Datenschutz

Datenschutz-Folgenabschätzungen bei der Anonymisierung von Daten

Ist die Anonymisierung personenbezogener Daten rechtfertigungsbedürftig und auf welche Rechtsgrundlage stützt sich eine Anonymisierung? Ein Positionspapier des Bundesbeauftragten für Datenschutz will Orientierung geben.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) hat am 29. Juni 2020 ein Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche veröffentlicht. Es entstand nach der Durchführung des ersten öffentlichen Konsultationsverfahrens der Behörde.

Hierbei stellte sich der BfDI die Frage, ob die Anonymisierung personenbezogener Daten rechtfertigungsbedürftig ist und auf welche Rechtsgrundlage sich eine Anonymisierung stützen lässt.

Im Positionspapier wurde der aktuelle rechtliche Rahmen für die Anonymisierung aus Sicht des BfDI aufgezeigt. Das Positionspapier soll den Verantwortlichen eine Orientierung bei der datenschutzrechtlichen Bewertung ihrer Anonymisierungspraktiken bieten.

Auch wenn der BfDI nur für öffentliche Stellen des Bundes zuständig ist und seine Ansichten somit keine direkte Wirkung für nicht öffentliche Stellen haben, hat dieses Positionspapier dennoch eine starke Signalwirkung für die für den Finanzsektor zuständigen Landesbehörden.

In der Praxis besteht eine große Spannbreite an möglichen Konstellationen und Anwendungsfällen für Anonymisierungen, und das nicht erst seit Einführung der DSGVO. Rechtliche Fragen rund um eine Anonymisierung im Datenschutzrecht haben eine hohe praktische Bedeutung. Für die Neugestaltung internationaler Datentransfers in unsichere Drittländer – nach der EuGH-Entscheidung Schrems II 2 zum EU-US Privacy Shield – werden auch Anonymisierungsmöglichkeiten als Option für technische Schutzmaßnahmen diskutiert.

Würde ein Verantwortlicher personenbezogene Daten vor einer internationalen Übermittlung anonymisieren, stellten sich datenschutzrechtliche Folgethemen aus Schrems II nicht mehr.

AUTOR UND ANSPRECHPARTNER

Dennis Heinemeyer
Beauftragter Informationssicherheit & Datenschutz,
E-Mail: dennis.heinemeyer@dz-cp.de

Gesetzliche Grundlage

Die DSGVO enthält keine (dem § 3 Abs. 6 BDSG-alt vergleichbare) gesetzliche Regelung zur Anonymisierung. Die DSGVO erwähnt die Anonymisierungsthematik lediglich im Erwägungsgrund Nr. 26 sowie im Erwägungsgrund Nr. 162. Zudem gibt es einen Bezug zu Anonymisierung in Art. 89 Abs. 1 S. 4 DSGVO. Gemäß Erwägungsgrund Nr. 26 S. 5 und S. 6 ist die DSGVO nicht auf Daten anwendbar, die bereits anonym sind. Die DSGVO betreffe somit nicht die (technische) „Verarbeitung" anonymer Daten.

Im deutschen und europäischen Datenschutzrecht gilt das Prinzip des Vorbehaltes des Gesetzes. Danach ist eine Verarbeitung von personenbezogenen Daten im Grundsatz nicht zulässig, wenn diese nicht durch eine Rechtsgrundlage erlaubt ist, z. B. gemäß Art. 6 Abs. 1 S. 1 DSGVO. Wenn ein Verantwortlicher daher personenbezogene Daten verarbeiten möchte, ist eine Rechtsgrundlage erforderlich. Dies gilt nach Ansicht des BfDI aufgrund des weiten Verarbeitungsbegriffes nach Art. 4 Nr. 2 DSGVO auch für Verarbeitungen, um den jeweiligen Personenbezug aufzuheben.

Wann sind Daten anonym

Mit der Breyer-Entscheidung des EuGH ist für den Personenbezug von Daten und damit auch für deren Anonymität davon auszugehen, dass legale Mittel zu berücksichtigen sind, um (Zusatz-)Informationen durch Dritte zu erlangen. >

Anonymisierung ist auch nach Ansicht des BfDI jeder Vorgang, der darauf gerichtet ist, den Personenbezug von Daten aufzuheben. Mit anderen Worten soll mit dem Einsatz von Anonymisierungstechniken erreicht werden, dass die betroffene Person nicht mehr identifiziert werden kann.

Einige Datenschutzgesetze der Länder definieren die Anonymisierung – mit Abweichungen im Detail – als das Verändern personenbezogener Daten wie folgt: Die Einzelangaben über persönliche oder sachliche Verhältnisse können nicht mehr oder nur mit einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden.

Eine hinreichende Anonymisierung führt dazu, dass die Grundsätze des Datenschutzrechts – wie z. B. der Grundsatz der Zweckbindung – nicht mehr anwendbar sind.

Anforderungen an die Anonymisierung personenbezogener Daten

Wann eine Anonymisierung als hinreichend angesehen werden kann, darüber gibt die DSGVO, wie auch der BfDI feststellt, keine Auskunft.

Weiter stellt der BfDI fest, dass eine absolute Anonymisierung (Wiederherstellung des Personenbezugs für niemanden möglich) häufig nicht erreichbar sein dürfte und im Regelfall datenschutzrechtlich auch nicht gefordert ist. Ausreichend ist in der Regel, dass der Personenbezug derart aufgehoben wird, dass eine Re-Identifizierung praktisch nicht durchführbar ist, weil der Personenbezug nur mit einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft wiederhergestellt werden kann.

Der BfDI hebt hierbei besonders hervor, dass eine valide Anonymisierung – je nach Art der zu anonymisierenden Daten und Kontext der Verarbeitung – eine Herausforderung für den jeweiligen Verantwortlichen bedeuten kann. Er unterstreicht dabei, dass nicht vorschnell von einer hinreichenden Anonymisierung ausgegangen werden darf.

Von anonymisierten Daten abzugrenzen sind insbesondere pseudonymisierte Daten. Darunter versteht die DSGVO gemäß Art. 4 Nr. 5 „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".

Während bei den pseudonymisierten Daten der berechtigte Inhaber der zusätzlichen Informationen mittels dieser den Personenbezug wiederherstellen kann, ist die Wiederherstellung des Personenbezugs bei den anonymen Daten für jedermann zumindest praktisch unmöglich. Bei den pseudonymisierten Daten handelt es sich um personenbezogene Daten, auf die das Datenschutzrecht anwendbar ist.

Verpflichtung zur Datenschutz-Folgenabschätzung bei jeder Anonymisierung

Der BfDI stellt insbesondere heraus, dass gemäß Art. 35 Abs. 1 DSGVO eine Datenschutz-Folgenabschätzung durchzuführen ist, wenn die Verarbeitung – insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke – voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Bei einer Anonymisierung müsse demnach der Verantwortliche in der Regel davon ausgehen, dass ein hohes Risiko besteht, weil bei der Anonymisierung eben regelmäßig das Kriterium „Verarbeitung in großem Umfang" und zumindest aktuell immer noch das Kriterium „neue Technologien" zuträfen. Die Notwendigkeit der Durchführung einer Datenschutz-Folgenabschätzung sei insbesondere deshalb begründet, weil die Generierung eines anonymen Datenbestandes eine komplexe Aufgabe des Verantwortlichen darstellt und viele Fehlerquellen birgt. Dabei hat der Verantwortliche darüber hinaus die Folgen einer möglichen De-Anonymisierung in die Betrachtung einzubeziehen.

Vor einer Anonymisierung ist nach Ansicht des BfDI daher immer eine Datenschutz-Folgenabschätzung durchzuführen.

Unterstützung

Das Thema Datenschutz-Folgenabschätzung ist vielschichtig und komplex. Es erfordert Know-how im rechtlichen und technischen Sektor sowie Kenntnisse des Risikomanagements. Nutzen Sie unsere langjährige Erfahrung und unser breites Fachwissen. Gerne unterstützen wir Sie im Rahmen von Einzelprojekten oder dauerhafter Beratung und entlasten dabei Ihre internen Ressourcen. Selbstverständlich stehen wir auch in allen anderen Fragen zum Datenschutz bis hin zur Auslagerung des Datenschutzbeauftragten zur Verfügung. ▬