Republik Österreich
Datenschutzbehörde

A-1010 Wien, Hohenstaufengasse 3
Tel.: ++43-1-53115 207310
Fax: ++43-1-53109 202690
E-Mail: dsb@dsb.gv.at
DVR: 0000027

GZ: DSB-D054.766/0001-DSB/2017 Sachbearbeiterin: Mag. Stefanie PITSCH

Präsidium des Nationalrates

Dr. Karl Renner Ring 3
1017 Wien

Stellungnahme der Datenschutzbehörde

per E-Mail: begutachtungsverfahren@parlament.gv.at

Betrifft: Stellungnahme der Datenschutzbehörde zum do. Gesetzesentwurf eines Bundesgesetzes, mit dem die Strafprozessordnung 1975 geändert wird (Strafprozessrechtsänderungsgesetz 2017)

Die Datenschutzbehörde nimmt in o.a. Angelegenheit aus Sicht Ihres Wirkungsbereiches wie folgt Stellung:

Zu § 134 Z 3 und 3a:

Unklar ist, worin der Unterschied zwischen „gesendeten“ und „übermittelten“ Nachrichten liegt. Auch § 3 Z 22 deutsches TKG (Begriffsdefinition von „Telekommunikation“: der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen), auf welchen die Erläuterungen auf S. 5 Bezug nehmen, bringt keine Klärung dieser Begriffe. Eine Klarstellung im Gesetzesentwurf wird angeregt.

Zu § 134 Z 3a:

Die Bestimmung sieht vor, dass neben den verschlüsselt gesendeten, übermittelten und empfangenen Nachrichten „damit im Zusammenhang stehende(r) Daten im Sinn des § 76a und des § 92 Abs. 3 Z 4 und 4a TKG“, also Stamm-, Verkehrs- und Zugangsdaten (§ 92 Abs. 3 TKG 2003), ermittelt werden sollen. Dies wird jedoch in den Erläuterungen nicht in dieser Klarheit zum Ausdruck gebracht und es wird angeregt in den Materialien klarzustellen, dass sich die Überwachung im Sinne des § 134 Z 3a auch auf Daten bezieht, die weder gesendet, übermittelt oder empfangen werden.

Mit diesem Programm soll - so die Erläuterungen auf Seite 7 und 9 - keine Online-Durchsuchung erfolgen, das heißt, es sollen insbesondere keine lokal abgespeicherten, mit einem Übertragungsvorgang nicht in Zusammenhang stehenden Daten (wie etwa lokale Adressbücher oder Kontaktverzeichnisse) ermittelt werden. Da aber zum jetzigen Zeitpunkt nicht garantiert werden kann, ob es technisch möglich ist, ein solches Programm zu schaffen (siehe dazu Seite 9 der Erläuterungen: „Bedenken zur technischen Umsetzbarkeit Rechnung tragend, ist vorgesehen, ein unabhängiges Audit der Programmarchitektur durchzuführen."), das sich tatsächlich innerhalb der gesetzlichen Vorgaben bewegt und keine Online-Durchsuchung durchführt, ist zumindest das Verwendungsverbot in § 140 Abs. 1 Z 2 und 4 StPO zu begrüßen.

Zu § 134 Z 3a und § 135a:

1) Auf Seite 9 unten der Erläuterungen, wo auf „die Installation eines Programms in dem Computersystem" Bezug genommen wird, wird ausgeführt:

„Eine praktische Umsetzung der gesetzlichen Vorgaben (Programmierung einer Software, die nur die gesetzlich vorgesehenen Vorgänge des Sendens, Übermittelns und Empfangens überwacht) ist nach dem derzeitigen Stand der Technik möglich, **wobei die konkrete Durchführung in die Zuständigkeit des Bundesministeriums für Inneres fällt.** Bedenken zur technischen Umsetzbarkeit Rechnung tragend, ist vorgesehen, ein unabhängiges Audit der Programmarchitektur durchzuführen. Dieses soll sowohl die Beschränkung des Programms auf die gesetzlich vorgesehenen Funktionen und die Nachvollziehbarkeit der getroffenen Maßnahmen sicherstellen als auch die berechtigten Sicherheits- und Geheimhaltungsinteressen des Staates berücksichtigen. **Die Architektur des Programms wird entsprechend den Bestimmungen des DSG 2000 bei der Datenschutzbehörde anzumelden sein**."

Die „Überwachung verschlüsselter Nachrichten"(§ 134 Z 3a) soll gemäß § 135 a des vorliegenden Entwurfs mit 1. August 2019 in Kraft treten (siehe dazu § 514 Abs. 36 zweiter Satz des vorliegenden Entwurfs). Wenn nun die Erläuterungen davon sprechen, dass „die Architektur des Programms (…) entsprechend den Bestimmungen des DSG 2000 bei der Datenschutzbehörde anzumelden sein (wird)", ist darauf hinzuweisen, dass **die im Datenschutzgesetz 2000 vorgesehene Pflicht, Datenanwendungen** - hier: ein Programm zur Überwachung verschlüsselter Nachrichten - **beim Datenverarbeitungsregister der Datenschutzbehörde zu melden, ab dem 25. Mai 2018 nicht mehr existieren wird (Geltungsbeginn des Datenschutzgrundverordnung).**

Ab dem 25. Mai 2018 gilt nicht mehr das Datenschutzgesetz 2000 - DSG 2000 (mit Ausnahme der Verfassungsbestimmungen), sondern es tritt das Datenschutz-Anpassungsgesetz 2018 in Kraft, das die Verordnung (EU) 2016/679 („Datenschutz-Grundverordnung (DSGVO)") durchführt und die Richtlinie (EU) 2016/680 („Datenschutzrichtlinie-Polizei Justiz (DSRL-PJ)") umsetzt.

§ 69 Abs. 2 des Datenschutz-Anpassungsgesetzes 2018 (BGBl. I Nr. 120/2017) sieht vor, dass ab dem 25. Mai 2018 und bis zum 31. Dezember 2019 das Datenverarbeitungsregister nur mehr zu Archivzwecken fortzuführen ist. In diesem Zeitraum dürfen keine Eintragungen und inhaltlichen Änderungen im Datenverarbeitungsregister mehr vorgenommen werden.

Ab dem 25. Mai 2018 gilt vielmehr, dass Datenanwendungen nicht mehr bei der Datenschutzbehörde zu melden sind, sondern der datenschutzrechtlich Verantwortliche (in der „alten" Terminologie des DSG 2000: der datenschutzrechtliche „Auftraggeber") selbst ein „Verzeichnis von Verarbeitungstätigkeiten" führen muss (siehe dazu § 4 Datenschutz-Anpassungsgesetz 2018 iVm Art. 30 DSGVO sowie § 49 Datenschutz-Anpassungsgesetz 2018).

Der datenschutzrechtliche „Verantwortliche" eines „Programms zur Überwachung verschlüsselter Nachrichten" muss also selbst - statt einer Meldung bei der Datenschutzbehörde - ein Verzeichnis seines „Überwachungs-Programms" bzw. seiner „Überwachungs-Software" führen (siehe dazu § 49 Datenschutz-Anpassungsgesetz 2018). Darüber hinaus treffen den datenschutzrechtlichen „Verantwortlichen" eines solchen Programms zukünftig zahlreiche andere Pflichten, wie etwa § 51 (Zusammenarbeit mit der Datenschutzbehörde), § 52 (Durchführung einer Datenschutz-Folgenabschätzung) und § 53 (Vorherige Konsultation der Datenschutzbehörde) des Datenschutz-Anpassungsgesetzes 2018.

Darüber hinaus geht aus dem vorliegenden Gesetzesentwurf nicht hervor, wer der datenschutzrechtliche Verantwortliche eines solchen Programms zur „Überwachung verschlüsselter Nachrichten" sein wird. Es wird daher angeregt, dies im Gesetzestext klarzustellen, da sich dazu lediglich in den Erläuterungen der Hinweis findet, dass die „Durchführung in die Zuständigkeit des Bundesministeriums für Inneres fällt." Der Begriff Durchführung ist dem Datenschutzregime in diesem Kontext fremd und es wird angeregt festzulegen, wer datenschutzrechtlich Verantwortlicher für dieses Programm sein wird.

2) Sollte der oben wiedergegebene Passus auf S. 9 der Erläuterungen aber so zu verstehen sein, dass das Audit eines Programms zur „Überwachung verschlüsselter Nachrichten" von der Datenschutzbehörde vorgenommen werden soll, ist anzumerken, dass unklar ist, was mit „Audit" genau gemeint ist und eine etwaige Zuständigkeit der Datenschutzbehörde zum „Audit" eines solchen Programms gesetzlich vorgesehen ist. Wenn mit diesem Audit die Konsultation der DSB nach einer Datenschutzfolgeabschätzung gemeint ist, wird auf Art 36 DSGVO hingewiesen.

Die vorherige Konsultation der Datenschutzbehörde vor Einsatz eines solchen „Überwachungs-Programms" würde zudem einen nicht abschätzbaren Mehraufwand in personeller und finanzieller Hinsicht für die Behörde bedeuten, zumal - nach Einschätzung von SC Dr. Mathias Vogl (Seite 8 der Erläuterungen) - „**für jeden Fall** (der Überwachung verschlüsselter Nachrichten) eine individuelle Software er- bzw. zusammengestellt werden" müsste.

21. August 2017
Die Leiterin der Datenschutzbehörde:
JELINEK

REPUBLIK ÖSTERREICH DATENSCHUTZBEHÖRDE @ AMTSSIGNATUR	Unterzeichner	serialNumber=1119505,CN=Datenschutzbehörde,C=AT
	Datum/Zeit	2017-08-21T12:36:39+02:00
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: https://www.dsb.gv.at/-/amtssignatur
	Hinweis	Dieses Dokument wurde amtssigniert.