verbraucherzentrale
Bundesverband

# ANONYMISIERUNG UNTER DER DSGVO

Stellungnahme des vzbv zur Konsultation des BfDI

20. März 2020


**Impressum**

*Verbraucherzentrale*
*Bundesverband e.V.*

*Team*
*Digitales und Medien*

*Rudi-Dutschke-Straße 17*
*10969 Berlin*

*digitales@vzbv.de*

Bundesverband der Verbraucherzentralen und Verbraucherverbände

Verbraucherzentrale Bundesverband e.V.

# I. EINLEITUNG

Die Bestrebungen des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI), für weitere Klarheit im Kontext der Anonymisierung von personenbezogenen Daten zu sorgen, kommt aus Sicht des Verbraucherzentrale Bundesverbands e.V. (vzbv) zum richtigen Zeitpunkt. Zwar ist das Konzept der Anonymisierung im Bereich des Datenschutzes bereits seit vielen Jahren etabliert, es erhält aber derzeit besonders durch verschiedene gesetzgeberische Initiativen, den Austausch von Daten zu erleichtern, weiteren Aufwind. Beispielhaft seien hier die Datenstrategien der Europäischen Kommission sowie der deutschen Bundesregierung genannt, in denen die Anonymisierung eine wesentliche Rolle einnehmen muss.

Eine technisch einwandfreie Anonymisierung stellt jedoch im Big Data Kontext eine anspruchsvolle Herausforderung dar, insbesondere wenn die Daten über einen unbestimmten Zeithorizont mit unbestimmten Empfängern geteilt oder gar veröffentlicht werden sollen und somit aus verschiedenen Quellen zusammengeführt werden können. Daher sind aus Sicht des vzbv zum einen klare Anforderungen an die Anonymisierung erforderlich, zum anderen bedarf es weiterführender Schutzkonzepte, die das Risiko einer De-Anonymisierung verringern.

# II. POSITIONEN DES VZBV ZU DEN FRAGEN DES BFDI

### 1. ANONYMISIERUNG ALS VERARBEITUNG

Der vzbv teilt die Einschätzung des BfDI, dass es sich bei der Anonymisierung von personenbezogenen Daten um eine Verarbeitung handelt, die den Anforderungen der Datenschutz-Grundverordnung unterliegt.

So ist der Verarbeitungsbegriff der Datenschutz-Grundverordnung weit zu verstehen und schließt beispielsweise auch die Löschung von Daten ein. Im Vergleich zur Löschung ist die Anonymisierung von personenbezogenen Daten jedoch für die Betroffenen mit einem höheren Risiko behaftet. Zum einen stellt die Anonymisierung von personenbezogenen Daten eine große Herausforderung dar, bei der – wie die Vergangenheit gezeigt hat – eine Fehleranfälligkeit besteht, die eine mögliche Fehleranfälligkeit der Löschung übersteigt (höhere Schadenseintrittswahrscheinlichkeit). Hinzu kommt, dass durch eine Anonymisierung zumeist die Zweckbindung der vormals personenbezogenen Daten aufgehoben wird, wodurch die potenzielle Schadenshöhe für die Betroffenen steigt.

Vor diesem Hintergrund ist es nach Ansicht des vzbv angemessen, auch die Anonymisierung als eine Verarbeitung zu betrachten, die eine Rechtsgrundlage nach Artikel 6 DSGVO erfordert.

### 2. MÖGLICHE RECHTSGRUNDLAGEN FÜR DIE ANONYMISIERUNG

Der vzbv stimmt dem BfDI zu, dass prinzipiell jeder der in Artikel 6 DSGVO genannten Erlaubnistatbestände als Rechtsgrundlage für die Anonymisierung in Betracht kommen

kann. Insbesondere begrüßt der vzbv die Ausführungen des BfDI zu Artikel 6 Absatz 4 DSGVO in Verbindung mit der ursprünglichen Rechtsgrundlage („Zweckänderung“), die stark auf die Besonderheiten des Einzelfalls abzielen.

Wünschenswert wäre jedoch noch eine ähnliche Einschätzung des BfDI darüber, unter welchen Umständen die Rechtsgrundlage der Interessenabwägung für die Anonymisierung herangezogen werden kann. Denn auch hier sieht der vzbv eine deutliche praktische Relevanz – vor allem da oft argumentiert wird, dass eine Anonymisierung im Interesse der Betroffenen sei und daher eine Interessenabwägung stets als eine geeignete Rechtsgrundlage betrachtet werden könne.

Vor dem Hintergrund, dass es sich bei der Anonymisierung zumeist um eine Maßnahme handelt, die den Datenschutz sicherstellen soll, mag man dieser Aussage auch grundsätzlich zustimmen. Wie bei der Zweckänderung hängt jedoch die Geeignetheit auch hier von den Umständen des Einzelfalls ab. Dies bedeutet, dass auch bei dieser Abwägung die Anforderungen an eine angemessene Anonymisierung von wesentlicher Bedeutung sind (siehe unten). Weitere entsprechende Ausführungen des BfDI wären daher wünschenswert.

Darüber hinaus sollte der BfDI klarstellen, dass es unabhängig von der gewählten Rechtsgrundlage erforderlich ist, die Betroffenen entsprechend der Artikel 13 beziehungsweise Artikel 14 DSGVO über die geplante Anonymisierung zu informieren. Auch weitere Anforderungen der DSGVO, wie beispielsweise eine gegebenenfalls erforderliche Datenschutz-Folgenabschätzung, sollten im Papier des BfDI thematisiert werden.

## 3. GLEICHSETZUNG VON LÖSCHUNG UND ANONYMISIERUNG

Der vzbv erkennt an, dass nach dem Wortlaut der Datenschutz-Grundverordnung – sowie den bisherigen Entwürfen für eine europäische ePrivacy-Verordnung – grundsätzlich von einer Gleichsetzung der Löschung von Daten auf der einen Seite sowie ihrer Anonymisierung auf der anderen Seite ausgegangen werden kann. Doch obwohl auch eine Löschung von Daten nicht zwangsläufig zu ihrer endgültigen Vernichtung führt und damit weiterhin ein gewisses Risiko für die Betroffenen besteht, ist der vzbv der Ansicht, dass dieses Risiko wiederum bei einer Anonymisierung der Daten im Vergleich zu ihrer Löschung deutlich erhöht ist. Das Risiko einer De-Anonymisierung ist insbesondere gegeben, wenn die anonymisierten Daten mit weiteren Datensätzen verknüpft werden oder Dritten zugänglich gemacht werden sollen.

Auch dieses Risiko sollte dadurch minimiert werden, dass hohe Qualitätsanforderungen an die entsprechende Anonymisierung gestellt werden (siehe unten).

## 4. ANFORDERUNGEN AN DIE ANONYMISIERUNG

Der Europäische Gesetzgeber hat sich dazu entschieden, in der Datenschutz-Grundverordnung Abstand von einem absoluten Anonymisierungsbegriff zu nehmen. Daraus folgt, dass eine Anonymisierung entsprechend der Datenschutz-Grundverordnung nicht binär betrachtet werden kann, sondern dass es ein Spektrum verschiedener Anonymisierungsmaßnahmen und –techniken gibt, die eine unterschiedliche Qualität aufweisen und damit für verschiedene Zwecke unterschiedlich angemessen und geeignet sind.

Wie auch der BfDI betont, gibt die Datenschutz-Grundverordnung jedoch keine Auskunft darüber, unter welchen Umständen eine Anonymisierung als hinreichend angesehen werden kann.

Der Validität des eingesetzten Anonymisierungsverfahrens muss jedoch bei der Beurteilung der einzelnen Rechtsgrundlagen Rechnung getragen werden. So hängt es beispielsweise von den möglichen Folgen einer beabsichtigten Weiterverarbeitung für die betroffenen Personen ab, ob der neue Zweck der Anonymisierung mit dem Zweck vereinbar ist, für den die Daten ursprünglich erhoben wurden. Die möglichen Folgen ergeben sich bei der Anonymisierung jedoch auch aus der Validität des eingesetzten Verfahrens.

Bei dieser Beurteilung macht es auch einen Unterschied, ob beispielsweise eine Anonymisierung als reine unternehmensinterne Maßnahme der Datenminimierung in Fällen durchgeführt wird, in denen laut der Datenschutz-Grundverordnung auch eine Pseudonymisierung angemessen wäre oder ob auf der anderen Seite beispielsweise sensitive Daten anonymisiert werden sollen, um diese einer unbestimmten Anzahl Dritter für unbestimmte Zwecke zugänglich zu machen. Besonders hohe Anforderungen an die Qualität der Anonymisierung sind aus den oben genannten Gründen insbesondere auch in den Fällen zu stellen, in denen diese eine Löschung ersetzen soll. Aus Sicht des vzbv ist daher eine Datenschutz-Folgenabschätzung mindestens dann erforderlich, wenn sensitive Daten anonymisiert werden sollen oder wenn die Anonymisierung eine Löschung ersetzen soll.

Um Unternehmen beim Einsatz der Anonymisierung weiter zu unterstützen, sollten Kriterien oder Best Practices für die Frage entwickelt werden, welche Anonymisierungsmaßnahmen ausreichend sind, um die Risiken der Identifizierbarkeit, Aussonderung, Verkettbarkeit und Inferenz einzelner Betroffener auszuschließen. Wünschenswert wären darüber hinaus weitere Hilfestellungen für Unternehmen, welches Wissen und welche technischen Fähigkeiten bei möglichen Angreifern vorausgesetzt werden können.

# III. WEITERE SCHRITTE

Diese Erwägungen zeigen auch, dass weiterführende Schutzkonzepte diskutiert werden sollten, mit denen das Risiko einer De-Anonymisierung verringert werden kann. So sollte sich der BfDI dafür einsetzen, dass durch gesetzgeberische Vorgaben und die Entwicklung von Standards konkrete Anforderungen an die Anonymisierung sowie an die Verwendung anonymisierter Daten definiert werden.

Eine gute Orientierung über erwägenswerte Maßnahmen liefert das Gutachten der Datenethikkommission (DEK) der Bundesregierung.[1] Dementsprechend ist es notwendig:

- Rechtssicherheit zu schaffen durch die Entwicklung standardisierter Technologien und Verfahren unter laufender Berücksichtigung der technischen Entwicklungen.
- Anonymisierungsstandards zu entwickeln, einschließlich Regeln für eine gesetzliche widerlegliche Vermutung, die dem Anwender Rechtssicherheit vermitteln, nicht

[1] Vgl. Datenethikkommission der Bundesregierung: Gutachten der Datenethikkommission (2019), S. 129ff, URL: https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_DE.pdf [Zugriff: 05.03.2020]

dem Anwendungsbereich der DSGVO unterworfen zu sein – unter Einschränkungen, wie der zeitlichen Gültigkeit oder den zugelassenen Verarbeitungsformen, also, dass beispielsweise keine Veröffentlichung oder Zugänglichmachung gegenüber einer unbestimmten Zahl von Personen erfolgen darf.
- Standardisierte Prüfmethoden des Personenbezugs zu etablieren und vorzugeben.
- Strafbewehrte Verbote der De-Anonymisierung einzuführen – so gefasst, dass die Forschung zum Erkennen und Entfernen eines Personenbezugs in Datenbeständen nicht behindert wird.

Beispiele für weiterführende Schutzkonzepte lassen sich bereits im außereuropäischen Ausland betrachten. So hat beispielsweise Japan im Zuge einer umfassenden Datenschutzreform den Begriff der „anonymously processed information“ (API) eingeführt.[2] Für die Herstellung solcher Informationen gelten weitreichende Anforderungen, die eine De-Anonymisierung unmöglich machen oder zumindest wesentlich erschweren sollen. Auch nachdem die anonymisierten Daten erstellt wurden, müssen die Verantwortlichen weitere Datensicherheitsmaßnahmen ergreifen. Darüber hinaus wurde es verboten, anonymisierte Daten mit anderen Daten zusammenzuführen, um den Personenbezug wiederherzustellen sowie im Anonymisierungsverfahren entfernte, aber noch andernorts vorhandene Merkmale zu erwerben. Ferner wurden Informationspflichten gegenüber der Öffentlichkeit eingeführt, unter anderem in Bezug auf die Kategorien von Informationen, die in den anonymisierten Daten enthalten sind.

Wesentlich für solche Ansätze ist jedoch zu erkennen, dass sowohl die Anonymisierungsverfahren als solche, als auch entsprechende rechtliche Vorgaben, als fortlaufende Prozesse betrachtet werden müssen. Dementsprechend müssen auch die Verfahren und Regeln einer laufenden Aktualisierung unterliegen, um mit der künftigen technologischen Entwicklung in der Datenverarbeitung Schritt halten zu können.

[2] Vgl. Geminn, Christian; Laubach, Anne; Fujiwara, Shizuo: Schutz anonymisierter Daten im japanischen Datenschutzrecht (2018), in: ZD, S. 413–420, URL: https://beck-online.beck.de/Bcid/Y-300-Z-ZD-B-2018-S-413-N-1 [Zugriff: 12.03.2020].