Anonymisierung aus Sicht des Datenschutzes und des Datenschutzrechts*

Jörg Pohle[1], Julian Hölzel[2]

[1] Alexander von Humboldt Institut für Internet und Gesellschaft
Französische Straße 9, 10117 Berlin
joerg.pohle@hiig.de
[2] Rechtsreferendar am Kammergericht Berlin
hoelzelj@mailbox.org

Zusammenfassung. Eine Anonymisierung ist eine Operation, die personenbezogene Daten (Input) in nicht-personenbezogene Daten (Output) transformiert. Sie fällt in den Anwendungsbereich der Datenschutz-Grundverordnung. Der Zweck jeder Anonymisierung besteht darin, den Anwendungsbereich der DSGVO zu verlassen. Damit einher geht der Verlust des effektiven Schutzes der Grundrechte und Grundfreiheiten natürlicher Personen. Vor einer Anonymisierung ist demnach notwendig eine Datenschutz-Folgenabschätzung (DSFA) nach Artikel 35 DSGVO durchzuführen.

Schlüsselwörter: Datenschutz · Datenschutzrecht · DSGVO · Anonymisierung · personenbezogene Daten · anonyme Daten · anonymisierte Daten · Datenschutz-Folgenabschätzung

0 Vorbemerkungen

Der vorliegende Beitrag zum öffentlichen Konsultationsverfahren des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Thema „Anonymisierung unter der DSGVO“ analysiert das Problem der Anonymisierung aus einer dezidiert rechtsinformatischen Sicht. Dazu wird im Folgenden konsequent zwischen Datenschutz, Datenschutzrecht und der Datenschutz-Grundverordnung (DSGVO) unterschieden, mit Datenschutz als der „Menge der Vorkehrungen zur Verhinderung unerwünschter Folgen von Informationsverarbeitung“, Datenschutzrecht als der „Menge der Datenschutz-Rechtsnormen“,[1] und der DSGVO mit ihrem Ziel, „die Grundrechte und Grundfreiheiten natürlicher Personen“ zu schützen (Artikel 1 Abs. 2).

1 Einleitung

Eine Anonymisierung ist eine *Operation*, kein Zustand. Sie ist – wie alle Operationen – gekennzeichnet durch einen *Input* und einen *Output*: Sie transformiert Input in

[1] Vgl. dazu Wilhelm Steinmüller u. a. *Grundfragen des Datenschutzes*. Gutachten im Auftrag des Bundesministeriums des Innern. BT-Drs. VI/3826, Anlage 1. 1971, S. 44.

Output. Eine Anonymisierung ist – unabhängig vom konkret gewählten Anonymisierungs*verfahren* – eine Operation, die personenbezogene Daten (Input) in nicht-personenbezogene Daten (Output) transformiert.

In dieser Hinsicht ist die Anonymisierung vergleichbar mit dem *Löschen*. Auch das Löschen operiert auf personenbezogenen Daten als Input und transformiert diese in nicht-personenbezogene Daten (Output), genauer: in das leere Datum {}. Das Löschen ist in der Datenschutz-Grundverordnung (DSGVO) explizit als *Verarbeitung* geregelt (Artikel 4 Nr. 2).

Artikel 4 Abs. 2 DSGVO fasst „jeden [...] Vorgang oder jede [...] Vorgangsreihe im Zusammenhang mit personenbezogenen Daten“ als *Verarbeitung*. Unter den in der Verordnung aufgeführten Operationen, d.h. Vorgängen, sind solche, die personenbezogene Daten *nur als Input* verwenden, etwa „das Löschen oder die Vernichtung“, solche, die personenbezogene Daten *nur als Output* erzeugen, etwa „das Erheben“, sowie solche, die personenbezogene Daten *sowohl als Input wie als Output* haben, etwa „die Anpassung oder Veränderung“ oder „die Verwendung“. Anonymisierung ist eine Verarbeitung im Sinne der DSGVO.[2]

Das generelle Ziel der statistischen sowie der informatisch-technischen Forschung und Entwicklung im Bereich der Anonymisierungsverfahren besteht darin, ein Minimum an Identifizierbarkeit unter Zugrundelegung eines technischen, d. h. außerrechtlichen, „Anonymitätsmaßes“[3] zu gewährleisten bei gleichzeitiger Minimierung des Nutzwertverlustes der ausgegebenen anonymisierten gegenüber den eingegebenen personenbezogenen Daten.[4] Da es in den meisten Fällen darum geht, die anonymisierten Daten für statistische Aussagen zu nutzen, verfolgt die Forschung und Entwicklung insbesondere das Ziel der Aufrechterhaltung der statistischen Eigenschaften der Daten, einschließlich des in ihnen enthaltenen *Bias*.

2 Zweck und Folgen der Anonymisierung

Die Anonymisierung als Operation verarbeitet personenbezogene Daten mit dem Ziel, sie in nicht-personenbezogene Daten zu transformieren.

[2] So auch *Roßnagel* in Simitis / Hornung / Spieker, *Datenschutzrecht*, Artikel 4 Nr. 2, Rn. 12, 14 und 32.

[3] Siehe umfassend zu den diese Forschung und Entwicklung leitenden Annahmen und Anforderungen und deren Verhältnis zu den rechtlichen Anforderungen Julian Hölzel. „Anonymisierungstechniken und das Datenschutzrecht“. In: *Datenschutz und Datensicherheit* 42.8 (2018), S. 502–509.

[4] Vgl. Article 29 Data Protection Working Party. *Opinion 05/2014 on Anonymisation Techniques*. Working Paper WP 136. 2014, S. 5: Das Ziel bestehe darin, „retaining as much of the underlying information as required for the task“. Ein vergleichbares Ziel wird mit *Privacy-Enhancing Technologies* verfolgt: maximale Anonymisierung, „without losing the functionality of the information system“, G. W. van Blarkom, John J. Borking und J. G. E. Olk. *Handbook of Privacy and Privacy-Enhancing Technologies: The case of Intelligent Software Agents*. Den Haag: PISA Consortium, 2003, S. 3.

Der Zweck jeder Anonymisierung besteht darin, den Anwendungsbereich der DSGVO zu verlassen (dazu 2.1) und sich von der Pflicht zum Schutz der Grundrechte und Grundfreiheiten der Betroffenen sowie zur Wahrung der Betroffenenrechte zu befreien (dazu 2.2).

Vor dem Hintergrund, dass Zweck und Zweckbindung die Kernpunkte des Datenschutzrechts darstellen,[5] überrascht es sehr, dass der *BfDI-Entwurf* auf den Zweck, der mit der Anonymisierung verfolgt wird, an keiner Stelle eingeht.

2.1 Verlassen des Anwendungsbereichs der DSGVO

Der Anwendungsbereich der DSGVO ist nur dann eröffnet, wenn *personenbezogene Daten* verarbeitet werden (Artikel 2 Abs. 1).

Die offenkundig allgemein unterstellte Kausalität – im Sinne einer sowohl notwendigen wie hinreichenden Bedingung – zwischen der Verarbeitung „personenbezogenen Daten“ und den „unerwünschten Folgen von Informationsverarbeitung“[6] ist bisher, unabhängig selbst von der Beschränkung der unerwünschten Folgen von Informationsverarbeitung auf diejenigen für die Grundrechte und Grundfreiheiten natürlicher Personen, wie sie die DSGVO vornimmt, weder vom nationalen Gesetzgeber, vom europäischen Verordnungsgeber noch von der Literatur bewiesen oder auch nur plausibilisiert worden.[7] Die Verarbeitung „personenbezogener Daten“ ist weder notwendige noch hinreichende Bedingung für Riskanz moderner Informationsverarbeitung für Grund- und Freiheitsrechte: Sie ist keine notwendige Bedingung, weil nicht jede Verarbeitung solcher Daten Grundrechtsrisiken birgt, und sie ist keine hinreichende Bedingung, weil auch die Verarbeitung anderer als personenbezogener Daten Grundrechtsrisiken bergen kann.[8]

Tatsächlich ist das Grundrecht auf „Schutz personenbezogener Daten“ nach Artikel 8 GRCh das einzige Grundrecht, dessen Schutzbereich nur genau dann eröffnet

[5] Vgl. umfassend Bernhard Hoffmann. *Zweckbindung als Kernpunkt eines prozeduralen Datenschutzansatzes*. Baden-Baden: Nomos Verlagsgesellschaft, 1991; zuletzt Maximilian von Grafenstein. *The Principle of Purpose Limitation in Data Protection Laws – The Risk-based Approach, Principles, and Private Standards as Elements for Regulating Innovation*. Baden-Baden: Nomos, 2018.

[6] Steinmüller u. a., *Grundfragen des Datenschutzes*, S. 44.

[7] Historisch lauteten die breit diskutierten Alternativen, entweder nur „private“ oder „sensitive“ Informationen als schützenswert zu betrachten oder alle personenbezogenen Informationen. Die umfassendere Konzeption hat sich durchgesetzt, musste sich aber nie als solche rechtfertigen, vgl. Jörg Pohle. „PERSONAL DATA NOT FOUND: Personenbezogene Entscheidungen als überfällige Neuausrichtung im Datenschutz“. In: *Datenschutz Nachrichten* 39.1 (2016), S. 14–19, S. 15 f. Gegen den Ausschluss von anonymisierten Daten sprach sich allerdings schon früh Walter Schmidt. „Die bedrohte Entscheidungsfreiheit“. In: *Juristenzeitung* 28.8 (1974), S. 241–250, S. 241 aus. Zu den Desideraten der Debatte siehe auch umfassend Jörg Pohle. „Datenschutz und Technikgestaltung: Geschichte und Theorie des Datenschutzes aus informatischer Sicht und Folgerungen für die Technikgestaltung“. Diss. Mathematisch-Naturwissenschaftliche Fakultät, Humboldt-Universität zu Berlin, 2018. DOI: 10.18452/19136. URL: https://edoc.hu-berlin.de/handle/18452/19886, S. 170 ff.

[8] So explizit Article 29 Data Protection Working Party, *Opinion 05/2014 on Anonymisation Techniques*, S. 10 f.; sowie *Hansen* in Simitis / Hornung / Spieker, *Datenschutzrecht*, Artikel 4 Nr. 5, Rn. 24.

ist, wenn der Angreifer die oder den Grundrechtsbetroffene:n vor dem oder zum Zeitpunkt des Grundrechtseingriffs identifizieren kann. Diese absolute Ausnahmestellung unter allen Grundrechten ist bisher in der Rechtswissenschaft vollständig unbeachtet geblieben.

Soweit das konkret gewählte Anonymisierungsverfahren hinreichend dafür ist, dass der Output nicht als personenbezogene Daten gilt,[9] wird mit seiner Anwendung der Anwendungsbereich der DSGVO verlassen. Anonymisierung ist insoweit, wie auch die Löschung und die Vernichtung, eine legale Möglichkeit zur *Flucht aus dem Datenschutzrecht*. Und gerade diese Möglichkeit zur Flucht aus der DSGVO ist es, die inzwischen immer mehr öffentliche, mehr allerdings noch private Stellen dazu treibt, Forschung und Entwicklung im Bereich der Anonymisierungsverfahren durchzuführen oder zu unterstützen – darunter gerade auch solche *global players*, denen der Schutz ihrer Nutzerinnen und Nutzer sonst explizit gleichgültig ist.[10]

Der Zweck der Anonymisierung ist kategorial von dem Zweck zu trennen, der mit der weiteren Verarbeitung der anonymisierten Daten verfolgt wird. Bei der Anonymisierung handelt es sich um eine Einzweckverarbeitung, die primär den Interessen der Verantwortlichen dient und nicht zuletzt deshalb unter Bedingungen gestellt werden muss.[11]

2.2 Entpflichtung vom Schutz der Grundrechte und Grundfreiheiten der Betroffenen sowie von der Wahrung der Betroffenenrechte

Während öffentliche Stellen auch bei der Verarbeitung nicht-personenbezogener Daten an die Grundrechte gebunden sind (Artikel 1 Abs. 3 GG),[12] beschränkt sich die Pflicht privater Stellen, die Grundrechte und Grundfreiheiten natürlicher Personen zu schützen, auf Informationsverarbeitungen im Anwendungsbereich der DSGVO. Zwar mögen andere Grundrechte einschlägig sein, aber Private sind grundsätzlich nicht unmittelbar an Grundrechte gebunden.[13]

[9] Siehe umfassend zum Problem, ob, inwieweit und unter welchen Bedingungen eine *technische* Anonymisierung eine Anonymisierung *im Sinne des Rechts* darstellt, Hölzel, „Anonymisierungstechniken und das Datenschutzrecht“.

[10] Vgl. Mark Zuckerbergs Bezeichnung der Facebook-Nutzer:innen als „Dumb fucks“, Nicholas Carlson, „Well, These New Zuckerberg IMs Won't Help Facebook's Privacy Problems“, *Business Insider*, 13. Mai 2010.

[11] Vgl. Jörg Pohle. „Zur Zeitdimension der Schutzziele“. In: *Datenschutz und Datensicherheit* 42.1 (2018), S. 19–22, S. 22.

[12] Vgl. die Ausführungen des BVerfG im Mikrozensus-Urteil, wonach es mit der Menschenwürde nicht zu vereinbaren sei, als Mensch vom Staat zwangsweise in seiner oder ihrer ganzen Persönlichkeit registriert und katalogisiert zu werden, „sei es auch in der Anonymität einer statistischen Erhebung“, BVerfGE 27, 1, 6.

[13] Deshalb geht der bei Aufsichtsbehörden wie in der Literatur beliebte Verweis auf Artikel 7 GRCh zur „Achtung des Privat- und Familienlebens“ fehl, vgl. etwa Article 29 Data Protection Working Party, *Opinion 05/2014 on Anonymisation Techniques*, S. 11; oder *Hansen* in Simitis / Hornung / Spieker, *Datenschutzrecht*, Artikel 4 Nr. 5, Rn. 24.

Die mit der Anonymisierung einhergehende Entpflichtung der Verarbeiter vom Schutz der Grundrechte und Grundfreiheiten der Betroffenen betrifft sowohl die Verantwortung des für die Verarbeitung Verantwortlichen nach Artikel 24 DSGVO als auch den Datenschutz durch Technikgestaltung nach Artikel 25 DSGVO, die die Umsetzung geeigneter technischer und organisatorischer Maßnahmen fordern, um die Rechte der betroffenen Personen zu schützen. Auch von der Wahrung der DSGVO statuierten Betroffenenrechte, deren Funktion die effektive Kontrolle der sie betreffenden personenbezogenen Daten und ihrer Verarbeitung durch die Betroffenen ist, werden die Verantworlichen durch die Anonymisierung entpflichtet.

Im Zuge einer Anonymisierung wird der konkrete Grundrechtsschutz, den die DSGVO verlangt, aber eben auch nur innerhalb ihres Anwendungsbereiches erzwingen kann, und der sich auf alle Grund- und Freiheitsrechte erstreckt, zugunsten eines vagen Versprechens aufgegeben, dass sich aus dem Wegfall des Personenbezugs der verarbeiteten Daten eine Verringerung oder gar ein Ausschluss von Grundrechtsrisiken ergebe. Nicht nur gibt es in der wissenschaftlichen Forschung für die Begründetheit dieser Annahme bislang – von sehr speziellen Situationen mit besonderen Akteurskonstellationen und -interessen abgesehen – keinerlei Nachweise, die Diskussionen innerhalb der Wissenschaft, aber auch in der Öffentlichkeit etwa zu „Algorithmen“, „algorithmischen Entscheidungssystemen“ oder der Modellbildung bzw. Modellgenerierung im Bereich des maschinellen Lernens zeigen, dass es „unerwünschte Folgen von Informationsverarbeitung“ für Individuen, Gruppen und die Gesellschaft unabhängig von der konkreten Input-Klasse „personenbezogene Daten“ geben kann.[14]

3 Datenschutz-Folgenabschätzung

Vor dem Hintergrund der zuvor beschriebenen Auswirkungen der Anonymisierung mit dem Verlust der Garantie des Schutzes der Grundrechte und Grundfreiheiten sowie aller Betroffenenrechte nach der DSGVO ist vor einer Anonymisierung notwendig eine Datenschutz-Folgenabschätzung (DSFA) nach Artikel 35 DSGVO durchzuführen.

Bezugspunkt dieser DSFA sind die Risiken für Grundrechte und Grundfreiheiten, die durch die Verarbeitung der anonymisierten Daten entstehen, deren Realisierung in einer DSGVO-konformen, d. h. grundrechtsschützenden Verarbeitung gerade hätte verhindert oder zumindest weitgehend entschärft werden müssen und können, zu

[14] So betrachten etwa Article 29 Data Protection Working Party, *Opinion 05/2014 on Anonymisation Techniques*, S. 11; und *Hansen* in Simitis / Hornung / Spieker, *Datenschutzrecht*, Artikel 4 Nr. 5, Rn. 24 mögliche Auswirkungen der Verarbeitung anonymer Daten, nicht aber Auswirkungen der Anonymisierung.

deren Verhinderung bzw. Entschärfung die Verarbeiter nach der Durchführung der Anonymisierung jedoch nicht mehr verpflichtet sind.[15]

Aus dem Zweck der Anonymisierung, der Entpflichtung der Verantwortlichen von effektivem Schutz der Grundrechte und Grundfreiheiten sowie der Betroffenenrechte folgt aus jeder Anonymisierung ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen gem. Artikel 35 Abs. 1 DSGVO, denn „die betroffenen Personen [werden] um ihre Rechte und Freiheiten gebracht“ und „daran gehindert [...], die sie betreffenden personenbezogenen Daten zu kontrollieren“ (Erwägungsgrund 75).[16]

[15] Der Sache handelt es sich also um eine Pflicht zur Verhinderung der Umgehung des von der Verordnung postulierten Schutzzwecks. Zu einer verwandten Intention des Verordnungsgebers siehe Erwägungsgrund 15 des DSGVO.

[16] Die Beschränkung der Pflicht zur Durchführung einer DSFA auf Fälle, in denen es sich um eine „Anonymisierung von besonderen personenbezogenen Daten nach Artikel 9 DS-GVO nicht nur in Einzelfällen (in Bezug auf die Zahl der betroffenen Personen und die Angaben je betroffener Person) zum Zweck der Übermittlung an Dritte“ handelt, wie sie die DSK in ihrer Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist, Version 1.1 vom 17.10.2018, Nr. 15, vornimmt, greift demnach zu kurz. Sie ist weder im Hinblick auf die „besonderen personenbezogenen Daten“ begründet oder begründbar noch im Hinblick auf die „Übermittlung an Dritte“.