Republik Österreich
Datenschutzbehörde

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

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

GZ: DSB-D055.023/0001-DSB/2019 Sachbearbeiter: Dr. Matthias SCHMIDL

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 das Wehrgesetz 2001, das Heeresdisziplinargesetz 2014, das Heeresgebührengesetz 2001, das Auslandseinsatzgesetz 2001, das Militärbefugnisgesetz, das Sperrgebietsgesetz 2002, das Munitionslagergesetz 2003, das Militärauszeichnungsgesetz 2002, das Verwundetenmedaillengesetz und das Truppenaufenthaltsgesetz geändert werden (Wehrrechtsänderungsgesetz 2019 – WRÄG 2019); do. GZ S91000/5-ELeg/2018 (1)

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

Zu Artikel 5 (Änderung des Militärbefugnisgesetzes):

Zu Z 5 (§ 8 Abs. 2a):

Gemäß dieser Bestimmung soll es militärischen Organen im Wachdienst ermöglicht werden, Personen zu kontrollieren, die einer öffentlichen Beleidigung des Bundesheeres oder einer selbständigen Abteilung des Bundesheeres verdächtig sind.

Nach den Erläuterungen soll diese Bestimmung insbesondere der Feststellung der Identität von Personen dienen, obgleich sich dies – anders als etwa in den Abs. 1 und 2 explizit angeordnet – aus dem Gesetzestext nicht ergibt.

Die Feststellung der Identität stellt einen Eingriff in das verfassungsgesetzlich gewährleistete Recht nach § 1 DSG dar und darf nur unter den in § 1 Abs. 2 iVm §§ 36 ff leg. cit. normierten Voraussetzungen erfolgen.

Nach der ständigen Rechtsprechung des Verfassungsgerichtshofes muss eine Ermächtigungsnorm iSd § 1 Abs. 2 DSG (2000) ausreichend präzise, also für jedermann vorhersehbar, bezeichnen, unter welchen Voraussetzungen die Ermittlung bzw. die Verwendung der Daten für die Wahrnehmung konkreter Verwaltungsaufgaben zulässig ist. Der jeweilige Gesetzgeber muss somit iSd § 1 Abs. 2 DSG 2000 eine materienspezifische Regelung in dem Sinn vorsehen, dass die Fälle zulässiger Eingriffe in das Grundrecht auf Datenschutz konkretisiert und begrenzt werden (siehe dazu VfSlg. 18.146/2007 u.a.).

Gemessen an diesen Vorgaben erweist sich die angestrebte Norm als zu unpräzise. So ist der Norm nicht zu entnehmen, was unter den Begriff einer „öffentlichen Beleidigung des Bundesheeres oder einer selbständigen Abteilung des Bundesheeres“ fällt. Nur die Erläuterungen verweisen diesbezüglich auf die §§ 116 f StGB.

Sollte intendiert sein, militärische Organe im Wachdienst zur Identitätsfeststellung einer Person, die einer gerichtlich strafbaren Handlung verdächtig ist, zu ermächtigen, wird ungeachtet dessen auf folgende grundsätzliche Frage hingewiesen:

Der oben angeführten Rechtsprechung des Verfassungsgerichtshofes ist zu entnehmen, dass die Verwendung von Daten für die Wahrnehmung konkreter Verwaltungsaufgaben zulässig sein muss. Dies setzt implizit auch eine entsprechende behördliche Zuständigkeit zur Verwendung dieser Daten voraus.

§ 38 DSG, der für die Datenverarbeitung im Rahmen der militärischen Eigensicherung einschlägig ist, normiert, dass die Verarbeitung personenbezogener Daten u.a. nur dann rechtmäßig ist, soweit sie gesetzlich vorgesehen und für die Erfüllung einer Aufgabe erforderlich und verhältnismäßig ist, die von der zuständigen Behörde zu den in § 36 Abs. 1 DSG genannten Zwecken wahrgenommen wird.

Die Zuständigkeit zur Feststellung der Identität zwecks Einleitung eines strafprozessualen Verfahrens scheint jedoch vom Zweck der militärischen Eigensicherung (vgl. dazu § 2 MBG sowie §§ 36 und 38 DSG) nicht erfasst.

Es wird daher angeregt, die angestrebte Norm einer nochmaligen Beurteilung zu unterziehen.

Zu Z 8 (§ 22 Abs. 2a und 2b):

Zu Abs. 2a:

Mit dieser Bestimmung sollen militärische Organe und Dienststellen der militärischen Nachrichtendienste ermächtigt werden, von Betreibern öffentlicher Telekommunikationsdienste und sonstigen Diensteanbietern Auskünfte über bestimmte Kommunikationsdaten zu verlangen.

Auskunftsverlangen über diese Daten stellen einen Eingriff in das Grundrecht auf Datenschutz nach § 1 DSG dar.

Es wird daher einleitend auf die oben angeführte Rechtsprechung des Verfassungsgerichtshofes zur Qualität einer Eingriffsnorm verweisen. Ebenso misst der Verfassungsgerichtshof bei Eingriffen in das Grundrecht auf Datenschutz einem ausreichenden Rechtsschutz große Bedeutung (vgl. dazu etwa VfSlg. 19.657/2012 sowie das Erkenntnis vom 29. November 2017, G 223/2016).

Die Erläuterungen verweisen diesbezüglich auf § 53 Abs. 3a SPG, welcher Abs. 2a nachempfunden ist.

Ein Vergleich von Abs. 2a mit § 53 Abs. 3a SPG erhellt, dass die Referenzbestimmung im SPG wesentlich genauer determiniert, zu welchen Zwecken Auskunft über eine Internetprotokolladresse (IP-Adresse) (Z 2) bzw. Namen und Anschrift eines Benutzers, dem eine IP-Adresse zu einem bestimmten Zeitpunkt zugewiesen war (Z 3), verlangt werden kann. Ebenso ist in Abs. 53 Abs. 3a SPG durch Verweise auf die einschlägigen Materiengesetze sichergestellt, was unter den Begriffen „Betreiber öffentlicher Kommunikationsdienste“ und „sonstiger Diensteanbieter“ zu verstehen ist.

Zusätzlich sind in § 53 Abs. 3c SPG flankierende Bestimmungen zur Sicherstellung der Wahrung der Rechte von Betroffenen (insbesondere die nachträgliche Informationspflicht) vorgesehen.

Der vorliegende Entwurf führt als Zweck lediglich die „wesentliche Voraussetzung zur Erfüllung von Aufgaben“ an.

Gemessen an der oben zitierten Rechtsprechung des Verfassungsgerichtshofes zu § 1 Abs. 2 DSG und zum erforderlichen Rechtsschutz bei Eingriffen erscheint § 22 Abs. 2a Z 2 und 3 daher zu wenig determiniert.

Eine § 53 Abs. 3c bzw. § 91c Abs. 1 SPG nachempfundene Regelung zur Wahrung der Rechtsschutzinteressen Betroffener fehlt gänzlich. Nähere Bestimmungen zur Speicherdauer sind dem Entwurf ebenso nicht zu entnehmen.

Abgesehen davon wird auf folgendes hingewiesen:

Der Zugriff staatlicher Behörden auf Kommunikationsdaten fußt unionsrechtlich auf der Ausnahme nach Art. 15 Abs. 1 der Richtlinie 2002/58/EG. Der EuGH hat in seiner Rechtsprechung klargestellt, dass auch die Ausnahmen von der genannten Richtlinie – dazu zählen u.a. die nationale Sicherheit und die

Landesverteidigung – in den Anwendungsbereich des Unionsrechts fallen und folglich einer Prüfung durch den EuGH zugänglich sind (vgl. dazu das Urteil vom 21. Dezember 2016, C-203/15 und C-698/15).

Im genannten Urteil hat der EuGH festgehalten, dass der Zugriff staatlicher Behörden auf Kommunikationsdaten einen besonders schweren Eingriff in die durch Art. 7 und 8 EU-GRC gewährten Rechte darstellt und daher nur zur Bekämpfung schwerer Kriminalität zulässig ist. Der Zugriff auf Kommunikationsdaten ist einer vorherigen Genehmigung durch ein Gericht oder eine unabhängige Verwaltungsbehörde zu unterwerfen.

Im Urteil vom 2. Oktober 2018, C-207/16, hat der EuGH seine Aussagen im Urteil vom 21. Dezember 2016 dahingehend präzisiert, dass die Schwere des Grundrechtseingriffes infolge eines Zugriffs staatlicher Behörden auf Kommunikationsdaten in Relation zur Schwere der zu verfolgenden strafbaren Handlung zu stehen hat. Folglich stellt etwa ein Auskunftsverlangen, das lediglich darauf abzielt, die Identität der Inhaber von SIM-Karten während eines bestimmten Zeitraums herauszufinden, keinen so schweren Eingriff dar, dass er lediglich zur Bekämpfung besonders schwerer Formen der Kriminalität zulässig wäre.

Die Auslegung von Art. 15 Abs. 1 der Richtlinie 2002/58/EG ist derzeit Gegenstand weiterer Verfahren vor dem EuGH.

Umgelegt auf die intendierte Regelung nach § 22 Abs. 2a Z 2 und 3 bedeutet dies nach Ansicht der Datenschutzbehörde folgendes:

Auch im Lichte der genannten Rechtsprechung des EuGH erweist sich die genannte Norm als zu wenig determiniert. Insbesondere geht nicht mit der erforderlichen Klarheit hervor, für welche konkreten Zwecke Auskunft über bestimmte Kommunikationsdaten verlangt werden kann.

Darüber hinaus ist vor einer Ermittlung von Daten nach Abs. 2a auch keine Einbindung des Rechtsschutzbeauftragten nach § 22 Abs. 8 MBG vorgesehen, obwohl dies erforderlich sein könnte (vgl. dazu § 91c Abs. 1 SPG, wo zumindest eine ex-post Information des Rechtsschutzbeauftragten vorgesehen ist).

Zu Abs. 2b:

Die Erläuterungen verweisen auf § 11 Abs. 1 Z 7 PStSG als Referenzbestimmung. Ein Vergleich zeigt, dass auch hier die Referenzbestimmung einen wesentlich höheren Determinierungsgrad aufweist, als die angestrebte Norm.

So geht aus Abs. 2b nicht hervor, was unter die Begriffe „Verkehrsdaten“, „Zugangsdaten“ und „Standortdaten“ fällt. Ein Verweis auf die Legaldefinitionen im TKG 2003 – wie auch in § 11 Abs. 1 Z 7 PStSG vorgesehen – wird angeregt.

Zudem ist ein Auskunftsverlangen nach § 11 Abs. 1 Z 7 PStSG an strengere Voraussetzungen gebunden als in Abs. 2b vorgesehen: So hat über eine solche Maßnahme gemäß § 14 Abs. 3 PStSG der Rechtsschutzsenat – bestehend aus dem Rechtsschutzbeauftragten und zwei seiner Stellvertreter – mit Stimmenmehrheit zu entscheiden.

Eine vergleichbare Regelung ist Abs. 2b nicht zu entnehmen, es wird lediglich auf § 22 Abs. 8 verwiesen, der jedoch keine dem § 14 Abs. 3 PStSG vergleichbare Regelung darstellt.

Auch eine § 11 Abs. 1 Z 7 letzter Satz PStSG vergleichbare Einschränkung ist Abs. 2b nicht zu entnehmen.

Im Übrigen wird auf die Ausführungen zu Abs. 2a verwiesen.

Es wird daher angeregt, sowohl Abs. 2a als auch Abs. 2b im Lichte der angeführten Rechtsprechung des Verfassungsgerichtshofes sowie der einschlägigen Rechtsprechung des EuGH einer nochmaligen Prüfung zu unterziehen.

Zu Z 12 (§ 25 Abs. 1 Z 2):

Die Zulässigkeit einer Datenübermittlung nach dem 3. Hauptstück des DSG, welches im Kontext des MBG einschlägig ist, richtet sich nach § 40 Abs. 2 DSG.

Demgemäß ist eine Übermittlung für einen nicht in § 36 Abs. 1 DSG genannten Zweck nur zulässig, wenn dies gesetzlich oder in unmittelbar anwendbaren Rechtsvorschriften, die innerstaatlich den Rang eines Gesetzes haben, ausdrücklich vorgesehen ist und der Empfänger zur Verarbeitung dieser personenbezogenen Daten für diesen anderen Zweck befugt ist.

Insofern ist fraglich, ob die Wortfolge „oder die Übermittlung der Wahrung eines wichtigen öffentlichen Interesses dient“ Deckung in § 40 DSG findet.

Eine Kopie dieser Stellungnahme geht an das Präsidium des Nationalrates.

13. Februar 2019
Die Leiterin der Datenschutzbehörde
JELINEK