Sehr geehrte Damen und Herren,
liebe Kolleginnen und Kollegen,

haben Sie vielen Dank für die Einladung, am öffentlichen Konsultationsprozess teilzunehmen.

Falsche Inhalte haben wir in dem Entwurf nicht gefunden.

Uns erscheint es, als befasste sich das Papier intensiver als nötig mit der Frage, wann Anonymisierung als Verarbeitungsschritt überhaupt erlaubt ist.

Dagegen wird eher am Rande erwähnt , dass Anonymisierung nicht trivial ist und welche rechtlichen (z.B. § 16 Abs. 1 S. 3 Nr. 4 im Gegensatz zu § 16 Abs. 6 Nr. 1 BStatG) und technischen Hürden zu beachten sind.

Wir befürchten daher, dass die zutreffenden Ausführungen in der Praxis (bewusst oder unbewusst) verkürzt rezipiert und unzureichend umgesetzt werden.

Unsere Empfehlungen/Hinweise:

1. Das Papier sollte die Anonymisierung von der Pseudonymisierung abgrenzen, weil Pseudonymisierung (z.B. Hashwerte) oft für Anonymisierung gehalten/ausgegeben wird, u.a. durch die Verkettbarkeit aber zusätzliche Risiken birgt (s. z.B. HK-DS-GVO, 2. Aufl. 2018, Art. 4 Rn. 90 ff. und insb. Roßnagel/Scholz, MMR 2000, 721).

2. Das Papier sollte die Unterschiede zwischen absoluter, faktischer und formaler Anonymisierung darlegen und insbesondere klarstellen, dass faktische Anonymisierung (z.B. Weglassen des Namens) oft nicht ausreicht.

3. Die technische Umsetzung einer ausreichenden Anonymisierung und häufige Fehler sollten breiten Raum einnehmen oder auf diese Themen jedenfalls deutlich verwiesen werden (z.B. Art.-29-Gruppe:WP 216, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf> oder Petrlic/Sorge, Datenschutz, 1. Aufl. 2017, S. 12 ff.).

Die Pflicht des Verantwortlichen, technische Entwicklungen, die zur De-Anonymisierung führen können, zu beobachten und ggf. nachzubessern, wird im Entwurf durchaus angedeutet („Die Überprüfung der Anonymisierung auf ihre Validität ist eine fortwährende Aufgabe des Verantwortlichen“).

Dieses Problem sollte u.E. deutlicher dargestellt werden.

4. Fachrecht kann auch zu (faktisch) anonymen Daten Regelungen treffen, so das Statistikrecht und Art. 5 Abs. 3 e-Privacy-RL 2002/58/EG.

5. Speziell für den TK-Bereich: Das Papier beschreibt in Nr. 4, alle Entwürfe einer e-Privacy-VO würden die Anonymisierung von TK-Inhalten durch den Provider als für die Löschung ausreichend erachten (so z.B. die Fassung vom 31.10.2019, Art. 7, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_13632_2019_INIT&from=DE <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_13632_2019_INIT&from=DE> oder die Fassung vom 21.2.2020, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_5979_2020_INIT&from=EN <https://eur-lex.europa.eu/legal-

content/EN/TXT/PDF/?uri=CONSIL:ST_5979_2020_INIT&from=EN> ). Das könnte auf eine ewige Speicherung/Veröffentlichung aller Nachrichteninhalte unter Streichung von Absender/Empfänger hinauslaufen. Wir halten es für wenig wahrscheinlich, dass eine mindestens faktische Anonymität von TK-Inhaltsdaten strukturell sichergestellt werden kann (man denke nur an E-Mail-Texte und Bilder oder Videos im Anhang). Entsprechend verlangt Art. 5 Abs. 1 S. 2 e-Privacy-RL bisher, dass Mitgliedstaaten vorsehen, dass Nachrichten nach Übertragung grundsätzlich nicht weiter gespeichert werden. Das Papier sollte sich u.E. zu diesen Problemfeldern und Plänen (kritisch) verhalten.

6. Hinweis „off topic“: der letztgenannte Entwurf der e-Privacy-VO sieht in Art. 7 Nr. 4 eine (Schon-) Wieder-Einführung der Vorratsdatenspeicherung von TK-Verkehrsdaten vor.

Dr. Ziebarth

Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg