PLATTFORM INDUSTRIE 4.0

DISKUSSIONSPAPIER

Anonymisierung im Datenschutz als Chance für Wirtschaft und Innovationen

Impressum

Herausgeber
Bundesministerium für Wirtschaft
und Energie (BMWi)
Öffentlichkeitsarbeit
11019 Berlin
www.bmwi.de

Redaktionelle Verantwortung
Geschäftsstelle Plattform Industrie 4.0
Bülowstraße 78
10783 Berlin

Gestaltung
PRpetuum GmbH, München

Stand
April 2020

Bildnachweis
Adobe Stock / Artem

Diese und weitere Broschüren erhalten Sie bei:
Bundesministerium für Wirtschaft und Energie
Referat Öffentlichkeitsarbeit
E-Mail: publikationen@bundesregierung.de
www.bmwi.de

Zentraler Bestellservice:
Telefon: 030 182722721
Bestellfax: 030 18102722721

Inhalt

Management Summary

- Für alle Bereiche der Digitalisierung ist die Nutzung anonymer Daten von größter Relevanz. Das zeigt einmal mehr das aktuelle Beispiel der Corona-Pandemie.

- Um Chancen für Wirtschaft und Innovationen zu eröffnen und nutzbar zu machen, sind unnötige datenschutzrechtliche Hürden für die Anonymisierung zu vermeiden.

- Ob Daten personenbezogen sind, beurteilt sich subjektiv aus der aktuellen Situation des konkreten Verarbeiters. Dieselben Daten können für verschiedene Verarbeiter personenbezogen, pseudonym oder anonym sein. Daher gibt es auch keine objektive Abgrenzung zwischen pseudonymen und anonymen Daten.

- Eine Anonymisierung ist nur im Einzelfall eine Verarbeitung personenbezogener Daten, was auch von der konkreten Umsetzung abhängt. Eine Rechtsgrundlage für die Anonymisierung ist daher nicht stets erforderlich.

- Eine im Einzelfall erforderliche Rechtsgrundlage kann bei einer Weiterverarbeitung (Art. 6 Abs. 4 DS-GVO) die ursprüngliche Rechtsgrundlage bieten oder bei einer Neuverarbeitung jede einschlägige Rechtsgrundlage (Art. 6 Abs. 1 DS-GVO).

- Als im Einzelfall erforderliche Rechtsgrundlage kommt auch berechtigtes Interesse in Betracht (Art. 6 Abs. 1 lit. f DS-GVO). Die entsprechende Interessenabwägung ermöglicht regelmäßig eine Anonymisierung.

- Verarbeitungszweck der Anonymisierung ist die Entfernung eines vorhandenen Personenbezugs, nicht etwa eine bestimmte Nutzung anonymer Daten.

- Eine Anonymisierung nach aktueller Technologie führt zu anonymen Daten, die weder der DS-GVO noch einer Zweckbindung unterliegen. Die zukünftige Herstellung eines Personenbezugs von anonymen Daten bedürfte als neue Verarbeitung personenbezogener Daten einer Rechtsgrundlage.

Arbeitsgruppe „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.

Einleitung

Die Plattform Industrie 4.0 hat sich durch die Arbeitsgruppe „Rechtliche Rahmenbedingungen“ am Konsultationsverfahren des *Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI)* zum Thema „Anonymisierung unter der DS-GVO unter besonderer Berücksichtigung der TK-Branche“ beteiligt.[1] Das nimmt die Arbeitsgruppe „Rechtliche Rahmenbedingungen“ („wir“) zum Anlass, ihren Standpunkt darzustellen.

Anonymisieren von Daten und der Umgang mit anonymen Daten sind nicht nur für die Plattform Industrie 4.0 relevant, sondern für die gesamte Digitalisierung in allen Branchen. Die Bedeutung der Anonymisierung für eine zukunftsfähige Wirtschaft kann man kaum überschätzen.

Eine Anonymisierung bietet zahlreiche Vorteile. Auch Verbraucher und Endkunden profitieren davon, wenn Unternehmen mit anonymen Daten ihre Produktion, Dienst- und Serviceleistungen verbessern können. Gleichzeitig zeigen wir die Risiken für die Wirtschaft und Innovationen auf, wenn die Möglichkeiten von Unternehmen beschränkt werden, anonymisierte Daten zu generieren und zu nutzen.

Die Datenschutz-Grundverordnung (DS-GVO) bietet genügend Möglichkeiten, um einen Ausgleich zwischen dem Recht des Einzelnen auf Schutz seiner Privatsphäre und den Unternehmensinteressen mit Blick auf eine Anonymisierung zu ermöglichen.

I. Bedeutung der Anonymisierung für Wirtschaft und Innovationen

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, autonomem Fahren oder die Verbesserung eigener Dienstleistungen und Serviceangebote – um nur einige Beispiele zu nennen.

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.

Wir stellen im Folgenden die Rolle des Datenschutzes für die Anonymisierung sowie damit verbundene Herausforderungen und Chancen dar. Zur Veranschaulichung wird ein Beispiel verwendet:

> Die Kundin A kauft sich einen Laptop. Bei der Inbetriebnahme registriert sie ihren Laptop beim Hersteller des Betriebssystems, der Firma X, um das Betriebssystem über einen Testzeitraum hinaus nutzen zu können. Die Firma X fragt die Kundin A dabei, ob sie freiwillig Meldungen über etwaige Fehler an die Firma X automatisch übermitteln möchte. Die Firma X möchte damit ihr Betriebssystem verbessern. A erklärt sich einverstanden.

1 Abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Konsultationsverfahren/2020/01_Anonymisierung-TK.pdf?__blob=publicationFile&v=6 (zuletzt besucht am 25.03.2020).

II. Welche Rolle spielt Datenschutz für die Anonymisierung?

1. Grundprinzipien des Datenschutzes

a) Verbotsprinzip mit Erlaubnisvorbehalt

Im europäischen Datenschutzrecht gilt als Grundsatz das Verbot einer Verarbeitung personenbezogener Daten, wenn diese nicht ausnahmsweise erlaubt ist (Verbotsprinzip mit Erlaubnisvorbehalt). Eine Verarbeitung von personenbezogenen Daten setzt voraus, dass ein Datenverarbeiter eine Rechtsgrundlage nutzen kann, um personenbezogene Daten in erlaubter Weise rechtmäßig zu verarbeiten. Ein Datenverarbeiter kann etwa ein Unternehmen sein und ist Verantwortlicher nach der DS-GVO (Art. 4 Nr. 7 DS-GVO).

Als Rechtsgrundlagen können unter anderem in Betracht kommen:

- Einwilligung der betroffenen Person (Art. 6 Abs. 1 lit. a DS-GVO)
- Vertragsanbahnung oder Vertragserfüllung (Art. 6 Abs. 1 lit. b DS-GVO)
- Berechtigtes Interesse des Verantwortlichen (Art. 6 Abs. 1 lit. f DS-GVO)

b) Was sind personenbezogene Daten?

Der Europäische Gerichtshof (EuGH) versteht den Begriff „Personenbezogene Daten weit.

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (Betroffener) beziehen. Ein Betroffener wird als identifizierbare Person angesehen, wenn er direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann (Art. 4 Nr. 1 DS-GVO).

c) Was sind pseudonymisierte Daten?

Pseudonymisierte Daten sind personenbezogene Daten. Allerdings ist zwischen einem pseudonymisierten Datum und einem Klardatum ein Zwischenschritt erforderlich. Pseudonymisierung bedeutet die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden (Art. 4 Nr. 5 DS-GVO).

Man sieht also nicht auf den ersten Blick, welcher Betroffene hinter einem Pseudonym steht. Der Betroffene ist aber identifizierbar, wenn ihm sein Pseudonym zugeordnet werden kann.

d) Was sind anonyme Daten?

Anonyme Daten sind keine personenbezogenen Daten. Von einem anonymen Datum kann nicht (mehr) auf ein personenbezogenes Datum (zurück-)geschlossen werden.

Die Grundsätze des Datenschutzes gelten nicht für anonyme Informationen (Erwägungsgrund 26 S. 5 und 6 DS-GVO), d.h. für Informationen, die sich nicht (mehr) oder noch nicht auf einen Betroffenen beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass der Betroffene nicht oder nicht mehr identifiziert werden kann. Die DS-GVO, das deutsche und europäische Datenschutzrecht sind also auf anonyme Daten nicht anwendbar.

Man sieht also nicht, welcher Betroffene in Verbindung mit einem anonymen Datum stand. Ob ein anonymes Datum in der Zukunft einem Betroffenen zugeordnet werden kann, spielt im Zeitpunkt, zu dem das Datum anonym ist, keine Rolle. Ob eine Zuordnung in der Zukunft rechtmäßig ist, muss der Verantwortliche in der Zukunft prüfen, wenn sich diese Frage stellt.

e) Was ist eine Verarbeitung?

Der EuGH und die DS-GVO verstehen auch den Begriff Verarbeitung weit.

Ein Verantwortlicher muss nur irgendetwas mit personenbezogenen Daten machen, damit eine Verarbeitung gegeben ist. Eine Verarbeitung ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung (Art. 4 Nr. 2 DS-GVO).

Die Firma X möchte von der Kundin A Informationen über etwaige Fehler im Zusammenhang mit ihrer Nutzung des Betriebssystems erhalten. Nachdem die Kundin A ihre Einwilligung erteilt hat, solche Fehler automatisch zu melden, kann die Firma X solche Fehlermeldungen der Kundin A zuordnen.

Die Firma X ist Verantwortliche für diese Verarbeitung personenbezogener Daten. Die Firma X verarbeitet diese Daten aufgrund einer Einwilligung der Kundin A, um das eigene Betriebssystem verbessern zu können.

2. Grenzen zwischen personenbezogenen, anonymen und pseudonymen Daten

Ob ein anonymes oder personenbezogenes Datum vorliegt, beurteilt sich nach der Definition von Art. 4 Nr. 1 DS-GVO unter Beachtung der Breyer-Entscheidung des EuGH.[2] Dabei ist auf den konkreten Datenverarbeiter in seiner aktuellen subjektiven Situation abzustellen (relativer Personenbezug). Dasselbe Datum kann für einen Datenverarbeiter personenbezogen, für einen anderen Datenverarbeiter pseudonym und für einen weiteren Datenverarbeiter anonym sein.

Wir möchten in diesem Zusammenhang auf unser Ergebnispapier *„Wie das Recht Schritt hält“* verweisen, das beschreibt, dass die Regelungen zur Verarbeitung pseudonymisierter Daten im derzeitigen Recht unterentwickelt sind.[3] Aus den Erwägungsgründen 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.

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 verbraucherorientierten 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.

Die Bedeutung der Anonymisierung und des Umgangs mit anonymen Daten kann gar nicht überschätzt werden.

Dabei ist aufgrund der maßgeblichen relativen Beurteilung eines Personenbezugs nach der aktuellen subjektiven Situation des konkreten Verarbeiters keine objektive Abgrenzung zwischen anonymen und pseudonymen Daten möglich. Die Abgrenzung zwischen personenbezogenen, anonymen und pseudonymen Daten muss daher jeweils im Einzelfall und aus Sicht eines jeden konkreten Datenverarbeiters erfolgen.

Wenn die Firma X von der Kundin A erfährt, dass das Betriebssystem abstürzt, wenn die Kundin A die Anwendung 123 startet, sind dies personenbezogene Daten.

Wenn die Firma X an den Entwickler der Anwendung 123 weitergibt, „beim Start dieser Anwendung stürzt das Betriebssystem ab“, ist das für diesen Entwickler kein personenbezogenes Datum. Der Entwickler weiß erst recht nicht, bei welchen Kunden dies passiert ist. Er weiß nicht, dass die Kundin A dies gemeldet hat. Er erfährt nur, dass beim Start seiner Anwendung das Betriebssystem der Firma X abstürzt.

2 EuGH, Urteil vom 19.10.2016, Az. C-582/14 = BeckRS 2016, 82520.

3 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.

III. Wann ist eine Anonymisierung datenschutzrechtlich zulässig?

Aus datenschutzrechtlicher Sicht kann eine Anonymisierung zulässig sein, wenn eine Rechtsgrundlage gegeben ist oder wenn die DS-GVO bereits gar nicht anwendbar ist.

1. Anonymisierung nur im Einzelfall als Verarbeitung

Es kann bereits diskutiert werden, ob eine Anonymisierung stets eine Verarbeitung personenbezogener Daten im Sinne des deutschen und europäischen Datenschutzrechts darstellt.[4] Zwar könnte der weite Begriff der Verarbeitung dafür sprechen, aber systematisch hat die DS-GVO die Anonymisierung nicht geregelt. Die Erwägungsgründe 26 S. 5 und 6 DS-GVO zeigen, dass die Grundsätze des Datenschutzes nicht für anonyme Daten gelten.

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.

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. 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.

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

Aus Art. 6 Abs. 1 lit. e der Richtlinie 95/46/EG[5] und der ePrivacy-Richtlinie hat die Artikel-29-Gruppe in WP 216 geschlossen, dass personenbezogene Daten zumindest „standardmäßig“ anonymisiert werden sollten.[6]

Würde für den Anonymisierungsvorgang[7] 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.

> Die Firma X kann die Information „beim Start der Anwendung 123 stürzt das Betriebssystem ab“ in eine gesonderte Datenbank ablegen. Wenn sie dem Entwickler nur Zugang zu dieser Datenbank gibt, verarbeitet der Entwickler beim Lesen dieser Information keine personenbezogenen Daten.

4 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.

5 Entspricht Art. 5 Abs.1 lit. e DS-GVO.

6 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 (WP216).

7 Diese Stellungnahme geht nur von Anonymisierungsvorgängen aus, die zu echter Anonymisierung führen.

Daher ist eine Einzelfallbetrachtung erforderlich. Eine Rechtsgrundlage kann für die jeweilige Anonymisierung erforderlich sein. In anderen Fällen kann eine solche entbehrlich sein, weil bereits der Anwendungsbereich des Datenschutzrechts nicht eröffnet ist.

2. Neuverarbeitung und Weiterverarbeitung

Wie bereits dargestellt ist eine Anonymisierung nicht immer eine Verarbeitung im datenschutzrechtlichen Sinn. Dies bedeutet, es gibt relevante Fälle, in denen ein Verantwortlicher keine datenschutzrechtliche Rechtfertigung benötigt, weil er von Anfang nur mit anonymen Daten umgeht.

Es gibt jedoch auch Fälle, in denen ein Verantwortlicher zunächst auf personenbezogene Daten zugreift und sich fragt, ob und gegebenenfalls wie er diese Daten anonymisieren kann, etwa um seinen Service zu verbessern.

Als mögliche Rechtsgrundlagen für eine Anonymisierung kann insbesondere das berechtigte Interesse nach Art. 6 Abs. 1 lit. f DS-GVO herangezogen werden. Vorhandene personenbezogene Daten könnten für einen neuen Zweck, hier die Anonymisierung, (neu) verarbeitet werden. Wenn Art. 6 Abs. 1 lit. f DS-GVO als Rechtsgrundlage greift, ist es nicht erforderlich, dass der Verantwortliche den Betroffenen nach dessen Einwilligung in die Anonymisierung (Art. 6 Abs. 1 lit. a DS-GVO) fragt. Zudem ist eine zulässige Weiterverarbeitung nach Art. 6 Abs. 4 DS-GVO denkbar, wenn diese Daten für einen anderen Zweck bereits rechtmäßig verarbeitet werden.

Beide Alternativen setzen die Einhaltung der weiteren Anforderungen der DS-GVO voraus. Die erforderliche Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO wird aus unserer Sicht immer zugunsten des Datenverarbeiters ausfallen. Wirtschaftliche Interessen, die ein Datenverarbeiter regelmäßig verfolgt, sind zulässige Interessen im Rahmen dieser Abwägung. Dem Interesse des Betroffenen nach Schutz seiner Privatsphäre wird entsprochen, wenn der jeweilige Personenbezug (vollständig) aufgehoben wird, also seine Daten anonymisiert werden und ihm nicht mehr zugeordnet werden können.

Wir sind der Ansicht, dass Art. 6 Abs. 4 DS-GVO als Zulässigkeitsvorschrift zwar grundsätzlich anwendbar ist, aber diese Norm für die Praxis oft ungeeignet ist. Es verbleibt ein zu hohes Maß an Rechtsunsicherheit. Die Rechtsnatur von Art. 6 Abs. 4 DS-GVO ist in mehrfacher Hinsicht unklar.[8] Jedenfalls entfaltet Art. 6 Abs. 4 DS-GVO aber keine Sperrwirkung für andere Rechtfertigungsgründe.[9] Aus Erwägungsgrund 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.[10]

Ein Datenverarbeiter kann daher im Einklang mit der DS-GVO jedenfalls nach Art. 6 Abs. 1 lit. f DS-GVO personenbezogene Daten aufgrund überwiegender berechtigter Interessen anonymisieren. Gleichzeitig ist zu betonen, dass nicht jede Anonymisierung auch eine Verarbeitung im Sinne der DS-GVO ist.

Ist eine Anonymisierung erfolgreich durchgeführt, ist der Personenbezug eines Datums aufgehoben. Der (weitere) Umgang mit solchen anonymen Daten stellt keine Verarbeitung im Sinne der DS-GVO dar. Ein Unternehmer, der mit solchen Daten umgeht, muss jedenfalls nicht die Anforderungen der DS-GVO einhalten, solange die Daten anonym sind.

> Die Firma X kann die Information „beim Start der Anwendung 123 stürzt das Betriebssystem ab", gemeldet von Kundin A", in einer Datenbank ablegen. Die Firma X kann später die Zusatzinformation „gemeldet von Kundin A" vollständig entfernen. Wenn diese Zusatzinformation nicht mehr zugeordnet werden kann, weil auch die ursprüngliche automatische Meldung nicht mehr vorhanden ist, ist die verbleibende Information, „beim Start der Anwendung 123 stürzt das Betriebssystem ab", ein anonymes Datum.
>
> Die Privatsphäre der Kundin A ist jetzt besser geschützt als vorher, ihr Name ist in der Datenbank gar nicht mehr vorhanden.

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

9 *Assion/Nolte/Veil,* in: Gierschmann/Schlender/Stentzel/Veil, DS-GVO, 2017, Art. 6 Rdnr. 201 ff.

10 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.

IV. Anonymisierung als Herausforderung für die Wirtschaft und Innovationen

Die Herausforderungen für die Wirtschaft und für Innovationen ergeben sich daraus, dass ein Anonymisierungsvorgang im Einzelfall von Datenschutzaufsichtsbehörden und Rechtswissenschaftlern als eine Verarbeitung im datenschutzrechtlichen Sinne angesehen wird.

Wenn eine Anonymisierung im Einzelfall eine datenschutzrechtliche Verarbeitung darstellt, kommt es auch auf eine Rechtsgrundlage und die weiteren Anforderungen der DS-GVO an. Vor diesem Hintergrund werden auch Anforderungen der DS-GVO für einen Anonymisierungsvorgang als datenschutzrechtliche Verarbeitung angesprochen.

1. Kein uneingeschränkter Datenschutz

Zur Einordnung dieser Herausforderung stellen wir betroffene Grundrechtspositionen dar.

Art. 8 Charta der Grundrechte der Europäischen Union (Charta) schützt personenbezogene Daten. Art. 16 der Charta schützt gleichzeitig die unternehmerische Freiheit. Diesem Spannungsverhältnis trägt Erwägungsgrund 4 S. 4 DS-GVO auch Rechnung.

Um einen praktischen Ausgleich zwischen diesen Grundrechtspositionen zu erreichen, ist dieses Spannungsverhältnis zu 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.

Daher sind wir der Auffassung, dass in diesem Spannungsfeld für eine Anonymisierung keine Hürden aufgestellt werden sollten, die der Grundrechtsschutz von Betroffenen nicht zwingend erfordert.

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

Eine Herausforderung ist die Unsicherheit im Umgang mit Art. 6 Abs. 4 DS-GVO.

Im Rahmen von Art. 6 Abs. 4 DS-GVO ist auf die konkrete Weiterverarbeitung abzustellen. Wenn eine konkrete Anonymisierung eine datenschutzrechtliche Verarbeitung darstellen würde, wäre die Weiterverarbeitung nach Art. 6 Abs. 4 DS-GVO (nur) die Anonymisierung der Daten selbst.

Der ursprüngliche Verarbeitungszweck personenbezogener Daten, etwa die Begründung und Ausgestaltung eines Vertragsverhältnisses, darf nicht zu dem künftigen Zweck eines künftigen Umgangs mit anonymisierten Daten in Relation gesetzt werden.

Der Zweck der Anonymisierung als (Weiter-)Verarbeitung ist die Entfernung des Personenbezugs. Ein Zweck des späteren Umgangs mit den anonymen Daten 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.

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 bei der Anonymisierung geprüften Zweck begrenzt sein soll. Das würde durch Art. 16 Charta geschützte Rechte ohne erforderliche Legitimation beeinträchtigen und verbietet sich auch deswegen klar.

Ein Kompatibilitätstest im Rahmen von Art. 6 Abs. 4 DS-GVO kann dabei verallgemeinert werden: Einer betroffenen Person kann bei einer Anonymisierung nichts passieren; sie kann nicht besser geschützt werden, als gar nicht mehr betroffen zu sein.

Selbst wenn eine Anonymisierung als datenschutzrechtliche Verarbeitung angesehen würde, muss diese regelmäßig nach Art. 6 Abs. 4 DS-GVO zulässig sein.

3. (Re-)Identifizierung als neue Verarbeitung

Eine weitere Herausforderung ist die Annahme des BfDI im Rahmen der Konsultation, bei einer Anonymisierung würde ein Restrisiko der Re-Identifizierung verbleiben.[11]

11 Vgl. BfDI, Anonymisierung unter der DS-GVO unter besonderer Berücksichtigung der TK-Branche, S. 9.

Wenn eine Anonymisierung nach aktuellem Stand verfügbarer Technologien erfolgt, ist auch eine Re-Identifizierung nach diesem Stand der Technik zu beurteilen. So anonymisierte Daten sind mit *Status quo* anonym.

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 denklogisch nicht für alle Zukunft unwiderruflich unmöglich gemacht werden.[12]

Eine Anonymisierung nach „state of the art" verpflichtet daher auch nicht zur ständigen Überwachung etwaiger (Rest-)Risiken.[13] So gibt es etwa im Bereich des maschinellen Lernens erste praktikable Ansätze für kryptografische Verfahren für kollaboratives Lernen, wie die „sichere Mehrparteienberechnung" (engl. "secure multiparty computation").[14]

Dies bedeutet, 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.

4. Vorabinformation bei Weiter- und Neuverarbeitung

Zusätzlich sind als Herausforderung die weiteren Anforderungen der DS-GVO zu beachten.

Wenn eine Anonymisierung im Einzelfall eine Weiter- oder Neuverarbeitung darstellt, gelten dafür auch die Informationspflichten nach 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, exbetroffene Personen zu informieren. Ein solcher Datenschutzhinweis unterbleibt daher in der Regel. Ein Verantwortlicher wird in solchen Fällen regelmäßig Maßnahmen nach Art. 14 Abs. 5 lit. b S. 2 DS-GVO ergreifen.

Daneben ist es jedenfalls nach Art. 13, 14 DS-GVO zulässig, Informationspflichten für eine Anonymisierung als Verarbeitung auch vorweg einzulösen. Dies folgt aus dem Wortlaut der DS-GVO.[15]

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.

Stellt eine Anonymisierung im Einzelfall eine datenschutzrechtliche Verarbeitung dar, muss ein Verantwortlicher die Anforderungen der DS-GVO einhalten, solange für zu anonymisierende Daten der Anwendungsbereich der DS-GVO (noch) gegeben ist.

5. Technische Aspekte einer Anonymisierung

Neben den rechtlichen Herausforderungen bestehen auch technische Herausforderungen.

Eine echte Anonymisierung setzt dabei oftmals mehrere unterschiedlich komplexe Arbeitsschritte voraus. Nachdem der Personenbezug eines Datums weit zu verstehen ist, können umfangreiche Maßnahmen erforderlich sein, um eine Anonymisierung rechtlich und tatsächlich zu erreichen. Ein praxisrelevantes Beispiel ist die Kürzung einer IP-Adresse. Wird von der Beispiel-IP-Adresse 123.456.789.123 das letzte Oktett „.123" irreversibel abgeschnitten, kann die vollständige Beispiel-IP-Adresse aus dem verbleibenden Adressteil nicht mehr ermittelt werden.

Als rechtliche Absicherung ist auch die Zusage eines Unternehmens denkbar, keine Zusatzinformationen einem anderen Unternehmen bereitzustellen. Dieses andere Unternehmen kann zudem darauf verzichten, irgendwie geartete Ansprüche auf Erteilung solcher Zusatzinformationen geltend zu machen.

12 Möglicherweise anders interpretierbar WP 216, S. 3.

13 Möglicherweise anders interpretierbar WP 216, S. 29 f.

14 Vgl. *Winter/Battis/Halvani,* Herausforderungen für die Anonymisierung von Daten, ZD 2019, 489, 492.

15 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.

Das Bundesministerium für Wirtschaft und Energie (*BMWi*) hat in einer Studie entsprechende Ergebnisse zu technischen Anonymisierungsmöglichkeiten veröffentlicht.[117]

Weitere Ausführungen dazu enthält auch der Technical Report des *BMWi*-Technologieprogamms Smart Data – Innovationen aus Daten: „Smart Data – Smart Privacy?".[17]

Die Firma X kann eine Anonymisierung auf verschiedenen Wegen erreichen.

Sie kann die personenbezogenen Daten „beim Start der Anwendung 123 stürzt das Betriebssystem ab, gemeldet von Kundin A" erheben. Sie kann dann den Personenbezug „gemeldet von Kundin A" abschneiden. Die Firma X sollte über diese Verarbeitung transparent im Rahmen ihrer Datenschutzhinweise informieren.

Sie kann von Anfang an nur die Information erheben „beim Start der Anwendung 123 stürzt das Betriebssystem ab". Dies setzt voraus, dass in keinem Fall identifizierende Zusatzinformationen vorhanden sind.

Die Firma X kann in beiden Varianten ihr Vorgehen rechtfertigen. Dem Entwickler der Anwendung 123 sollte die Firma X nur dann nähere Informationen zur Kundin A mitteilen, hier den Namen und die Kundenbeziehung, wenn dafür die Rechtmäßigkeit geklärt ist.

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

17 Vgl. Technical Report des BMWi-Technologieprogramms „Smart Data – Innovationen aus Daten", Smart Data – Smart Privacy?, 11/2015, S. 7 ff.; abrufbar unter: https://www.hiig.de/wp-content/uploads/2015/12/SmartData_Thesenpapier_smart_Privacy.pdf.

V. Anonymisierung als Chance für die Wirtschaft und Innovationen

Durch Anonymisierung können Chancen für die Wirtschaft und Innovationen geschaffen und genutzt werden.

1. Anonymisierte Daten ohne Zweckbindung

Es gibt unter keinem Gesichtspunkt eine direkte oder indirekte Fortsetzung einer Zweckbindung für anonyme Daten. Für anonyme Daten gilt die DS-GVO nicht.[18] 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.

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. Ein Verantwortlicher kann rechtmäßig verarbeitete personenbezogene Daten jederzeit auch vor einer gesetzlichen Lösch- oder Anonymisierungspflicht anonymisieren. Er kann diese anonymen Daten auch für eine weitere, anonyme und damit datenschutzrechtlich nicht relevante Verarbeitung verwenden.

2. Beispielhafte Anwendungsfelder

Anwendungen im Bereich künstlicher Intelligenz sind davon abhängig, dass eine künstliche Intelligenz trainiert wird. Dazu sind möglichst viele (aussagekräftige) Daten erforderlich.

Das autonome Fahren setzt voraus, dass Kameras und Sensoren die Umwelt richtig erfassen. Ein intelligentes Auto muss nicht wissen, wer an einem Zebrastreifen steht. Die Software muss aber erkennen, ob dass ein Mensch oder ein Tier am Zebrastreifen steht. Dazu muss die Software ausreichend mit (aussagekräftigen) Daten befüllt werden.

Die Entwicklung und Verbesserung eines Betriebssystems setzt voraus, möglichst alle Fehler auszuwerten, die im Live-Betrieb auftreten können.

Diese Beispiele haben eines gemeinsam: Ein Personenbezug ist nicht erforderlich, auch wenn er zuvor einmal bestand oder für bestimmte Verantwortliche noch immer besteht.

Der Entwickler der Anwendung 123 und die Firma X werden durch die Information „beim Start der Anwendung 123 stürzt das Betriebssystem ab“ möglicherweise erst auf ein Problem aufmerksam. Das ist der erste Schritt zur Lösung des Problems, damit beim Start der Anwendung 123 das Betriebssystem nicht mehr abstürzt.

18 Vgl. EG. 26 Sätze 5 und 6 DS-GVO.

Fazit

Anonymisierung ist für die gesamte Digitalisierung eine zentrale Fragestellung.

Zu hohe Hürden an eine Anonymisierung, die zudem im Spannungsverhältnis verschiedener Grundrechtspositionen nicht in jedem Einzelfall angezeigt sind, können Wirtschaft und Innovationen hemmen. Ohne praktikable Anonymisierungsmöglichkeiten für die deutsche Wirtschaft werden Entwicklungen in den datengetriebenen Zukunftsbereichen woanders stattfinden. Wertschöpfungsketten, die im Zusammenhang mit Daten greifbar sind, wären dann unerreichbar.

Dabei gibt es keinen Grund, solche Hürden aus datenschutzrechtlicher Sicht zu fordern. Ein Betroffener kann nicht besser geschützt werden, als nicht mehr betroffen zu sein. Zugleich können Unternehmen durch die Nutzung von Daten, auch von maschinengenerierten Daten, die Digitalisierung vorantreiben. Sie können die Entwicklung von künstlicher Intelligenz, autonomem Fahren oder die Verbesserung eigener Dienstleistungen und Serviceangebote fördern. Davon profitieren auch Verbraucher und Endkunden.

Nach unserer Auffassung können Betroffene und Verantwortliche nur profitieren. Daher überraschen manche datenschutzrechtlichen Diskussionen im Kontext der Anonymisierung.

AUTOREN

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

Diese Publikation ist ein Diskussionspapier der AG 4 „Rechtliche Rahmenbedingungen“ der Plattform Industrie 4.0.

www.plattform-i40.de