REPUBLIK ÖSTERREICH DATENSCHUTZRAT

An das
Bundesministerium für Inneres
Herrengasse 7
1010 Wien

Mit E-Mail:
bmi-III-A-4-stellungnahmen@bmi.gv.at

BMJ - Kompetenzstelle GDSR (Geschäftsstelle des Datenschutzrates)

dsr@bmj.gv.at
+43 1 52152 2918
Museumstraße 7, 1070 Wien

E-Mail-Antworten sind bitte
unter Anführung der Geschäftszahl an
dsr@bmj.gv.at zu richten.

Geschäftszahl: 2025-0.390.681

GZ des Begutachtungsentwurfes:
2025-0.272.220

Entwurf eines Bundesgesetzes, mit dem das Staatsschutz- und Nachrichtendienst-Gesetz, das Sicherheitspolizeigesetz, das Telekommunikationsgesetz 2021, das Bundesverwaltungsgerichtsgesetz und das Richter- und Staatsanwaltschaftsdienstgesetz geändert werden; Stellungnahme des Datenschutzrates

Der Datenschutzrat hat in seiner 281. Sitzung am 21. Mai 2025 einstimmig beschlossen, zu der im Betreff genannten Thematik folgende Stellungnahme abzugeben:

I. Materialien zum Entwurf

1 **Laut den Erläuterungen zum Entwurf** soll mit dieser Novelle einerseits für den Aufgabenbereich des Verfassungsschutzes eine gesonderte Möglichkeit des Aufschubs sicherheitspolizeilichen Einschreitens oder kriminalpolizeilicher Ermittlungen geschaffen werden. Entsprechend der maßgeblichen Bestimmungen in § 23 SPG sowie § 99 Abs. 4 f StPO soll es den Organisationseinheiten gemäß § 1 Abs. 3 künftig möglich sein, unter Einhaltung sämtlicher dort bereits genannter Voraussetzungen, sicherheitspolizeiliches Einschreiten oder kriminalpolizeiliche Ermittlungen aufzuschieben, soweit ein überwiegendes Interesse an der Erfüllung der Aufgabe nach § 6 Abs. 1 oder 2 besteht.

1 Andererseits habe die Praxis seit Inkrafttreten des SNG gezeigt, dass die strikte Aufgabenzuweisung der erweiterten Gefahrenerforschung zur Beobachtung einer Gruppierung

(§ 6 Abs. 1) zu der für den Aufgabenbereich Nachrichtendienst zuständigen Organisationseinheit der Direktion und des vorbeugenden Schutzes vor verfassungsgefährdenden Angriffen durch Einzelpersonen (§ 6 Abs. 2) zu den für den Aufgabenbereich Staatsschutz zuständigen Organisationseinheiten (§ 1 Abs. 3) trotz Einrichtung einer Informationsschnittstelle eine rasche, zweckmäßige und effiziente Aufgabenerfüllung in gewissen Fallkonstellationen erschweren kann, weshalb eine Rechtsgrundlage geschaffen werden soll, damit der Direktor im Einzelfall unter gesetzlich festgelegten Kriterien den Aufgabenbereich Nachrichtendienst zu der Wahrnehmung einer Aufgabe nach § 6 Abs. 2 ermächtigen kann.

2 Weiters soll laut den Erläuterungen eine Rechtsgrundlage im SNG geschaffen werden, um in bestimmten, gesetzlich klar definierten Fällen die Überwachung von Inhaltsdaten nach dem Vorbild der Regelungen in der StPO zu ermöglichen. Angesichts der – insbesondere im Bereich grenzüberschreitender terroristischer Aktivitäten – erfolgten zunehmenden Verlagerung herkömmlicher, unverschlüsselter Telekommunikation auf internetbasierte, zumeist end-to-end-verschlüsselte Kommunikation (wie etwa über WhatsApp, Skype oder Signal) soll zusätzlich eine Rechtsgrundlage für die Überwachung verschlüsselter Nachrichten zur effektiven Bekämpfung verfassungsschutzrelevanter Bedrohungslagen geschaffen werden.

3 Im Rahmen der Novelle sollen auch Ergänzungen des Deliktskatalogs der verfassungsgefährdenden Angriffe um für den Verfassungsschutz relevante Tatbestände insbesondere des Strafgesetzbuches und des Waffengesetzes vorgenommen werden.

4 Außerdem handle es sich um Anpassungen des SPG, durch die einerseits eine verpflichtende Vertrauenswürdigkeitsprüfung des Rechtsschutzbeauftragten, seiner Stellvertreter und sonstigen administrativen Mitarbeiter verankert werden soll. Andererseits soll eine Möglichkeit zur Abberufung des Rechtsschutzbeauftragten bzw. seiner Stellvertreter durch den Bundespräsidenten im Falle grober Pflichtverletzungen oder einer nachträglichen Unvereinbarkeit mit der Funktion geschaffen werden.

5 Mit den Änderungen des Telekommunikationsgesetzes 2021 (TKG 2021) sollen die für die allfällige Mitwirkung der (Kommunikationsdienste)Anbieter an der Nachrichtenüberwachung erforderlichen Anpassungen vorgenommen werden.

6 Schließlich soll durch die Anpassungen im Bundesverwaltungsgerichtsgesetz (BVwGG) und im Richter- und Staatsanwaltschaftsdienstgesetz (RStDG) die Einführung einer Rufbereitschaft sowie eines Journaldienstes beim Bundesverwaltungsgericht ermöglicht werden.

II. Inhaltliche Bemerkungen

A. Grundsätzliches

7 a. Der Datenschutzrat hat in seiner 279. Sitzung am 23. September 2024 zum Entwurf eines Bundesgesetzes, mit dem das Staatsschutz- und Nachrichtendienstgesetz geändert wird, eine einstimmige Stellungnahme abgegeben (Stellungnahme des Datenschutzrates vom 24. September 2024, GZ 2024-0.679.067).

8 Vorweg wird angemerkt, dass die Anmerkungen des Datenschutzrates aus der zit. Stellungnahme nur teilweise umgesetzt wurden. Nachdem der vorliegende Begutachtungsentwurf eines Bundesgesetzes, mit dem das Staatsschutz- und Nachrichtendienst-Gesetz, das Sicherheitspolizeigesetz, das Telekommunikationsgesetz 2021, das Bundesverwaltungsgerichtsgesetz und das Richter- und Staatsanwaltschaftsdienstgesetz geändert werden, zT inhaltsgleiche Regelungen enthält, wird an den diesbezüglichen Anmerkungen aus der zit. Stellungnahme – soweit diese für den vorliegenden Entwurf relevant sind – festgehalten bzw. werden diese nochmals dargelegt.

9 b. Der Entwurf schafft eine Rechtsgrundlage für die Überwachung verschlüsselter Nachrichten und unter welchen Voraussetzungen eine solche stattfinden darf. Derartige Ermittlungsmaßnahmen stellen nach der Rechtsprechung einen erheblichen Eingriff in das Grundrecht auf Datenschutz gemäß § 1 DSG dar und können nur dann verhältnismäßig sein, wenn diese Überwachung verschlüsselter Nachrichten geeignet und erforderlich ist und das gelindeste Mittel hinsichtlich des Eingriffes in das Grundrecht auf Datenschutz darstellt.

10 Im Anhang zum Vorblatt wird zwar ausgeführt, dass von einem Anfall von etwa 30 Verfahren pro Jahr für die Überwachung unverschlüsselter Nachrichten nach § 11 Abs. 1 Z 8 und 5 bis 15 Verfahren pro Jahr für die Überwachung verschlüsselter Nachrichten nach Z 9 auszugehen wäre. Es stellt sich jedoch die Frage, auf welcher Grundlage diese Annahme beruht. Dies wäre zu ergänzen. Konkrete Angaben zur Erforderlichkeit sowie zur Eignung dieser Maßnahme sind aus den vorliegenden Erläuterungen nicht ausreichend erkennbar. Seitens des informierten Vertreters der DSN wurden in der 279. Sitzung am 23. September 2024 zwar Anwendungsfälle zur Begründung der Erforderlichkeit genannt, die Erläuterungen müssten aber um entsprechende Begründungen und Datenmaterial ergänzt werden.

11 Für den Fall, dass eine derartige eingriffsintensive Überwachungsmaßnahme beschlossen wird, sollte – wie auch in der oben zit. Stellungnahme des Datenschutzrates ausgeführt

wurde – jedenfalls in den Entwurf eine Regelung zur verpflichtenden Evaluierung der Maßnahme aufgenommen werden sowie vorgesehen werden, dass dem Datenschutzrat jährlich – beginnend ab dem ersten Jahr nach dem Inkrafttreten des Entwurfes – ein detaillierter Bericht über die Anwendung sowie den Nutzen der Überwachung übermittelt wird. Zudem sollte auch ausführlicher dargelegt werden, weshalb mit weniger eingriffsintensiven (Alternativ-)Maßnahmen nicht auch das erforderliche Ziel mit gelinderen Mitteln erreicht werden kann.

12 Aufgrund der mangelnden Kenntnis der technischen Spezifikationen ist eine abschließende datenschutzrechtliche Beurteilung, insbesondere auch hinsichtlich der Verhältnismäßigkeit, weiterhin nicht möglich.

B. Zum Entwurf

Artikel 1 – Änderung des Staatsschutz- und Nachrichtendienst-Gesetzes

Zu Z 3 (§ 6 Abs. 4 und 5):

13 Die vorgesehene Aufweichung der bislang strikten Trennung zwischen den Aufgabenbereichen Nachrichtendienst und Staatsschutz wird in den Erläuterungen damit begründet, dass die strikte Aufgabenzuweisung in der Praxis seit Inkrafttreten des SNG trotz Einrichtung der Informationsschnittstelle eine rasche, zweckmäßige und effiziente Aufgabenerfüllung in gewissen Fallkonstellationen erschweren kann.

14 Es stellt sich die Frage, welche Konsequenzen die Möglichkeit zur punktuellen Wahrnehmung von Aufgaben des Staatsschutzes durch die für den Aufgabenbereich Nachrichtendienst zuständige Organisationseinheit der Direktion in Bezug auf die Weiterverarbeitung personenbezogener Daten für andere Zwecke als jenen, zu dem sie ermittelt wurden, hat. Lt. Auskunft des informierten Vertreters in der Sitzung vom 21. Mai 2025 werden Daten, für andere Zwecke als jenen, zu dem sie ermittelt wurden, gelöscht.

15 Den Erläuterungen zufolge erfolgt die Verarbeitung bereits ermittelter Daten *„auch im Rahmen der Aufgabenübertragung nach den bestehenden Datenverarbeitungsregelungen, vgl. insbesondere § 10 Abs. 2 bzw. § 12“*.

16 Gemäß § 10 Abs. 2 SNG dürfen die Organisationseinheiten gemäß § 1 Abs. 3 SNG (dh. die DSN und die für den Staatsschutz zuständigen OE der Landespolizeidirektionen) Daten, die sie in Vollziehung von Bundes- oder Landesgesetzen rechtmäßig verarbeitet haben, für die Zwecke des Abs. 1 verarbeiten, wobei ein automationsunterstützter Datenabgleich iSd

§ 141 StPO davon nicht umfasst ist und bestehende Übermittlungsverbote unberührt bleiben. Die Verarbeitungsermächtigung nach § 10 Abs. 2 SNG ist nicht auf die konkreten Aufgabenbereiche Staatsschutz bzw. Nachrichtendienst bzw. die dafür zuständigen Organisationseinheiten beschränkt; § 12 SNG regelt jedoch näher, welche konkreten Datenkategorien für welche Zwecke verarbeitet werden dürfen.

17 Fraglich ist, ob mit der in § 6 Abs. 5 vorgesehenen Aufweichung der bislang strikten Trennung zwischen den Aufgaben Nachrichtendienst und Staatsschutz iVm der in § 10 Abs. 2 SNG vorgesehenen pauschalen Verarbeitungsermächtigung künftig Weiterverarbeitungen für andere Zwecke in weiterem Umfang möglich sind als im Rahmen der bestehenden Trennung zwischen den Aufgabenbereichen Nachrichtendienst und Staatsschutz.

18 Damit stellt sich im Lichte der datenschutzrechtlich gebotenen Zweckbindung (vgl. § 37 Abs. 1 Z 2 DSG) weiterhin die Frage, inwieweit im Falle einer punktuellen Ermächtigung zur Erfüllung einer Aufgabe des Staatsschutzes nach § 6 Abs. 5 die im Rahmen des Nachrichtendienstes ermittelten personenbezogenen Daten für die betreffende Aufgabe des Staatsschutzes verwendet werden dürfen (und vice versa) und ob dies ggf. Auswirkungen auf die Zulässigkeit von Übermittlungen an für den Aufgabenbereich Staatsschutz zuständige Organisationseinheiten hat.

19 Die mit einer punktuellen Ermächtigung iSd § 6 Abs. 5 verbundenen Auswirkungen in Bezug auf Datenverarbeitungen sollten in den Erläuterungen verständlicher und ausführlicher dargestellt werden.

Zu Z 5 (§ 11 Abs. 1):

20 a. In den Erläuterungen wird die Adaptierung der Vorgaben für die bestehenden Ermittlungsbefugnisse in § 11 Abs. 1 Z 1, 2, 3, 5 und 7 mit den neuen Ermittlungsmaßnahmen der Überwachung unverschlüsselter und verschlüsselter Nachrichten gemäß § 11 Abs. 1 Z 8 und 9 als ultima-ratio-Maßnahme begründet und ausgeführt, dass die „begriffliche Neuordnung“ in den Z 1 bis 7 „keine Herabsetzung der Zulässigkeitsvoraussetzungen“ für diese Ermittlungsmaßnahmen bedeute.

21 Dies erscheint insoweit nur bedingt nachvollziehbar, als künftig für den Einsatz der in Z 1, 2, 3, 5 und 7 geregelten Ermittlungsmaßnahmen nicht mehr die Schwelle der sonstigen Aussichtslosigkeit (sondern in Z 1, 2 und 3 lediglich der wesentlich erschwerten Aufgabenerfüllung) gelten soll.

22 Angemerkt wird idZ, dass im Sinne der Ausführungen in der zit. Stellungnahme des Datenschutzrates die Erforderlichkeit und Verhältnismäßigkeit der jeweiligen Ermittlungsmaßnahmen unter den künftig weniger strengen Voraussetzungen vornehmlich vom für die Materie zuständigen Bundesministerium für Inneres zu beurteilen ist, in den Erläuterungen jedoch im Einzelnen mit Bezug auf die jeweilige Ermittlungsmaßnahme näher dargelegt werden sollte. Auf den in § 1 Abs. 2 letzter Satz DSG verankerten Grundsatz des gelindesten Mittels wird in diesem Zusammenhang hingewiesen.

23 b. Die in Z 8 und 9 leg.cit. neu vorgesehene Ermächtigung zur Überwachung von (verschlüsselten) Nachrichten und Informationen ermöglicht weitreichende Eingriffe in das Grundrecht auf Datenschutz (und allgemein die grundrechtlich geschützte Privatsphäre).

24 Die Erforderlichkeit und Verhältnismäßigkeit der betreffenden Grundrechtseingriffe zu den damit verfolgen Zwecken ist – wie bereits in der zit. Stellungnahme des Datenschutzrates hervorgehoben wurde – vornehmlich vom Bundesministerium für Inneres zu beurteilen.

25 Nach der Definition in § 11 Abs. 1 Z 8 würde die genannte Ermittlungsmaßnahme über den Umfang der Überwachung von Nachrichten iSd § 134 Z 3 StPO hinausgehen, da sie nicht auf Kommunikationsvorgänge unter Beteiligung natürlichen Personen beschränkt ist. Die Erläuterungen bestätigen, dass „auch die autonome Kommunikation zweier Endgeräte ohne menschliches Zutun (M2M-Kommunikation) inklusive der Datenübermittlung an Server im Rahmen von automatisierten Backups erfasst“ sein soll. Begründet wird diese abweichende Begriffsbestimmung in den Erläuterungen lediglich mit einer Anpassung „an den Bedarf des Verfassungsschutzes“, ohne diesen Bedarf (auch in Gegenüberstellung zum strafprozessualen Bedarf) näher zu konkretisieren. Der Entwurf enthält auch keine Differenzierungen in Bezug auf Kommunikationsvorgänge, die aus verfassungsrechtlichen Gründen besonders geschützt sind (etwa mit Journalisten, Rechtsanwälten oder sonstigen Berufsgeheimnisträgern).

26 In datenschutzrechtlicher (und allgemein grundrechtlicher) Hinsicht stellt die Überwachung von (verschlüsselten) Nachrichten iSd § 11 Abs. 1 Z 8 und 9 durch diese Ausdehnung einen deutlich intensiveren Grundrechtseingriff dar als die (ebenfalls bereits eingriffsintensive) strafprozessuale Überwachung von Nachrichten iSd § 134 Z 3 StPO. Dabei ist auch zu berücksichtigen, dass die M2M-Kommunikation potentiell deutlich größeren Umfang haben kann und möglicherweise nicht nur autonom und ohne menschliches Zutun in Bezug auf den einzelnen Kommunikationsvorgang stattfindet, sondern möglicherweise auch nicht vorab durch eine betroffene natürliche Person beschränkt oder auch nur überblickt werden kann. In diesem Sinn könnten sich die Ermittlungsmaßnahmen nach § 11 Abs. 1 Z 8 und 9

aus Sicht der betroffenen Person im Ergebnis ähnlich eingriffsintensiv darstellen wie eine (von der Definition § 11 Abs. 1 Z 8 formal nicht erfasste) Online-Durchsuchung. In diesem Zusammenhang ist auch auf den technologischen Fortschritt Bedacht zu nehmen, etwa iHa die automatisierte Generierung personenbezogener Daten, die Gegenstand von M2M-Kommunikation sein können (und insoweit mit einem bloßen automatisierten Backup, wie es in den Erläuterungen beispielhaft genannt ist, nicht vergleichbar wären).

27 Mit Blick auf die besondere (und über bestehende Ermittlungsmaßnahmen deutlich hinausgehende) Eingriffsintensität der Überwachung von (verschlüsselten) Nachrichten iSd § 11 Abs. 1 Z 8 und 9 sollte die Erforderlichkeit und Verhältnismäßigkeit der Ermittlungsmaßnahmen nochmals eingehend geprüft werden.

28 c. Die Überwachung verschlüsselter Nachrichten und Informationen nach Z 9 erfolgt „durch Einbringen eines Programms in ein Computersystem“ eines Betroffenen nach § 6 Abs. 2 SNG. Inwieweit derartige Programme technisch so gestaltet werden können, dass tatsächlich nur von der konkreten Bewilligung umfasste personenbezogene Daten verarbeitet werden, kann in technischer Hinsicht – wie bereits in der zit. Stellungnahme des Datenschutzrates dargelegt wurde – nicht beurteilt werden. In datenschutzrechtlicher Hinsicht setzt dies aber jedenfalls voraus, dass die Abgrenzung bereits unmittelbar bei der Ermittlung der personenbezogenen Daten (und nicht etwa erst bei deren Ausleitung) erfolgt.

29 Fraglich ist, ob auch die technischen Vorgänge vor der Ausleitung eine Verarbeitung personenbezogener Daten iSd § 36 Abs. 2 Z 2 DSG darstellen und davon auch Daten umfasst sind, die nicht zur Ausleitung bestimmt sind.

30 d. Zum Schaffen bzw. Ausnutzen von Sicherheitslücken und damit verbundene Risiken iHa die Cybersicherheit im Rahmen der Z 9 wird eingangs auf die Ausführungen in der zit. Stellungnahme des Datenschutzrates verwiesen. Das Einbringen eines solchen Programms in ein Computersystem erfordert mitunter – auch nach Auskunft der informierten Vertreter in der Sitzung vom 21. Mai 2025 – die Ausnützung bestehender Sicherheitslücken in diesem Computersystem, wenn dies aus der Ferne und/oder bei einem Smartphone erfolgen soll, denn die gängigen Smartphone-Betriebssysteme sehen dafür keine reguläre Möglichkeit vor. Sicherheitslücken stehen niemandem exklusiv zur Verfügung, sondern können jederzeit auch von Kriminellen oder für Spionagezwecke ausgenützt werden. Eine solche Sicherheitslücke betrifft alle, die das gleiche System nutzen. Dies können auch staatliche Behörden oder Berufsgeheimnisträger sein. Es gefährdet insofern die Datensicherheit im Allgemeinen, wenn man eine solche Sicherheitslücke für Zwecke der Überwachung

Einzelner nützt, anstatt sie dem Hersteller des Computersystems zu melden, damit sie möglichst rasch geschlossen werden kann. Die staatliche Nutzung einer solchen Überwachungssoftware steht insofern in einem Zielkonflikt mit dem datenschutzrechtlichen Grundsatz der Integrität und Vertraulichkeit.

31 Durch die (remote-)Einbringung und Nutzung von Überwachungsprogrammen in Computersystemen im Rahmen der Z 9 könnten auch zusätzliche Sicherheitslücken geschaffen werden, die in der Folge auch von Dritten (insbesondere Kriminellen, aber zB auch ausländischen Nachrichtendiensten) genutzt werden könnten. § 15b Abs. 1 zweiter Satz SNG ordnet an, dass das eingebrachte Programm „nach dem Stand der Technik" gegen unbefugte Nutzung zu schützen ist, womit eine solche offenbar nicht von vornherein ausgeschlossen werden kann. Zu bedenken ist auch, dass die verwendete Software selbst undokumentierte weitere Funktionen, etwa die Ausleitung der Inhalte an Dritte, enthalten kann. Die damit verbundenen Gefahren und Risiken für die Betroffenen nach § 6 Abs. 2 SNG, deren Kommunikationspartner sowie gegebenenfalls auch Dritte bzw. die Allgemeinheit sind für die Beurteilung der abstrakten Verhältnismäßigkeit der Ermittlungsmaßnahme nach § 11 Abs. 1 Z 9 wesentlich, weshalb auf diesen Aspekt in den Erläuterungen – allenfalls nach Einbeziehung der für Cybersicherheit zuständigen Stellen – näher eingegangen werden sollte.

Zu Z 7 (§ 14 Abs. 2):

32 Wie bereits in der zit. Stellungnahme des Datenschutzrates dargelegt wurde, stellt sich die Frage nach dem Mehrwert der betreffenden Regelung gegenüber den bereits jetzt in § 14 Abs. 2 SNG geregelten, auch für andere Ermittlungsmaßnahmen geltenden Vorgaben für die Ermächtigung. Insbesondere stellt sich (weiterhin) die Frage, für welchen Zeitraum (künftig und/oder vergangen) eine Ermächtigung für die Ermittlungsmaßnahmen nach § 11 Abs. 1 Z 1 bis 6 – mangels expliziter Regelung, wie sie für Z 7 vorgeschlagen wird – erteilt werden darf. Es wird daher neuerlich angeregt, eine Konsolidierung des bisherigen § 14 Abs. 2 letzter Satz SNG und des daran neu anzufügenden letzten Satzes zu prüfen.

33 Gemäß § 14 Abs. 6 hat der Rechtsschutzbeauftragte bei erstmaliger Nutzung binnen zwei Wochen nach Verständigung zu beurteilen, ob das Programm den Anforderungen gemäß § 15b Abs. 1 entspricht. Den Materialien ist nicht zu entnehmen, wie der Rechtsschutzbeauftragte die unabhängige Prüfmaßnahme, die auch komplexe technische Elemente beinhaltet, innerhalb kurzer Frist bewältigen kann. Zudem wird angemerkt, dass die informierten Vertreter in der 279. Sitzung am 23. September 2024 zugesagt haben, die Praktikabilität der Fristen mit dem Rechtsschutzbeauftragten abzuklären.

34 In den Erläuterungen sollten vor diesem Hintergrund auch Ausführungen zur Praktikabilität der Fristen im Hinblick auf den Rechtsschutzbeauftragten aufgenommen werden.

Zu Z 11 (§§ 15a bis 15c):

35 a. Wie bereits in der zit. Stellungnahme des Datenschutzrates dargelegt wurde, sollte in den Erläuterungen näher dargelegt werden, welche Angaben in § 15a Abs. 2 Z 8 mit Angaben über „die beabsichtigte Art des Einsatzes technischer Mittel“ konkret gemeint und wie detailliert diese zu gestalten sind.

36 b. Zu § 15b Abs. 1 Z 3, demzufolge bei der Durchführung der Ermittlungsmaßnahme nach § 11 Abs. 1 Z 9 technisch sicherzustellen ist, dass das eingebrachte Programm nach Beendigung der Ermittlungsmaßnahme entfernt oder funktionsunfähig wird, wird ebenfalls auf die zit. Stellungnahme des Datenschutzrates hingewiesen.

37 Die Frage, inwieweit eine vollständige Entfernung/Funktionsunfähigkeit in technischer Hinsicht – insbesondere mit Blick auf allfällige spätere Veränderungen des Computersystems durch den/die Benutzer – vorweg sichergestellt werden kann, ist weiterhin offen.

38 Weiterhin unklar sind zudem weiterhin die rechtlichen Konsequenzen, wenn sich dies im Zuge einer bereits laufenden Ermittlungsmaßnahme nachträglich als nicht (mehr) möglich erweisen sollte (vgl. das in den Erläuterungen genannte Bespiel). § 11 Abs. 1 letzter Satz ordnet zwar an, dass allgemein die Ermittlung personenbezogener Daten zu beenden ist, sobald ihre Voraussetzungen wegfallen. § 15b Abs. 1 regelt aber keine Voraussetzungen, sondern die Durchführung der Maßnahme. Die Fortführung einer Ermittlungsmaßnahme, die nicht mehr im Einklang mit den in § 15b Abs. 1 geregelten Anforderungen an die Durchführung steht, sollte jedenfalls unzulässig sein.

39 c. Im Hinblick auf § 15b Abs. 2 Z 3 ist (weiterhin) fraglich, ob der Begriff der „nicht nur flüchtigen“ Veränderungen ausreichend klar abgrenzbar ist.

40 d. Zur in § 15b Abs. 4 Z 1 vorgesehenen (gesonderten) Aufbewahrung ermittelter Nachrichten bis zur Erteilung einer Ermächtigung des Rechtsschutzbeauftragten für die Weiterverwendung für eine andere Aufgabe nach § 6 Abs. 2 SNG wird auf die zit. Stellungnahme des Datenschutzrates verwiesen.

41 In den Erläuterungen wird nunmehr ausgeführt, dass die Direktion „unverzüglich“ um die Ermächtigung des Rechtsschutzbeauftragten für die Aufgabe nach § 6 Abs. 2 SNG ansuchen soll. Dem Gesetzestext ist eine derartige Verpflichtung zur umgehenden Einholung einer

entsprechenden Ermächtigung (und somit Klärung der Zulässigkeit der Weiterverarbeitung) allerdings weiterhin nicht zu entnehmen. Eine Aufbewahrung ermittelter Nachrichten „auf Vorrat“, wenn zwar ein begründeter Gefahrenverdacht für einen anderen verfassungsgefährdenden Angriff, aber kein unmittelbarer Handlungsbedarf besteht, sollte jedenfalls – in gesetzlicher verankerter Form – unterbunden werden.

42 e. Die Erläuterungen zu § 15b führen aus, dass der Bundesminister für Inneres datenschutzrechtlich Verantwortlicher der Software sowie der im Rahmen des § 15b Abs. 2 zu führenden Dokumentationsverarbeitungen im Sinne der §§ 36 Abs. 2 Z 8, 46 ff DSG sei und als solcher für das Überwachungsprogramm ein Verzeichnis von Verarbeitungstätigkeiten zu führen (vgl. §§ 4, 49 DSG) habe, mit der Datenschutzbehörde nach Maßgabe des § 51 DSG zusammenzuarbeiten und eine Datenschutz-Folgenabschätzung durchzuführen habe (§ 52 DSG).

43 Im Zusammenhang mit der (weiterhin fraglichen) datenschutzrechtlichen Rollenverteilung iZm der Überwachung verschlüsselter Nachrichten wird auf die detaillierten Ausführungen in der zit. Stellungnahme des Datenschutzrates verwiesen. Zur Vermeidung von Rechtsunklarheiten und Vollzugsproblemen wird – soweit es sich nicht um eine alleinige Verantwortlichkeit der zuständigen Behörde, die die Ermittlungs-maßnahme einsetzt, handelt – empfohlen, die datenschutzrechtliche Rollenverteilung iZm Datenverarbeitungen nach § 11 Abs. 1 Z 9 bereits im Gesetzestext klar zu regeln. Zu beachten ist, dass eine von den allgemeinen Kriterien des § 36 Abs. 2 Z 8 DSG abweichende Festlegung nur zulässig ist, soweit die Zwecke und Mittel der Verarbeitung im Gesetz geregelt werden. Überdies muss sichergestellt sein, dass im Falle einer gesetzlichen Festlegung des Verantwortlichen dieser in der Lage ist, den datenschutzrechtlichen Verantwortlichenpflichten vollinhaltlich nachzukommen.

44 Ergänzend dazu wird auf das rezente Urteil des EuGH vom 27.2.2025, Rs. C-638/23, Amt der Tiroler Landesregierung, hingewiesen, in dem der EuGH sich iZm der gesetzlichen Festlegung eines Verantwortlichen gemäß Art. 4 Z 7 DSGVO (mit unmittelbarer Relevanz auch für die korrespondierende Regelung für den Strafverfolgungsbereich in Art. 3 Z 8 DSRL-PJ) ausführlich mit den Voraussetzungen für die Einstufung als Verantwortlicher (siehe Rn. 23-35 des Urteils) auseinandersetzt und auch die Möglichkeit eines allenfalls zu einem gesetzlich festgelegten Verantwortlichen hinzutretenden faktischen (Mit-)Verantwortlichen (vgl. idZ Rn. 48 des Urteils) anspricht.

Zu Z 12 (§ 16 Abs. 2 und 3):

45 Nach § 16 Abs. 3 kann die Information (von Betroffenen einer Aufgabe nach § 6 Abs. 1 oder 2 bzw. der von einer Überwachung von Nachrichten gemäß § 11 Abs. 1 Z 8 oder 9 betroffenen Personen) gemäß Abs. 2 mit Zustimmung des Rechtsschutzbeauftragten aufgeschoben werden, „solange durch sie die Aufgabenerfüllung gefährdet wäre“, und unterbleiben, „wenn die zu informierende Person bereits nachweislich Kenntnis erlangt hat, die Information unmöglich ist oder aus den Gründen des § 43 Abs. 4 DSG nicht erfolgen kann“.

46 Diesbezüglich wird darauf hingewiesen, dass nach § 43 Abs. 4 DSG die Unterrichtung der betroffenen Person über die Verarbeitung ihrer personenbezogenen Daten bei Vorliegen der dort geregelten Gründe stets nur „soweit und solange aufgeschoben, eingeschränkt oder unterlassen werden [kann], wie dies im Einzelfall unbedingt erforderlich und verhältnismäßig ist“. Insoweit wäre bei Wegfall von zunächst vorliegenden Gründen des § 43 Abs. 4 DSG die Information umgehend nachzuholen. Hervorzuheben ist, dass die Information der betroffenen Person über die Verarbeitung ihrer personenbezogenen Daten Grundvoraussetzung für die Geltendmachung ihrer Betroffenenrechte und daher auch entsprechend gewährleistet sein muss (vgl. idS auch VfGH 14.12.2023, G 352/2021, Rn. 101).

47 Die Formulierung in § 16 Abs. 2 vermittelt den Eindruck, dass bei Vorliegen von Gründen des § 43 Abs. 4 DSG (ebenso wie bei nachweislicher Kenntnis oder Unmöglichkeit) die Information dauerhaft unterbleiben kann, und sollte daher entsprechend überarbeitet werden.

Für den Datenschutzrat:
Der Vorsitzende
SCHILCHEGGER
22. Mai 2025

Elektronisch gefertigt