STIFTUNG DATENSCHUTZ

Aus Sicht der Stiftung Datenschutz

Macht die Anonymisierung attraktiv!

Frederick Richter, LL.M.

Juristinnen und Juristinnen lieben Grundsätze aus dem antiken Römischen Recht und nutzen gern die für sie griffigen lateinischen Bezeichnungen. Ihre Methodenlehre kennt verschiedene Formen des zulässigen Argumentierens, z.B. das *argumentum e simile*, den Gleichheitsschluss, oder das *argumentum a fortiori*, den Erst-recht-Schluss. Sogar ein eher exotisch anmutendes *argumentum ad absurdum* ist anzutreffen (bei dem das untragbare Ergebnis des alternativen Weges die Richtigkeit des gewählten Weges stützen soll). Ein Schluss, der in Bezug auf die EU-Datenschutz-Grundverordnung und auf das Thema der diesmaligen Kolumne eine wichtige Rolle spielt, ist das *argumentum e contrario*, die Darlegung aus dem Gegenteil.

Ist Namenloses nicht nennenswert?

Die DSGVO findet laut Art. 2 Abs. 1 i.V.m. Art. 4 Nr. 1 Anwendung auf personenbezogene Daten. Daraus lässt sich umgekehrt schließen, dass sie auf nicht-personenbezogene Daten eben keine Anwendung findet – für die Juristenzunft einfach und klar. Angesichts der immensen praktischen Bedeutung der Abgrenzung zu anonymen Daten ist die Regelung per Umkehrschluss jedoch recht lakonisch. Denn die Beantwortung der Frage, ob Daten einen Bezug zu natürlichen Personen aufweisen oder nicht, führt zu einer wichtigen Weggabelung: Entweder es gibt einen Personenbezug, dann führt der Weg in den kompletten Anwendungsbereich des Datenschutzrechts, mit all seinen Verantwortlichkeiten, Pflichten und Dokumentationslasten. Oder der Personenbezug fehlt, dann geht es sozusagen in die regulatorische Wildnis, in der Daten vogelfrei sind (jedenfalls wenn sie nicht anderen Rechtsbereichen wie dem Datenbankrecht unterfallen). Die anonymen Daten überhaupt nicht zu erwähnen, dies wäre dem Gesetzgeber dann wohl doch zu wenig gewesen, so dass er zumindest am Ende des ErwG. 26 explizit klarstellt, was anonyme Daten sind und dass die DSGVO für anonyme Daten nicht gilt.

Zum Vorgang des Anonymisierens äußert sich das Gesetz jedoch nicht einmal am Rande. Lediglich im Landesrecht finden sich bisweilen allgemeine Definitionen.[1]

Die große Bedeutung einer solchen Handlung liegt darin, dass mit dem Entfernen des Personenbezuges der Geltungsbereich des Datenschutzrechts komplett verlassen wird. Für anonyme Datensätze eröffnen sich damit deutlich weitere Einsatzmöglichkeiten und so mitunter auch Innovationspotentiale. An dieser Stelle sei nur kurz daran erinnert, dass die DSGVO in ihrem offiziellen Gesetzesnamen auch den „freien Datenverkehr“ nennt. Es sollte also sowohl im Sinne des Verordnungsgebers als auch im Sinne des Digitalwirtschaft sein, dass der Weg des Anonymisierens eher häufiger als seltener beschritten wird; im Sinne der Bürgerrechte wäre es sowieso. Denn eine echte und robuste Anonymisierung ist die logisch weitestgehende Senkung solcher Risiken, vor denen die DSGVO die Menschen zu schützen sucht.

Frederick Richter ist ständiger Autor bei „Privacy in Germany“. Seit Anfang 2013 leitet er die in Leipzig ansässige Bundesstiftung für Privatheit und Datenschutz. *(Foto: Lorenz Becker)*

Nichtregelung schafft Unsicherheit

Wenn sich jedoch – mangels Regelung – Unsicherheiten über die zu erfüllenden Voraussetzungen für einen erfolgreichen Eintritt in den Raum der anonymen Daten

---

[1] § 3 Abs. 7 Datenschutzgesetz Nordrhein-Westfalen.

ergeben, dann kann dies im Effekt dazu führen, dass Daten nicht genutzt werden, obwohl von ihnen regelmäßig gar kein Risiko für Rechte und Freiheiten natürlicher Personen mehr ausgehen kann. Genutzt werden sollten sie aber, im Sinne des Gemeinwohls oder der Wirtschaft. In der Forschung und ebenso beim Trainieren von Systemen von künstlicher Intelligenz können auch mit Daten ohne Personenbezug signifikante Fortschritte erzielt werden.

Der Schritt zum Zustand der Bezugslosigkeit von Daten ist ein datenschutzrechtlich entscheidender Schritt. Doch beim Anonymisieren, beim Durchschreiten dieses verheißungsvollen „Tores in die Datenfreiheit" können Dinge schiefgehen. Wenn man sich den Schritt durch dieses Tor als Schritt durch einen Filter vorstellt, der sämtliche Bezugspunkte zu einer natürlichen Person herausnimmt, dann können Bezugspunkte durchrutschen, wenn der Filter fehlerhaft ist. Eine Parallelproblematik eines demgegenüber zu feinen Filters stellt sich indes nicht. Das Problem einer „zu starken" Anonymisierung wäre kein Problem des Datenschutzes, sondern eher ein ökonomisches Problem, wenn nämlich die Werthaltigkeit der Daten zu stark sinke.

Zur Durchführung einer hinreichend belastbaren Anonymisierung bestehen bislang, bedauerlicherweise, keine offiziellen Maßgaben. Es liegen keine Kurzpapiere, Entschließungen, Orientierungshilfen oder andere Anwendungshinweise vor – weder von der Konferenz der deutschen Datenschutzaufsichtsbehörden noch vom EU-Datenschutzausschuss. Dieser Mangel an Orientierung sollte behoben werden.

Wenn Leitlinien weiter ausbleiben, wären alternativ Verhaltensregeln nach Art. 40 DSGVO gut denkbar, wie sie auch zur – praktisch nicht weniger bedeutsamen – Pseudonymisierung angestrebt werden. Die beim IT-Gipfel der Bundesregierung gebildete Fokusgruppe Datenschutz, in der auch die Stiftung Datenschutz mitwirkt, hat zum Digitalgipfel 2019 einen entsprechenden Entwurf vorgelegt.[2] Ebenso wie der Pseudonymisierung kommt der Anonymisierung eine Ermöglichungsfunktion zu. Sie kann eine Verarbeitung von Daten mitunter dort erst ermöglichen, wo sie bei bestehendem Personenbezug datenschutzrechtlich schwer möglich wäre.

Wer anonymisiert, der verarbeitet (?)

Als ersten Schritt hin zu mehr Rechtssicherheit hat der Bundesdatenschutzbeauftragte nach einer Konsultation im Sommer seinen Standpunkt veröffentlicht.[3] Um den konkreten Ablauf von Anonymisierungsvorgängen ging es in diesem Prozess zwar noch nicht, die Behörde nimmt aber einige wichtige Positionierungen vor.

So schließt sich der BfDI der Sicht an, die von einem lediglich relativen Begriff der Anonymisierung ausgeht und daher lediglich eine faktische Anonymität der betroffenen Daten verlangt, nicht jedoch eine absolute, welche ihm zu Folge unmöglich sei. Es reiche danach aus, dass eine De-Anonymisierung mit verhältnismäßig kleinem Aufwand nicht zu erwarten ist.

Der BfDI ist ebenfalls der Ansicht, dass es sich beim Anonymisieren um einen Verarbeitungsvorgang im Sinne von Art. 4 Nr. 2 DSGVO handelt, welcher stets einer Rechtsgrundlage bedarf. Wer die Anonymisierung bislang bloß als technische Maßnahme zur Risikosenkung und zur Gewährleistung von – absoluter – Vertraulichkeit ansah, muss demnach umdenken.

Für diese Sicht spricht, dass die Aufzählung der möglichen Verarbeitungsvorgänge in Art. 4 DSGVO nicht abschließend ist; schließlich ist dort die Datenverarbeitung definiert als „jeder Vorgang im Zusammenhang mit personenbezogenen Daten". Vom Wortlaut her ist somit jeglicher Umgang mit personenbezogenen Daten erfasst. Weiterhin spricht für diese Auffassung, dass von fehlerhaften Anonymisierungsprozessen konkrete Risiken für die Rechte und Freiheiten der zu schützenden Personen ausgehen können, so dass bereits vom Gesetzeszweck her eine Einordnung als Verarbeitungsvorgang geboten ist.

Gegen diese Einordnung spricht historisch, dass der Verordnungsgeber den ja nicht unbedeutenden Vorgang der Anonymisierung in Art. 4 ohne Not gerade nicht aufgenommen hat – weil er vermutlich keinen Bedarf dafür sah. Praktisch betrachtet spielt das wohl keine Rolle: Im Rahmen einer Zweckänderung wäre die Anonymisierung wohl immer zulässig. Ein berechtigtes Interesse des Verantwortlichen am Anonymisieren wäre stets gegeben und ein entgegenstehendes und überwiegendes Interesse des Betroffenen wäre kaum vorstellbar. Daneben ließe sich die Anonymisierung als Ausprägung der Datenminimierungspflicht begreifen, so dass sie privilegiert und ohne Rechtsgrundlage zulässig wäre.[4] In jedem Fall wird es sehr interessant sein, die Meinungen der Aufsichtsbehörden in anderen Mitgliedstaaten zu erfahren, denn die Thematik sollte ja europaweit einheitlich gehandhabt werden.

Fortschritt braucht Orientierung

Neben der Klärung dieser Grundsatzfragen wird es darauf ankommen, in absehbarer Zeit zu einer „best practice" bei der Entfernung von Personenbezügen zu gelangen. Aufzuzeigen ist, wie auf dem Stand der Technik und in wirtschaftlicher Weise ein ausreichendes Maß an Sicherheit vor Re-Personalisierungen/De-Anonymisierungen zu gewährleisten ist.

Ein derzeit nicht mehr ganz so erfolgreicher Politiker hat vor ein paar Jahren den Ausspruch geprägt, wonach lieber nicht regiert als falsch regiert werden solle. Übertragen auf das Thema dieser Kolumne würde das heißen, dass Verantwortliche sagen: „Lieber nicht anonymisieren als falsch anonymisieren". Deshalb brauchen wir klare und gleichzeitig erfüllbare Vorgaben, die zukünftig die Nutzung des vielversprechenden Instruments der Anonymisierung attraktiv machen, damit es stattdessen heißen kann: „Lieber richtig anonymisieren als gar nicht anonymisieren".

---

[2] Entwurf für einen Code of Conduct zum Einsatz DS-GVO konformer Pseudonymisierung; abrufbar unter: www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2019/p9-code-of-conduct.pdf?__blob=publicationFile&v=2.

[3] BfDI-Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche; abrufbar unter: www.bfdi.bund.de/DE/Infothek/Transparenz/Konsultationsverfahren/01_Konsulation-Anonymisierung-TK/Positionspapier-Anonymisierung-DSGVO-TKG.html?nn=5216976.

[4] So der BITKOM in seiner Stellungnahme im erwähnten Konsultationsverfahren.