Von: Marcus.Hild@dsb.gv.at <Marcus.Hild@dsb.gv.at>
Gesendet: Montag, 28. Mai 2018 18:12
An: Freiberger Christian <christian.freiberger@stmk.gv.at>
Betreff: DSB-D036.500/0091-DSB/2018 Antwort: Pseudonymisierung

Sehr geehrter Herr Freiberger,

Ich habe die Antworten unten eingefügt.

Für die Leiterin der Datenschutzbehörde

Mit freundlichen Grüßen,
Mag. Marcus Hild LL.M.

Datenschutzbehörde
Wickenburggasse 8
1080 Wien

"Freiberger Christian" ---03.05.2018 08:51:57---Sehr geehrter Damen und Herren, sehr geehrter Herr Mag. Hild!

Von: "Freiberger Christian" <christian.freiberger@stmk.gv.at>
An: "Datenschutzbehörde (dsb@dsb.gv.at)" <dsb@dsb.gv.at>, "Marcus Hild Mag. (marcus.hild@dsb.gv.at)" <marcus.hild@dsb.gv.at>
Datum: 03.05.2018 08:51
Betreff: Pseudonymisierung

Sehr geehrter Damen und Herren,
sehr geehrter Herr Mag. Hild!

Mit Interesse habe ich die Ausführungen der DSB zum Datenschutz-Anpassungsgesetz 2018 – Wissenschaft und Forschung – WFDSAG 2018 (DSB-D054.839/0001-DSB/2018) gelesen.
Darin findet sich folgende Passage:
„Es ist möglich, bPK für Zwecke der Pseudonymisierung zu verwenden, dabei sind aber dieselben Maßnahmen zu setzen, die bei anderen Pseudonymisierungsverfahren erforderlich sind. Da bPK des eigenen Bereichs typischerweise nicht für die Pseudonymisierung geeignet sind, weil diese ihrer Natur gemäß die eindeutige Identifizierung in diesem Bereich sicherstellen, muss ein eigens für diesen Zweck geschaffenes bPK verwendet werden. Gleiches gilt sinngemäß für die Verwendung anderer eindeutiger Identifikatoren.“

Für mich stellen sich in der Praxis folgende Fragen. Ich hoffe, die DSB (oder Sie persönlich) kann (können) mir weiterhelfen:

1. Wenn Datensätze mit bPK versehen (und die eigentlichen Personendaten entfernt) sind, können diese dann an externe Stellen weitergegeben werden (z.B. Daten aus dem Sozialbereich an die Universität zu Forschungszwecken): gelten diese Daten dann als für den Empfänger als ausreichend pseudonymisiert? Der Empfänger in einem anderen Bereich hat ja keine Möglichkeit, dieses bPK wieder herzustellen. In diesem Sinn wäre die bPK sehr hilfreich zu verwenden.

Nein, ein bPK ist grundsätzlich kein Pseudonymisierungswerkzeug, im Gegenteil, ein normales

bPK verstärkt den Personenbezug. Ausnahmen gibt es. Das bPK "amtliche Statistik" der Statistik Austria kann für Pseudonymisierungen verwendet werden.

2. Wenn in einem Bereich das bPK dieses Bereichs nicht als Pseudonym verwendet werden darf, sondern ein eigenes neues bPK als Pseudonym geschaffen werden muss: Wer legt fest, wie dieses bPK lautet? (Ist dies ein Sub-bPK des jeweiligen Bereiches? Oder kann dies ein frei gewähltes bPK sein, das es noch gar nicht gibt? Es gibt ja z.B. keinen Bereich: „Pseudonymisierung"). Würde die DSB unsere Anwendungen mit einem solchen bPK auf Aufforderung ausstatten?

Pseudonymisierung ist keine Kernaufgabe des bPK Systems. Wenn ein Gesetz das ausdrücklich vorsieht, ist es aber möglich.

3. Eine Pseudonymisierung kann helfen, Datensätze aus verschiedenen Bereichen zusammenzuführen. Dazu ist allerdings (wenn 2 Bereiche betroffen sind) ein drittes bPK erforderlich (es kann ja nicht ein bPK eines maßgeblichen Bereichs verwendet werden). Welches bPK wäre für eine solche Zusammenführung maßgeblich? Müsste nicht auch hier ein neues bPK verwendet werden, damit nicht irgendein Bezug zu einem bestehenden Bereich hergestellt werden kann? Würde die DSB ein solches bPK erstellen und damit als Pseudonymisierungsstelle fungieren?

Das bPK "amtliche Statistik" (AS) der Statistik Austria kann dies, bzw. die Statistik Austria kann das mithilfe des bPK AS.

4. Wenn die DSB eine solche Funktion nicht wahrnehmen kann/will, darf ich Sie bitten, mir mitzuteilen, welche Stelle eine solche Pseudonymisierung durchführen kann. In der Praxis zeigt sich nämlich, dass die Pseudonymisierung eine wesentliche Funktion hat, uns aber keine Stelle bekannt ist, die dies (als Geschäftsmodell) durchführt.

Eine kommerzielle Stelle ist mir nicht bekannt.

Ist es denkbar, dass das Land Steiermark selbst eine interne Pseudonymisierungsstelle einrichtet, die – unter besonderen Anforderungen, mit besonders geschulten, einer besonderen Aufsicht unterliegenden Personen, unter Umständen auch unter Überwachung durch den Datenschutzbeauftragten – Pseudonymisierungen durchführt, um Daten aus mehreren Bereichen zusammenführen zu können (verbunden wäre ja damit, dass diese Stelle zunächst die Echt-Daten sieht)? Welche Pseudonymisierungsmethode könnte dabei verwendet werden?

Wenn es dafür einen ordentlichen gesetzlichen Rahmen gibt, wäre das möglich. Die Methode sollte vom beabsichtigten Ziel/Zweck abhängig gemacht werden.

5. Welche Methode für die Pseudonymisierung ist zu verwenden, wenn Daten aus öffentlicher Quelle und privater Quelle zu Forschungs-/Auswertungszwecken verwendet werden soll? Kann hier die DSB einen Beitrag leisten? Wenn nein, wer sonst?

Die Methode der Herstellung des Pseudonyms ist nicht alleine ausschlaggebend, sondern das gesamte Paket muss eine effektive Pseudonymisierung sicherstellen. Ein sehr aufwendiges kryptographisches Verfahren bietet zum Beispiel keinerlei Schutz, wenn zuviele Daten im Sammeldatensatz eine Re-Identifizierung erlauben.

Sehr geehrte Damen und Herren, sehr geehrter Herr Mag. Hild, mir ist bewusst, dass dies ziemlich viele Fragen sind, aber es zeigt sich, dass die Theorie der Pseudonymisierung uns zwar bekannt ist, die Praxis aber nicht damit Schritt halten kann.
Jegliche Information, wie man praktisch mit der Pseudonymisierung umgeht, welche bPK für eine Pseudonymisierung geeignet sein können, welchen Beitrag die DSB leisten kann und was man allenfalls selbst durchführen kann, wäre für uns hilfreich.

Ich hoffe, Sie können sich meiner Fragen annehmen.

Mit freundlichen Grüßen
Christian Freiberger