Republik Österreich
Datenschutzbehörde

A-1080 Wien, Wickenburggasse 8
Tel.: +43-1-52152 302551

E-Mail: dsb@dsb.gv.at
DVR: 0000027

GZ: DSB-D054.852/0001-DSB/2018 Sachbearbeiter: Dr. Matthias SCHMIDL

Österreichischer Nationalrat, Justizausschuss

Stellungnahme der Datenschutzbehörde

per E-Mail: ausschussbegutachtung.justizausschuss@parlament.gv.at

Betrifft: Stellungnahme der Datenschutzbehörde zur Regierungsvorlage eines Bundesgesetzes, mit dem die Strafprozeßordnung 1975, das Staatsanwaltschaftsgesetz und das Telekommunikationsgesetz 2003 geändert werden (Strafprozessrechtsänderungsgesetz 2018) (17 der Beilagen)

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

1. Allgemeines

Die Datenschutzbehörde hat bereits zum Ministerialentwurf eines Strafprozessrechtsänderungsgesetzes 2017 (325/ME XXV. GP) Stellung genommen, weshalb – um Wiederholungen zu vermeiden – auf diese Stellungnahme verwiesen wird, soweit die vorliegende Regierungsvorlage Bestimmungen des Ministerialentwurfes übernimmt.

Aus Sicht der Datenschutzbehörde unterliegen die staatlich angeordnete, begrenzte Speicherung bestimmter Kommunikationsdaten zum Zweck der Strafverfolgung sowie die Überwachung verschlüsselter Nachrichten zur Gänze den Bestimmungen des 3. Hauptstückes des Datenschutzgesetzes – DSG, BGBl. I Nr. 165/1999 idF BGBl. I Nr. 120/2017. Darüber hinaus unterliegt die „Anlassdatenspeicherung“ – wie sich aus dem Urteil des EuGH vom 21. Dezember 2016, C-203/15 und C-698/15 ergibt – dem Unionsrecht.

2. Zu Art. 1 (Änderung der Strafprozeßordnung 1975):

Zu § 134:

Z 2b definiert „Anlassdatenspeicherung“ als „das Absehen von der Löschung der in Z 2 genannten Daten (§ 99 Abs. 2 Z 4 TKG).“

Nach der Systematik des Entwurfs stellt die „Anlassdatenspeicherung“ das zeitlich begrenzte Absehen einer Löschung aufgrund einer Anordnung einer Staatsanwaltschaft dar. Diese Intention kommt nach Ansicht der Datenschutzbehörde in der gewählten Definition nicht hinreichend klar zum Ausdruck, weshalb angeregt wird, die Definition zu überprüfen.

In Bezug auf Z 3 und 3a wird auf die Stellungnahme der Datenschutzbehörde zum Ministerialentwurf eines Strafprozessrechtsänderungsgesetzes 2017 verwiesen.

Zu § 135:

Abs. 2b normiert, unter welchen Voraussetzungen eine Anlassdatenspeicherung zulässig ist.

Nach der einschlägigen Rechtsprechung des EuGH im Urteil vom 21. Dezember 2016 ist die Anordnung der gezielten und begrenzten Speicherung von Verkehrs- und Standortdaten nur zur Bekämpfung schwerer Straftaten bzw. schwerer Kriminalität zulässig (vgl. dazu die Rz. 108 ff, insbesondere Rz. 111, des genannten Urteils).

Durch den Verweis auf § 135 Abs. 2 Z 2 bis 4 ist zwar klargestellt, dass eine Anlassdatenspeicherung nicht zur Bekämpfung jedweder Straftat zulässig ist; dies gilt jedoch nicht soweit auf § 76a Abs. 2 verwiesen wird. Eine Einschränkung auf schwere Straftaten, wie sie bspw. § 135a Abs. 1 Z 3 des vorliegenden Entwurfes vorsieht, ist der Regierungsvorlage nicht zu entnehmen. Auch das vom EuGH in Rz. 111 des genannten Urteils angeführte geographische Kriterium findet sich in der Regierungsvorlage nicht.

Es wird daher angeregt, Abs. 2b im Lichte der Judikatur des EuGH einer nochmaligen Prüfung zu unterziehen.

Zu § 135a:

Ein Vergleich mit dem Ministerialentwurf des Jahres 2017 erhellt, dass die Überwachung verschlüsselter Nachrichten auf zusätzliche Straftaten, nämlich solche gegen Leib und Leben oder die sexuelle Integrität und Selbstbestimmung, ausgeweitet werden soll. Eine Begründung hiefür ist den Erläuterungen nicht zu entnehmen. Da mit dieser Ausweitung ein erweiterter Eingriff in das Grundrecht auf Datenschutz nach § 1 DSG (2000) normiert wird, wäre in Hinblick auf § 1 Abs. 2 letzter Satz leg. cit. eine genauere Begründung erforderlich.

Der Entwurf lässt es offen, ob eine Installation der erforderlichen Software auch mittels Fernzugriff möglich ist. Den Erläuterungen zufolge wird dies offenbar in der Praxis als erforderliche Maßnahme angesehen

(siehe dazu S 9). Es wird daher angeregt, dies im Gesetzestext klarzustellen und – sollte von dieser Möglichkeit Gebrauch gemacht werden – flankierende Sicherheitsmaßnahmen im Sinne des § 54 DSG vorzusehen.

Nach den Erläuterungen ist vorgesehen, dass das Bundesministerium für Inneres datenschutzrechtlich Verantwortlicher der Überwachungssoftware iSd § 36 Abs. 2 Z 8 DSG sein soll und zur Zusammenarbeit mit der Datenschutzbehörde verpflichtet ist. Eine Zusammenarbeitspflicht mit der Datenschutzbehörde, außerhalb eines konkreten Verfahrens, kann sich nur im Zusammenhang mit der Durchführung einer Datenschutz-Folgenabschätzung nach §§ 52 und 53 DSG ergeben, weshalb angeregt wird, dies in den Erläuterungen klarzustellen. Unklar ist, was mit der Ausführung *„[Das Bundesministerium für Inneres wird als datenschutzrechtlich Verantwortlicher] für das Überwachungsprogramm ein Verzeichnis von Verarbeitungstätigkeiten führen*“ gemeint ist. Datenverarbeitung im Rahmen eines solchen Programmes sind nach Ansicht der Datenschutzbehörde in das allgemeine Verzeichnis der Verarbeitungstätigkeiten des Verantwortlichen gemäß § 49 DSG aufzunehmen.

Ob das Bundesministerium für Inneres beim angeordneten Einsatz dieser Software tatsächlich als datenschutzrechtlicher Verantwortlicher angesehen werden kann, ist aber fraglich, weil die Überwachung verschlüsselter Nachrichten nur aufgrund einer gerichtlichen Bewilligung anzuordnen ist (§ 137 Abs. 1 der Regierungsvorlage) und das Bundesministerium für Inneres dann unter der Aufsicht und Anleitung gerichtlicher Organe agiert. Die datenschutzrechtliche Verantwortung läge dann nach Ansicht der Datenschutzbehörde nicht mehr beim Bundesministerium für Inneres.

Zu § 137:

Gemäß Abs. 1 ist die Anlassdatenspeicherung nach § 135 Abs. 2b von der Staatsanwaltschaft anzuordnen.

Den Erläuterungen (S 7) zufolge kann „*die Staatsanwaltschaft wie bereits derzeit nach § 135 Abs. 2 StPO oder § 76a Abs. 2 StPO auf solcherart nicht gelöschte Daten zugreifen, weil es keinen Unterschied macht, ob – wie bisher – auf übliche historische Verrechnungsdaten oder die inhaltlich selben, Quick-Freeze‘-Daten zugegriffen wird*.“

Der EuGH hat im genannten Urteil in Rz. 120 ausdrücklich ausgeführt, dass es „*unabdingbar [ist], dass der Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten grundsätzlich – außer in hinreichend begründeten Eilfällen – einer vorherigen Kontrolle entweder durch ein Gericht oder eine unabhängige Verwaltungsstelle unterworfen wird und deren Entscheidung auf einen mit Gründen versehenen Antrag ergeht, der von den zuständigen nationalen Behörden u. a. im Rahmen von Verfahren zur Verhütung, Feststellung oder Verfolgung von Straftaten gestellt wird*.“

Zwar wird ebenfalls in den Erläuterungen (S 6 und 7) ausgeführt, dass „der Zugriff auf die gespeicherten Daten […] einer gerichtlichen Bewilligung [bedarf]“, jedoch kommt diese Unterscheidung – Anordnung der Anlassdatenspeicherung einerseits, Zugriff auf die gespeicherten Daten andererseits – in der Regierungsvorlage nach Ansicht der Datenschutzbehörde nicht ausreichend klar zum Ausdruck. Es entsteht vielmehr der Eindruck, dass die Staatsanwaltschaft bereits aufgrund ihrer Anordnung auf die gespeicherten Daten zugreifen darf, was jedoch der oben zitierten Rechtsprechung nicht entspräche.

Zu § 138:

Ein Vergleich mit dem Ministerialentwurf des Jahres 2017 sowie die Ausführungen in Z 1 und 2 legen nahe, dass in Abs. 1 offenbar ein Verweis auf § 135a unterblieben ist.

Zu § 147:

Abs. 1 Z 5 nimmt die Anordnung einer Anlassdatenspeicherung als einzige Ermittlungsmaßnahme von der Prüfung und Kontrolle durch den Rechtsschutzbeauftragten aus. Eine Begründung hiefür ist nicht ersichtlich. Angesichts der vom EuGH festgestellten Schwere eines derartigen Eingriffes erscheint jedoch eine entsprechende Kontrollbefugnis geboten.

15. März 2018
Die Leiterin der Datenschutzbehörde:
JELINEK

REPUBLIK ÖSTERREICH DATENSCHUTZBEHÖRDE @ AMTSSIGNATUR	Unterzeichner	serialNumber=1119505,CN=Datenschutzbehörde,C=AT
	Datum/Zeit	2018-03-15T13:24:04+01:00
	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.