REPUBLIK ÖSTERREICH DATENSCHUTZRAT

Museumstraße 7, A-1070 WIEN
BMVRDJ-817.483/0004-DSR/2018
TELEFON ● (+43 1) 52152/2906
E-MAIL ● DSR@BMVRDJ.GV.AT

An das
Präsidium des Nationalrates
Parlament

An die
Mitglieder des Justiz- und
Innenausschusses des Nationalrates

Per E-Mail:

begutachtungsverfahren@parlament.gv.at

Ausschussbegutachtung.Justizausschuss@parlament.gv.at

Stellungnahmen.Innenausschuss@parlament.gv.at

Ausschussbegutachtung gem. § 40 Abs. 1 GOG betreffend die Regierungsvorlagen zum Entwurf eines Bundesgesetzes, mit dem das Sicherheitspolizeigesetz, die Straßenverkehrsordnung 1960 und das Telekommunikationsgesetz 2003 geändert werden und zum Entwurf eines Bundesgesetzes, mit dem die Strafprozeßordnung 1975, das Staatsanwaltschaftsgesetz und das Telekommunikationsgesetz 2003 geändert werden (Strafprozessrechtsänderungsgesetz 2018)

Der **Datenschutzrat** hat in seiner **237. Sitzung am 9. März 2018 einstimmig** die Einsetzung eines **Arbeitsausschusses** des Datenschutzrates gemäß § 7 der Geschäftsordnung des Datenschutzrates beschlossen und diesen ermächtigt, eine **Stellungnahme** zu den im Betreff genannten Vorhaben **auszuarbeiten und abzugeben**.

Mit Schreiben vom 23. Februar 2018 stellten die Mitglieder des Datenschutzrates Stv. Klubdirektor PR Dr. Peter POINTNER (SPÖ) und KS Christian SCHIESSER (SPÖ) den **Antrag** auf Einberufung einer Sondersitzung des Datenschutzrates gemäß § 44 Abs. 1 DSG 2000 zur „Beratung über das Überwachungspaket bestehend aus dem Bundesgesetz,

mit dem das Sicherheitspolizeigesetz, die Straßenverkehrsordnung 1960 und das Telekommunikationsgesetz 2003 geändert werden und dem Bundesgesetz, mit dem die Strafprozeßordnung 1975, das Staatsanwaltschaftsgesetz und das Telekommunikationsgesetz 2003 geändert werden (Strafprozessrechtsänderungsgesetz 2018).“ In der 237. Sitzung des Datenschutzrates am 9. März 2018 wurde eine Generaldebatte zu diesem Thema mit informierten Vertretern des Bundesministeriums für Verfassung, Reformen, Deregulierung und Justiz und des Bundesministeriums für Inneres abgeführt.

Weiters wurde in der Sitzung des Datenschutzrates am 9. März 2018 der Beschluss gefasst, unter Leitung des Verfassungsdienstes einen nicht ständigen Arbeitsausschuss zur weiteren Behandlung dieses Themas einzusetzen.

Es wurden zu diesem Thema am 2. März 2018 und am 23. März 2018 **zwei Sitzungen** des Arbeitsausschusses abgehalten.

Der Arbeitsausschuss setzte sich aus folgenden Mitgliedern zusammen: (Vorsitz) SC Dr. Gerhard HESSE (BUND), Abg.z.NR Werner HERBERT (FPÖ), Stv. Klubdirektor PR Dr. Peter POINTNER (SPÖ), Mag. Ulrich JEDLICZKA (ÖVP) und Mag. Clemens Maria SAMPL (LISTE PILZ). Für die Geschäftsstelle des Datenschutzrates haben MR Dr. Eckhard RIEDL und MR Mag. Birgit Hrovat-Wesener an den Sitzungen teilgenommen.

Der Arbeitsausschuss hat **einstimmig** die nachstehende Stellungnahme beschlossen.

Der Arbeitsausschuss des Datenschutzrates gibt zu den beiden gegenständlichen Vorhaben einstimmig folgende Stellungnahme ab:

Zur RV betreffend ein Bundesgesetz, mit dem das Sicherheitspolizeigesetz, die Straßenverkehrsordnung 1960 und das Telekommunikationsgesetz 2003 geändert werden (15 Blg NR XXVI. GP)

Zu § 53 Abs. 5 SPG:

Nach dem vorgeschlagenen Gesetzestext sollen Rechtsträger des privaten Bereichs, „sofern letzteren ein öffentlicher Versorgungsauftrag zukommt“, bestimmten – in dieser Bestimmung näher umschriebenen – Verpflichtungen unterliegen. Es sollte im Gesetzestext klarer dargelegt werden, was unter dem Begriff „öffentlicher Versorgungsauftrag“ zu verstehen ist.

Darüber hinaus sind nach dieser Bestimmung im Einzelfall die genannten Rechtsträger verpflichtet, Aufnahmen „für die Zwecke der Vorbeugung wahrscheinlicher oder Abwehr gefährlicher Angriffe“ den Sicherheitsbehörden zu übergeben.

Vor dem Hintergrund des Datenschutzgrundrechtes (§ 1 DSG) und der Betroffenheit von Personen, die nicht unmittelbar in die betroffenen sicherheitspolizeilichen Vorkommnisse involviert sind, sollte der Begriff „wahrscheinlicher“ näher determiniert werden. Der Begriff scheint zu allgemein als Schwelle für den Grundrechtseingriff gewählt. Es sollte überlegt werden, ob mit der im geltenden Recht vorgesehenen Formulierung „wenn bestimmte Tatsachen auf eine schwere Gefahr für die öffentliche Sicherheit schließen lassen“ nicht das Auslangen gefunden werden könnte.

Zu § 53 Abs. 5 erster Satz wird festgehalten, dass die verarbeiteten Bild- und Tondaten „rechtmäßig“ verarbeitet sein müssen. Dies bedeutet, dass sie grundsätzlich nach den Bestimmungen der §§ 50a ff DSG 2000 zulässig sein müssen.

Darüber hinaus sollte klargestellt werden, auf welcher Rechtsgrundlage Tonaufzeichnungen erfolgen können, zumal §§ 50a ff DSG 2000 derartige Aufzeichnungen nicht vorsehen. Die Erläuterungen gehen offenkundig von einem anderen Verständnis aus. Dies sollte klargestellt werden.

Zu § 53a Abs. 6 SPG:

In Bezug auf personenbezogene Daten von Verdächtigen soll mit dieser Vorschrift die maximale Speicherdauer von drei auf fünf Jahre verlängert werden. In den Erläuterungen wird dies mit Ermittlungen im Bereich der organisierten Kriminalität begründet. Es sollte überlegt werden, ob die verlängerte Speicherdauer nicht auf Ermittlungen in Bezug auf

organisierte Kriminalität sowie allenfalls vergleichbare Vergehen mit einem ähnlichen Unrechtsgehalt beschränkt werden könnte.

Zu § 54 Abs. 4b SPG in Verbindung mit § 98a Abs. 2 StVO 1960:

Vor dem Hintergrund des Erkenntnisses des Verfassungsgerichtshofes VfSlg 18.146/2007 wird festgehalten, dass der Verfassungsgerichtshof die Section-Control deshalb für zulässig erachtet hat, weil einerseits die Datenverarbeitung einer strengen Zweckbindung unterliegt („Feststellung der Überschreitung einer ziffernmäßigen Höchstgeschwindigkeit“) sowie andererseits die Löschung aller anderen Daten vorgesehen ist.

In den Erläuterungen finden sich zu diesem Erkenntnis und insbesondere zum Grundsatz der Verhältnismäßigkeit keine Ausführungen. Ebenso sollte die Erforderlichkeit der Aufbewahrungsfrist von 14 Tagen, die in den Erläuterungen mit der Notwendigkeit der Strafverfolgung begründet und die grundsätzlich nicht in Zweifel gezogen wird, näher erläutert werden.

Zu § 97 Abs. 1a TKG 2003:

Angesichts der durch die Bestimmung bewirkten eingeschränkten Möglichkeit des Erwerbs eines Kommunikationsmittels sollte das Identifizierungsverfahren nicht weitgehend an eine Verordnung delegiert werden, sondern möglichst präzise im Gesetz selbst geregelt werden.

Zur RV betreffend den Entwurf eines Bundesgesetzes, mit dem die Strafprozeßordnung 1975, das Staatsanwaltschaftsgesetz und das Telekommunikationsgesetz 2003 geändert werden (Strafprozessrechtsänderungsgesetz 2018)
(17 Blg NR XXVI. GP)

Zu § 134 Z 3a in Verbindung mit § 135a Abs. 2 StPO:

Unbeschadet der grundsätzlichen Bewertung einer derartigen Überwachungsmaßnahme wird auf Folgendes hingewiesen:

Nach dem vorgeschlagenen § 135a Abs. 2 ist die Überwachung verschlüsselter Nachrichten nur zulässig, wenn nach Beendigung der Ermittlungsmaßnahme das Programm „funktionsunfähig ist oder ohne dauerhafte Schädigung oder Beeinträchtigung des Computersystems (…) entfernt wird“ und „keine Schädigung oder dauerhafte Beeinträchtigung dritter Computersysteme (…) bewirkt.“

Dies bedeutet, dass jede zu entwickelnde Technik diesen rechtlichen Anforderungen zu entsprechen hat.

In Bezug auf Einzelfälle ist sicherzustellen, dass entgegen den Voraussetzungen des § 135a Abs. 2 gewonnene Erkenntnisse in einem Strafprozess nicht verwertet werden können (vgl. § 140 Abs. 1 StPO).

Gemäß § 135a Abs. 1 Z 3 lit. b. ist die Überwachung auch zulässig, wenn „auf Grund bestimmter Tatsachen anzunehmen ist, dass eine einer solchen Tat dringend verdächtige Person das Computersystem, in dem ein Programm zur Überwachung verschlüsselter Nachrichten installiert werden soll, benützen oder mit ihm eine Verbindung herstellen werde“.

Angesichts des Umstands, dass dadurch Dritte, gegen die selbst kein Tatverdacht vorliegt, von einer derartigen Überwachungsmaßnahme betroffen sind, sollte überlegt werden, ob eine höhere Schwelle als die Annahme „auf Grund bestimmter Tatsachen“ im Gesetz verankert werden sollte.

Es sollte nochmals überlegt werden, ob dem Begriff „Nachrichten“ in § 134 Z 3a StPO nicht ein soziales Verständnis von Kommunikation als Nachrichteninhalt zugrunde gelegt werden sollte.

Zu § 134 Z 2a in Verbindung mit §135 Abs. 2a StPO:

Im Gesetz sind in § 135 Abs. 2a die Voraussetzungen für die Verwendung des sogenannten IMSI-Catchers festgelegt. Es sollte nochmals geprüft werden, ob damit eine ausreichende Begrenzung der Einsatzmöglichkeiten dieses IMSI-Catchers geschaffen wurde, zumal die technischen Möglichkeiten über die in der Regierungsvorlage (rechtlich) vorgesehenen Einsatzgebiete hinausgehen.

Zu § 134 Z 2b:

Zur Sicherung der Verfassungs- und Unionsrechtskonformität der Anlassdatenspeicherung sollte insbesondere die Definition, was unter einer schweren Straftat zu verstehen ist, vor dem Hintergrund der einschlägigen Judikatur des EuGH nochmals überprüft werden.

Es sollte die im Gesetz vorgesehene Aufbewahrungsdauer von längstens zwölf Monaten nochmals begründet werden.

Zu den Rechtsschutzbeauftragten:

Angesichts der Aufgabenstellung der Rechtsschutzbeauftragten in Bezug auf die in der StPO vorgesehenen Überwachungsmaßnahmen sollte sichergestellt werden, dass diese auch über ausreichende Ressourcen verfügen, um den im Gesetz vorgesehenen Aufgaben auch tatsächlich nachkommen zu können.

28. März 2018
Für den Arbeitsausschuss
Die Geschäftsstelle des Datenschutzrates:
HROVAT-WESENER

Elektronisch gefertigt