Datenschützer: Valide Anonymisierung als Herausforderung

Originalartikel

Backup

<html> <header class=„article-header“><h1 class=„articleheading“>Datenschützer: Valide Anonymisierung als Herausforderung</h1> Stefan Krempl </header><figure class=„aufmacherbild“><figcaption class=„akwa-caption“>(Bild: BABAROGA/Shutterstock.com)</figcaption></figure> Der Bundesdatenschutzbeauftragte Ulrich Kelber erklärt in einem Positionspapier eine „absolute Anonymisierung“ für oft nicht möglich oder nötig. „Eine absolute Anonymisierung“ in der Form, dass kein Außenstehender einen Personenbezug wiederherstellen kann, „dürfte häufig nicht möglich sein und ist im Regelfall datenschutzrechtlich auch nicht gefordert.“ Zu diesem Schluss kommt der Bundesdatenschutzbeauftragte Ulrich Kelber in einem Positionspapier. Damit fasst der oberste deutsche Datenschützer auch Stellungnahmen zusammen, die beim ersten öffentlichen Konsultationsverfahren der Behörde im Februar und März eingingen. „Trotz ihrer hohen praktischen Bedeutung ist die Anonymisierung datenschutzrechtlich nur rudimentär geregelt“, konstatiert Kelber. Besonders hervor hebt er, dass eine anzustrebende „valide Anonymisierung“ je nach „Art der zu anonymisierenden Daten und Kontext der Verarbeitung“ eine „Herausforderung für den jeweiligen Verantwortlichen bedeuten kann“. Niemand dürfe in der Praxis vorschnell „von einer hinreichenden Anonymisierung“ ausgehen. <h3 class=„subheading“ id=„nav_big_data_und0“>Big Data und die Freiheit des Einzelnen</h3> Die Menge der verfügbaren personenbezogenen Daten steige exponentiell an, führt der Sozialdemokrat in dem Papier [1] aus. Ihre Aussagekraft über das Verhalten der Menschen nehme in Wirtschaft, Wissenschaft und Forschung zu. Gerade von Big-Data-Analysen gingen aber „Risiken für die Freiheiten des Einzelnen“ aus. Das europäische Datenschutzrecht ziehe daher der „ökonomischen, politischen oder wissenschaftlichen Verwertung personenbezogener Daten Grenzen“. Für viele Forschungsprojekte und Geschäftsmodelle sei die Analyse von Datensätzen ausreichend, „deren abstrakter Gehalt erhalten bleibt, der Personenbezug jedoch aufgehoben wird“, unterstreicht Kelber. In diesen Fällen gebiete der Grundsatz der Datenminimierung im Sinne der Datenschutz-Grundverordnung (DSGVO [2]), persönliche Informationen „nur in

anonymisierter Form zu verarbeiten“. Die Anonymisierung könne ferner als ein Mittel angesehen werden, „im Einzelfall eine Verarbeitung von Daten gar erst zu ermöglichen“, wenn diese bei Personenbezug unzulässig wäre. Auch eine Pflicht, Messwerte unverzüglich zu löschen, sei durch das Instrument erfüllbar. <h3 class=„subheading“ id=„nav_aufwand_für1“>Aufwand für De-Anonymisierung</h3> Mit dem Einsatz von Anonymisierungstechniken soll dem Behördenchef zufolge erreicht werden, „dass die betroffene Person nicht mehr identifiziert werden kann“. Gelinge dies, müssten Grundsätze wie die Zweckbindung nicht mehr angewendet werden. Laut DSGVO sollten bei einer Prüfung alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren. Gerade im Big-Data-Kontext müssten so etwa erweiterte Analysefähigkeiten und damit verknüpfte Mittel zur De-Anonymisierung [3] teils schon mit abgewogen werden. Ausreichend ist es laut Kelber in der Regel, den Personenbezug derart aufzuheben, „dass eine Re-Identifizierung praktisch nicht durchführbar ist, weil der Personenbezug nur mit einem unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft wiederhergestellt werden kann“. Von anonymisierten Daten seien insbesondere pseudonymisierte abzugrenzen, bei denen der berechtigte Inhaber zusätzlicher Informationen den Personenbezug recht einfach wiederherstellen könne. Standortdaten dürfen nach dem Telekommunikationsgesetz im erforderlichen Umfang und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden, „wenn sie anonymisiert wurden oder wenn der Teilnehmer dem Anbieter des Dienstes mit Zusatznutzen“ wie einer Ortung seine Einwilligung erteilt habe, bringt der Kontrolleur ein Beispiel. Bei einer Anonymisierung müsse der Verantwortliche in der Regel davon ausgehen, „dass ein hohes Risiko besteht“, und daher im Vorfeld eine Datenschutz-Folgenabschätzung durchführen. () <hr /> URL dieses Artikels:
<small><code>https://www.heise.de/-4800149</code></small> Links in diesem Artikel:
<small><code>[1] https://www.bfdi.bund.de/DE/Infothek/Transparenz/Konsultationsverfahren/01_Konsulation-Anonymisierung-TK/Positionspapier-Anonymisierung-DSGVO-TKG.html</code></small>
<small><code>[2] https://www.heise.de/thema/DSGVO#liste</code></small>
<small><code>[3] https://www.heise.de/meldung/36C3-Wie-gaengige-Methoden-zur-Anonymisierung-von-Daten-versagen-4624450.html</code></small>
<small><code>[4] mailto:jk@ct.de</code></small>
 Copyright © 2020 Heise Medien </html>