtschaft in dieser Stellungnahme u. a. folgende Punkte:

- Differenziertere Betrachtung der Anforderungen an das Vorliegen einer Anonymisierung erforderlich
- Anonymisierung ist keine rechtfertigungsbedürftige Verarbeitung personenbezogener Daten
- Falls dennoch weiterhin eine Rechtsgrundlage verlangt wird:
  - verlässliche Rechtsgrundlage für die Anonymisierung besonderer Kategorien personenbezogener Daten erforderlich
  - Berechtigtes Interesse ist geeignete Rechtsgrundlage für die Anonymisierung
  - Anonymisierung selbst ist entscheidender Zweck bei zweckändernder Verarbeitung
  - Anonymisierung nach Art. 6 Abs. 1 lit. c i. V. m. Art. 32 Abs. 1 DSGVO zulässig

1. Einleitung

Die Anonymisierung von personenbezogenen Daten ist als Instrument zur Wahrung des Datenschutzes von höchster praktischer Relevanz im Unternehmensalltag. Sie fungiert zum einen als Alternative zur Löschung von Daten. Technische Restriktionen, insbesondere im Zusammenhang mit relationalen Datenbanken, führen dazu, dass die physische Löschung von Datenfeldern oftmals nur mit Unwägbarkeiten realisierbar ist. Zum anderen können durch Anonymisierung unternehmenswichtige Informationen auf aggregierter Basis für übergreifende, nicht abschließende Zwecke weiterverwendet werden. Ein Risiko für die Rechte und Freiheiten der Betroffenen ist dabei ausgeschlossen.

Wie der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) erwähnt, ist die Rechtslage in Bezug auf die Anonymisierung sehr unklar. Dadurch wird verhindert, dass ihre Potenziale effektiv genutzt werden können. Die EU-Kommission hat erst vor kurzem ihre Strategie für die Gestaltung der digitalen Zukunft Europas veröffentlicht, mit der sie künstliche Intelligenz und Datennutzung fördern möchte. Die Bundesregierung verfolgt einen ähnlichen Ansatz. Es ist allgemein anerkannt, dass anonymisierte Daten einen signifikanten Beitrag hierzu leisten können. Ohne rechtssichere und praktische Vorgaben zur Anonymisierung kann das Ziel, die EU zum Vorreiter für die effektive Nutzung von Daten und KI zu machen, jedoch nicht verwirklicht werden.

Vor diesem Hintergrund ist die Absicht des BfDI, für Klarheit zu sorgen, sehr begrüßenswert. Die deutsche Versicherungswirtschaft hat zur vorliegenden Konsultation folgende Anmerkungen:

2. Anforderungen an die Anonymisierung

Es wird angeregt, die Ausführungen zu den Anforderungen an die Anonymisierung zu ergänzen und die rudimentären Aussagen der DSGVO zu spezifizieren. Der BfDI geht zutreffend davon aus, dass eine absolute Anonymisierung weder möglich, noch gefordert ist, und verweist auf ErwGr. 26 der DSGVO. Für die Frage der Identifizierbarkeit kommt es auf Mittel an, die nach „allgemeinem Ermessen wahrscheinlich“ genutzt werden, um die natürliche Person zu identifizieren. Es sollte ausdrücklich darauf hingewiesen werden, dass die Nutzung rechtswidriger Mittel zur Identifizierung nicht nach „allgemeinem Ermessen wahrscheinlich“ ist. Gleichfalls kann die Nutzung eines Mittels zur Re-Identifizierung nicht nach allgemeinem Ermessen wahrscheinlich sein, wenn umfassende technische, organisatorische und rechtliche Maßnahmen getroffen wurden, um die Nutzung zu verhindern.

Ferner soll „bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, alle objektiven Faktoren […] herangezogen werden […].“ In das Papier des BfDI sollte aufgenommen werden, dass es nur um „alle objektiven Faktoren“ geht, die in der konkreten Konstellation relevant sind. Ob Daten als anonymisiert betrachtet werden können, muss immer Gegenstand einer Einzelfallbewertung sein. Werden Daten in einem Unternehmen anonymisiert, sodass für das Unternehmen eine Re-Identifizierung nicht mit verhältnismäßigem Aufwand durchführbar ist, und werden die anonymisierten Daten nur unternehmensintern ohne Zugriffsmöglichkeit durch Dritte verwendet, so kann es nicht darauf ankommen, ob eine außenstehende Person irgendwo auf der Welt über Mittel verfügt, um den Personenbezug mit verhältnismäßigem Aufwand wiederherzustellen. Daher richten sich die zu berücksichtigenden „objektiven Faktoren“ nach der subjektiven Komponente des Nutzerkreises der Daten.

3. Anonymisierung ist keine rechtfertigungsbedürftige Verarbeitung

Aus der Gesetzessystematik ist erkennbar, dass die Anonymisierung keine nach Art. 6 DSGVO rechtfertigungsbedürftige Verarbeitung personenbezogener Daten sein kann.

Die Anonymisierung stellt eine absolute Steigerung der Pseudonymisierung dar. Schon die Pseudonymisierung wird u. a. in Artt. 6 Abs. 4 lit. e, 25 Abs. 1, 32 Abs. 1 lit. a DSGVO als technisch organisatorische Maßnahme/geeignete Garantie zur Erreichung eines höheren Datenschutzniveaus bezeichnet. Ihr Vorhandensein ist somit Abwägungskriterium für die Zulässigkeit einer nach Art. 6 DSGVO zu rechtfertigenden (weiteren) Verarbeitung. Die Annahme liegt nahe, dass sie ihrerseits als privilegierte Verarbeitung keines Erlaubnistatbestands nach Art. 6 DSGVO bedarf, da sie anders als die in Art. 4 Nr. 2 DSGVO aufgezählten Verarbeitungen kein Risiko für den Betroffenen begründet.
Betrachtet man die Pseudonymisierung hingegen als rechtfertigungsbedürftigen Verarbeitungsvorgang, so könne sie regelmäßig als zweckändernde Verarbeitung nach Art. 6 Abs. 4 DSGVO eingestuft werden. Da sie aber dann sowohl Zweck der Verarbeitung als auch deren Voraussetzung nach Art. 6 Abs. 4 lit. e DSGVO ist, müsste sie sich im Ergebnis selbst rechtfertigen. Eine derartige Konstruktion kann nicht vom Gesetzgeber beabsichtigt sein.
Wenn schon die Pseudonymisierung aus den vorbenannten Gründen keine rechtfertigungsbedürftige Verarbeitung sein kann, muss dies erst recht für die Anonymisierung als deren absolute Steigerung gelten.

Im Papier des BfDI wird argumentiert, dass eine Anonymisierung einer Rechtsgrundlage bedarf, weil selbst das Löschen personenbezogener Daten gem. Art. 4 Nr. 2 DSGVO eine rechtfertigungsbedürftige Verarbeitung darstellt. An dieser Schlussfolgerung kann nicht festgehalten werden, da Löschen und Anonymisieren bei näherer Betrachtung nicht gleichgesetzt werden können. Zutreffend ist, dass das Ergebnis beider Vorgänge nicht mehr vom Anwendungsbereich der DSGVO erfasst ist. Im Übrigen müssen die Umstände beider Verfahren differenzierter behandelt werden. Der Grund für das Erfordernis einer Rechtsgrundlage für die Löschung liegt in dem Risiko, dass der Betroffene dadurch den Zugriff auf ihn betreffende Daten endgültig verliert. Diese Gefahr ist einer Anonymisierung dagegen nicht zwingend immanent. Sie soll nur zukünftige Verarbeitungen von Daten ohne Personenbezug ermöglichen, nicht aber zwangsläufig eine Weiterverarbeitung der ursprünglichen Daten mit ihrem Personenbezug verhindern. Ein Beispiel wäre das Training von Künstlicher Intelligenz mit Kundendaten. Die Kundendaten können in anonymisierter Form als Trainingsdaten genutzt werden. Dies schließt jedoch nicht die Möglichkeit aus, die Kundendaten nicht dennoch mit Personenbezug für andere Verarbeitungsvorgänge zu nutzen.
Auch der Erst-Recht-Schluss im Papier des BfDI ist dementsprechend nicht geeignet, um die Rechtfertigungsbedürftigkeit von Anonymisierungen zu begründen.

Schließlich kann die Anonymisierung auch deshalb keines Erlaubnistatbestandes bedürfen, weil ansonsten ein nicht nachvollziehbarer Wertungswiderspruch beim Umgang mit besonderen Kategorien personenbezogener Daten bestünde. Die Erlaubnistatbestände in Art. 9 Abs. 2 DSGVO sind weitaus enger formuliert als in Art. 6 Abs. 1 DSGVO. Verständlicherweise werden an die Verarbeitung sensibler Daten höhere Anforderungen gestellt als an einfache Daten. Deshalb sollten gerade besondere Kategorien personenbezogener Daten vor einer Weiterverarbeitung - wann immer möglich – anonymisiert oder pseudonymisiert werden, um den Betroffenen zu schützen. Es erscheint dann kaum vertretbar, dass für die Anonymisierung besonders schützenswerter Daten höhere Voraussetzungen gelten als für einfache Daten.

4. Rechtsgrundlagen der Anonymisierung

a) Fehlende Ausführungen zur Anonymisierung besonderer Kategorien personenbezogener Daten

Sofern man trotz der umfangreichen, dagegen sprechenden Argumente von der Prämisse ausgeht, dass die Anonymisierung einer Rechtsgrundlage bedarf, ist darauf hinzuweisen, dass im Papier des BfDI Ausführungen zum Umgang mit besonderen Kategorien personenbezogener Daten

aus Art. 9 DSGVO gänzlich fehlen. Da aber vor allem die Anonymisierung von Gesundheitsdaten etwa zu Forschungszwecken von überragender Bedeutung ist, sollten entsprechende Ausführungen ergänzt werden.

Im Einzelnen sind folgende Anpassungen geboten:

b) Einwilligung

Neben Art. 6 Abs. 1 lit. a DSGVO sollte Art. 9 Abs. 2 lit. a DSGVO genannt werden, um die besonderen Kategorien personenbezogener Daten zu erfassen. Anzumerken ist, dass die Einwilligung nur von äußerst geringer praktischer Relevanz ist. Eine Bereitschaft der Betroffenen zur Abgabe einer Einwilligung in eine Anonymisierung ihrer Daten wird realistisch kaum jemals zu erwarten sein. Dies gilt umso mehr, da bei allen bestehenden Datenverarbeitungen die Einwilligung zur Anonymisierung nicht von Anfang an eingeholt wurde, sondern erst nachträglich angefragt werden müsste.

Des Weiteren besteht ein Konflikt im Hinblick auf die Pflicht in Art. 7 Abs. 3 DSGVO, dem Betroffenen bei Einholung der Einwilligung über ihre jederzeitige Widerrufbarkeit in Bezug auf zukünftige Verarbeitungen zu informieren. Bei anonymisierten Daten sind zukünftige Verarbeitungen mangels Anwendbarkeit der DSGVO gerade nicht ausgeschlossen. Die Einwilligung liefe somit ins Leere.

c) Berechtigtes Interesse

Für einfache personenbezogene Daten kommen darüber hinaus überwiegende berechtigte Interessen des Verantwortlichen gem. Art. 6 Abs. 1 lit. f DSGVO in Betracht. Die Interessenabwägung dürfte dabei unter Vorbehalt der Besonderheiten des Einzelfalls grundsätzlich zu Gunsten des Verantwortlichen ausgehen. Von der Anonymisierung der Daten gehen für den Betroffenen regelmäßig keine Risiken oder Gefahren aus. Er dürfte daher kaum ein entgegenstehendes Interesse haben. Hingegen hat der Verantwortliche ein großes wirtschaftliches Interesse an der Verwendung von anonymisierten Daten. Dass auch wirtschaftliche Interessen berechtigte Interessen sein können, ergibt sich aus ErwGr. 47, der dies ausdrücklich für den Zweck der Direktwerbung feststellt. Zudem besteht ein erhebliches Interesse der Gesellschaft und der Allgemeinheit an der effektiven Verwendung anonymisierter Daten, da diese ohne Gefahr für Betroffene gesellschaftliche Mehrwerte generieren kann. Nicht ohne Grund sehen die Datenstrategien der Bundesregierung und der EU-Kommission vor, dass Deutschland und die EU sich als Vorreiter bei der effektiven Datennutzung etablieren sollen. Das Eckpunktepapier für die Datenstrategie der Bundesregierung befasst sich dementsprechend ausdrücklich mit der Anonymi-

sierung. Deshalb ist Art. 6 Abs. 1 lit. f DSGVO geeignete Rechtsgrundlage für die Anonymisierung. Nur in besonders gelagerten Ausnahmefällen wird ein entgegenstehendes Interesse des Betroffenen gegeben sein, das eine Anonymisierung auf Grundlage dieser Norm ausschließt.

Die Regelung des berechtigten Interesses als Rechtsgrundlage für Datenverarbeitungen findet sich nicht in Art. 9 Abs. 2 DSGVO, sodass besondere Kategorien personenbezogener Daten nicht auf dieser Basis anonymisiert werden können. Wie bereits erwähnt, zeigt dies, dass Anonymisierung und Pseudonymisierung bei gesetzessystematischer Betrachtung keine rechtfertigungsbedürftigen Verarbeitungen sein können.

d) Zweckändernde Verarbeitung

Der Einschätzung des BfDI ist zuzustimmen, dass eine Anonymisierung auch auf Grundlage von Art. 6 Abs. 4 DSGVO i. V. m. der ursprünglichen Rechtsgrundlage durchgeführt werden kann. Zu beachten ist allerdings, dass im Rahmen der Kompatibilitätsprüfung nicht auf die bezweckte Weiterverarbeitung der anonymisierten Daten abgestellt werden kann, sondern nur auf die Anonymisierung selbst. Anonymisierte Daten sollen gerade dem Anwendungsbereich der DSGVO entzogen sein. Käme es darauf an, für welche Zwecke die anonymisierten Daten weiterverarbeitet werden sollen, so würde der Anwendungsbereich der DSGVO durch die Hintertür auf anonymisierte Daten erstreckt. Dies kann in Anbetracht der Tatsache, dass anonymisierte Daten frei verarbeitet werden sollen, nicht sein.
Würde man auf den Zweck abstellen, zu dem die anonymisierten Daten weiterverarbeitet werden sollen, entstünde außerdem eine ungerechtfertigte Ungleichbehandlung von Verantwortlichen. Es würden sich einseitig Vorteile für solche Verantwortliche ergeben, die die Schranke des Art. 6 Abs. 4 DSGVO aufgrund eines kompatiblen Weiterverarbeitungszwecks überschreiten könnten. Ist diese Schranke überwunden, dürfte ein solcher Verantwortlicher die anonymisierten Daten auch für jegliche andere Zwecke verarbeiten. Einem Verantwortlichen, der diese Schranke nicht überwinden kann, ist die Weiterverarbeitung anonymisierter Daten verwehrt.
Da eine erfolgreiche Anonymisierung dazu führt, dass von der weiteren Verarbeitung der Daten ohnehin keine Gefahr mehr für die Betroffenen ausgeht, sind die Zwecke der Weiterverarbeitung für die Abwägung nach Art. 6 Abs. 4 DSGVO unerheblich. Vielmehr ist die Anonymisierung selbst der Zweck, der im Rahmen der Kompatibilitätsprüfung entscheidend ist. Die Kompatibilität dürfte grundsätzlich nur in besonderen Ausnahmefällen zu verneinen sein. Die im Abschnitt „c) Berechtigtes Interesse“ dieser Stellungnahme angeführten Erwägungen gelten entsprechend.

Um Unsicherheiten für nicht-öffentliche Verantwortliche zu vermeiden, sollte im Papier des BfDI zudem ausdrücklich darauf hingewiesen werden,

dass die Anonymisierung von besonderen Kategorien von Daten nach Art. 9 Abs. 1 DSGVO auf Grundlage von Art. 6 Abs. 4 DSGVO erfolgen kann. Die zweckändernde Verarbeitung stellt mangels anderer passender Erlaubnistatbestände in Art. 9 Abs. 2 DSGVO die einzige Rechtsgrundlage dar, mit der nicht-öffentliche Verantwortliche verlässlich etwa Gesundheitsdaten anonymisieren können.

e) Erfüllung einer rechtlichen Verpflichtung

Wie der BfDI zutreffend ausführt, kann die Anonymisierung dafür genutzt werden, um die Löschpflicht aus Art. 17 Abs. 1 DSGVO zu erfüllen. Insoweit hat der Verantwortliche die Wahlfreiheit, ob er die Daten löscht oder anonymisiert. Im Sinne der Vollständigkeit sollte ergänzt werden, dass die Erfüllung weiterer rechtlicher Verpflichtungen nach Art. 6 Abs. 1 lit. c DSGVO mittels Anonymisierung in Betracht kommt. Neben spezialgesetzlichen Vorschriften, die ausdrücklich eine Pflicht zur Anonymisierung vorsehen (z. B. § 27 Abs. 3 BDSG), kann insbesondere auf die Pflicht in Art. 32 Abs. 1 DSGVO verwiesen werden, geeignete technische und organisatorische Maßnahmen zu treffen. In Abs. 1 lit. a der Norm wird die Pseudonymisierung neben anderen, nicht abschließend genannten TOMs genannt. Wie bei der Erfüllung der Löschpflicht muss der Verantwortliche die Wahl haben, ob er der Pflicht aus Art. 32 DSGVO mit Hilfe der explizit genannten TOMs nachkommt oder durch Anonymisierung der Daten.

Für besondere Kategorien personenbezogener Daten sollte der BfDI auf den Art. 9 Abs. 2 lit. g DSGVO verweisen, der für die Anonymisierung sensibler Daten dem Art. 6 Abs. 1 lit. c DSGVO entspricht.

Berlin, den 23.03.2020