Bundesministerium
Justiz

bmj.gv.at

BMJ - IV 3 (Strafverfahrensrecht)

Parlamentsdirektion
Dr. Karl Renner Ring 3
1017 Wien
AT

Mag. Dascha Jocher-Uljanov, LL.M. (WU)
Sachbearbeiterin

dascha.jocher-uljanov@bmj.gv.at
+43 1 521 52-302223
Museumstraße 7, 1070 Wien

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

Geschäftszahl: 2025-0.372.598

Begutachtungsverfahren, Stellungnahme zum Entwurf eines Bundesgesetzes, mit dem das Staatsschutz- und Nachrichtendienst-Gesetz, das Sicherheitspolizeigesetz, das Telekommunikationsgesetz 2021, das Bundesverwaltungsgerichtsgesetz und das Richter- und Staatsanwaltschaftsdienstgesetz geändert werden (8/ME)

Allgemein:

Vorangestellt wird, dass die Stellungnahme des Bundesministeriums für Justiz (94/SNG-350/ME) im Begutachtungsverfahren zum Ministerialentwurf betreffend ein Bundesgesetz, mit dem das Staatsschutz- und Nachrichtendienstgesetz geändert wird (350/ME XXVII. GP), grundsätzlich aufrecht bleibt, sofern diesbezüglich keine Überarbeitung des Entwurfs erfolgt ist. Zur Vermeidung von Wiederholungen wird daher grundsätzlich auf die in jener Stellungnahme ausgedrückten Anregungen und Bedenken verwiesen.

Die erfolgten Änderungen im Ministerialentwurf und die Ergänzung iHa Änderungen des TKG 2021, des SPG, des BVwGG und des RStDG sowie die Vorlage einer WFA werden grundsätzlich begrüßt.

Die Übereinstimmung des im Entwurf vorliegenden Bundesgesetzes mit dem Recht der Europäischen Union ist vornehmlich vom do. Bundesministerium zu beurteilen.

Zu Artikel 1 (SNG):

Zu Ziffer 3 (§ 6 Abs. 4 und 5):

Die bereits in der Stellungnahme 94/SNG-350/ME festgehaltenen **Anmerkungen** bleiben inhaltlich auch hinsichtlich des überarbeiteten Entwurfs aufrecht. Nunmehr wurde der bisherige Entwurf eines Bundesgesetzes, mit dem das Staatsschutz- und Nachrichtendienstgesetz geändert wird (350/ME XXVII. GP) – trotz Stellungnahme des Bundesministeriums für Justiz – dahingehend ausgeweitet, dass der Aufschub von Ermittlungen und der Berichtspflicht im Gesetz verankert werden soll.

§ 6 Abs. 4 SNG sieht in der derzeit in Geltung stehenden Fassung nur die Möglichkeit eines Aufschubs der Berichtspflicht nach § 100 StPO hinsichtlich Vergehen, die kein verfassungsgefährdender Angriff nach Abs. 3 sind, und dies längstens für sechs Monate, vor.

Der Ministerialentwurf 350/ME XXVII. GP sah in § 6 Abs. 4 Z 2 sodann die Möglichkeit des Aufschubs kriminalpolizeilicher Ermittlungen nach Maßgabe des § 99 Abs. 4 Z 5 StPO vor, soweit ein überwiegendes Interesse an der Erfüllung der Aufgaben nach Abs. 1 oder 2 besteht.

Nach dem vorgeschlagenen § 6 Abs. 4 Z 2 SNG sollen Organisationseinheiten gemäß § 1 Abs. 3 SNG hingegen kriminalpolizeiliche Ermittlungen und die Berichterstattung nach § 100 StPO aufschieben können, soweit ein überwiegendes Interesse an der Erfüllung der Aufgabe nach § 6 Abs. 1 oder 2 SNG besteht, wenn mit dem Aufschub keine ernste Gefahr für Leben, Gesundheit, körperliche Unversehrtheit oder Freiheit Dritter verbunden ist. Die Gründe für den Aufschub sind zu dokumentieren. Der Staatsanwaltschaft soll binnen sechs Monaten der Bericht über den Aufschub samt der Gründe für den Aufschub zu übermitteln sein.

Die vorgeschlagene Ausweitung des Aufschubs der Berichterstattung um einen Aufschub der Ermittlungen würde – wie bereits in der Stellungnahme 94/SNG-350/ME festgehalten - die Leitungskompetenz der Staatsanwaltschaft im Ermittlungsverfahren untergraben, die jedoch seit vielen Jahren das Grundkonzept des Ermittlungsverfahrens ist (seit dem Strafprozessreformgesetz, BGBl. I Nr. 19/2004). Die in den Erläuterungen als Vorbild genannte Bestimmung des § 23 SPG ist mit der vorgeschlagenen Bestimmung nicht vergleichbar, befindet sie sich doch nicht in diesem Zielkonflikt (Aufschub des Einschreitens nach dem SPG). Auch die Bestimmung des § 99 StPO kann nicht als Vorbild für den Aufschub von Ermittlungen nach dem SNG herangezogen werden; so sieht § 99 Abs. 5 StPO vielmehr vor, dass die Kriminalpolizei die Staatsanwaltschaft von einem Aufschub nach Abs. 4 unverzüglich zu verständigen hat. § 99 Abs. 4 Z 1 StPO ermöglicht daher grundsätzlich keinen Aufschub kriminalpolizeilicher Ermittlungen wegen Aufgaben auf dem Gebiet des

Verfassungsschutzes. Die Staatsanwaltschaft kann aufgrund ihrer Leitungsbefugnis, falls sie es für erforderlich hält und nicht ohnehin Einvernehmen über das weitere Vorgehen erzielt werden kann, die Anordnung treffen, den Aufschub zu beenden und die kriminalpolizeilichen Ermittlungen einzuleiten (§ 98 StPO).

Die Staatsanwaltschaften sind in Erfüllung ihrer gesetzlichen Aufgaben zur Wahrung der Interessen des Staates in der Rechtspflege, vor allem in der Strafrechtspflege, berufen (§ 1 StAG). Die StPO regelt das Verfahren zur Aufklärung von Straftaten, über die Verfolgung verdächtiger Personen und über damit zusammenhängende Entscheidungen (§ 1 Abs. 1 StPO). Die Bestimmungen über Berichts- und Anzeigepflichten (§ 78, § 100 StPO) stellen Spezialbestimmungen zur Gewährleistung einer **effektiven Strafrechtspflege** dar und sollten nicht durch Bestimmungen in anderen – fremde Rechtsmaterien regelnden – Materiengesetzen wie dem SNG ausgehöhlt werden.

Für eine Beurteilung von Interessen im Bereich des Verfassungsschutzes, sei es im Aufgabenbereich Nachrichtendienst oder Staatsschutz, durch die Staatsanwaltschaft, insbesondere das Feststellen eines überwiegenden Interesses daran, besteht in der StPO kein Raum. § 99 Abs. 4 StPO ermöglicht zudem einen **Aufschub nur aus der Strafrechtspflege inhärenten Gründen**, nämlich zu den Zwecken der „Aufklärung einer wesentlich schwerer wiegenden strafbaren Handlung“ und der „Ausforschung von an der strafbaren Handlung führend Beteiligten“ (Z 1) und aus Interessen des Zeugen- bzw. Opferschutzes (Z 2; vgl. *Kirchbacher*, StPO15 § 99 Rz 6 f (Stand 15.11.2023, rdb.at)).

Das **verfassungsgesetzlich abgesicherte Beschleunigungsgebot** verbietet es zudem den an der Strafverfolgung bzw. am Strafverfahren beteiligten Behörden und Gerichten, eine Verzögerung des Strafverfahrens aus Gründen, die außerhalb des Strafverfahrens angesiedelt sind, herbeizuführen (§ 9 StPO, Art. 6 EMRK, vgl. *Kier* in *Fuchs/Ratz*, WK StPO § 9 Rz 10ff).

Dadurch, dass die Berichtspflicht nach der vorgeschlagenen Bestimmung bis zu 6 Monate aufgeschoben werden kann, wird – anders als nach § 99 StPO – der Staatsanwaltschaft die Möglichkeit genommen, in Ausübung ihrer **Leitungsbefugnis** die Anordnung zu treffen, den Aufschub zu beenden und die kriminalpolizeilichen Ermittlungen einzuleiten (§ 98 StPO). Gleichzeitig wird das Beschleunigungsgebot beeinträchtigt, indem für den Zeitraum von bis zu 6 Monaten die Durchführung von Ermittlungen aufgeschoben wird, was in einem Spannungsverhältnis zum Beschleunigungsgebot steht.

Aus Gründen der Vollständigkeit wird darauf hingewiesen, dass in dem vorgesehenen Bericht an die Staatsanwaltschaft über den Aufschub der Ermittlungen auch die Gründe für diesen

enthalten sein müssen. Dazu müssten der Sachverhalt und die Erwägungen nachvollziehbar dargelegt werden, wodurch nachrichtendienstliche und staatsschutzspezifische Erkenntnisse notwendigerweise zum Inhalt des Ermittlungsaktes (§ 34c StAG) würden, der jedoch spätestens nach allfälligem Ende des Aufschubs der Akteneinsicht durch die Verfahrensparteien unterliegt (vgl. §§ 51, 68 StPO). Die Gründe für eine Beschränkung der Akteneinsicht sind überdies in der StPO abschließend aufgezählt (vgl. 14 Os 82/22y und zuletzt 11 Os 24/23y), einer Beschränkung der Akteneinsicht, die mit einer Behinderung der Wahrnehmung der Rechte Betroffener verbunden ist, aus nachrichtendienstlichen oder staatsschutzspezifischen Gründen stünden überdies EU-rechtliche Vorgaben iHa Beschuldigten- und Opferrechten entgegen.

Da im SNG eine Ausnahme vom Offizialprinzip der StPO durch einen Aufschub von Ermittlungen und der Berichtspflicht festgelegt werden soll, hätte dies zudem Auswirkungen auf die Effizienz der Strafverfolgungen, können sich dadurch doch insbesondere auch **Verjährungsproblematiken** ergeben (vgl. insb. § 57, § 58 Abs. 3 Z 2 StGB).

Letztlich wird die Notwendigkeit des Aufschubs kriminalpolizeilicher Ermittlungen in den Erläuterungen auch nicht näher dargelegt (zB anhand konkreter Fallbeispiele).

Zu Ziffer 5 (§ 11 Abs. 1):

1. Vorauszuschicken ist, dass im Sinne der Ausführungen in der Stellungnahme des Bundesministeriums für Justiz 94/SN-350/ME die Erforderlichkeit und Verhältnismäßigkeit der einzelnen in § 11 Abs. 1 SNG geregelten Maßnahmen und deren Eingriffsvoraussetzungen vornehmlich vom für die Materie zuständigen Bundesministerium für Inneres zu beurteilen sind.

2. In den Erläuterungen wird die Adaptierung der Vorgaben für die bestehenden Ermittlungsbefugnisse in § 11 Abs. 1 Z 1, 2, 3, 5 und 7 SNG mit den neuen Ermittlungsmaßnahmen der Überwachung unverschlüsselter und verschlüsselter Nachrichten gemäß § 11 Abs. 1 Z 8 und 9 SNG 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.

Dies erscheint insoweit unzutreffend, als künftig für den Einsatz der in den 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. Für die (aus datenschutzrechtlicher Sicht gebotene) Einordnung der Ermittlungsmaßnahmen nach Z 8 und 9 als ultima-ratio-Maßnahmen

erscheint dies dagegen nicht erforderlich, da dieses Ergebnis auch durch einen bloßen Entfall der Bezugnahme auf den Einsatz anderer Ermittlungsmaßnahmen in den Z 2, 5 und 7 erreicht werden könnte. Ein Gebot des Gebrauchs gelinderer Ermittlungsmaßnahmen ergibt sich bereits unmittelbar aus dem in § 1 Abs. 2 letzter Satz DSG verankerten Gebot des Einsatzes des gelindesten, zum Ziel führenden Eingriffs (sowie dem in den Erläuterungen angeführten § 29 SPG).

3. Die in § 11 Abs. 1 Z 8 und 9 SNG neu vorgesehene Ermächtigung zur Überwachung von (verschlüsselten) Nachrichten und Informationen ermöglicht weitreichende Eingriffe in das Grundrecht auf Datenschutz (und allgemein die grundrechtlich geschützte Privatsphäre).

Nach der Definition in § 11 Abs. 1 Z 8 SNG 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.

In datenschutzrechtlicher (und allgemein grundrechtlicher) Hinsicht stellt die Überwachung von (verschlüsselten) Nachrichten iSd § 11 Abs. 1 Z 8 und 9 SNG 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 SNG aus Sicht betroffener Personen im Ergebnis ähnlich eingriffsintensiv darstellen wie eine (von der Definition in § 11 Abs. 1 Z 8 SNG 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).

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 SNG sollte die Erforderlichkeit und Verhältnismäßigkeit der Ermittlungsmaßnahmen nochmals eingehend geprüft werden.

4. 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 Stellungnahme des Bundesministeriums für Justiz 94/SN-350/ME dargelegt – nicht beurteilt werden. In datenschutzrechtlicher Hinsicht setzt dies aber jedenfalls voraus, dass die Abgrenzung bereits unmittelbar bei der initialen Verarbeitung (Erfassung) der personenbezogenen Daten (und nicht etwa erst bei deren Ausleitung) erfolgt. Daran würde auch der Umstand einer allfälligen vollautomatisierten Datenverarbeitung bis zur Ausleitung nichts ändern, weil auch dieser vorgelagerte Verarbeitungsvorgang bereits dem betreffenden Verantwortlichen zuzurechnen ist und von der gesetzlichen Grundlage (und gerichtlichen Bewilligung) zur Gänze gedeckt sein muss.

5. Zum Ausnutzen von Sicherheitslücken und damit verbundenen Risiken iHa die Cybersicherheit im Rahmen der Z 9 wird auf die Ausführungen in der Stellungnahme des Bundesministeriums für Justiz 94/SN-350/ME verwiesen.

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. 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 SNG wesentlich, weshalb auf diesen Aspekt in den Erläuterungen näher eingegangen werden sollte.

6. Aus strafprozessualer Sicht wird der Entfall des Verweises auf § 134 Z 3 StPO in den Definitionen der Überwachung (verschlüsselter) Nachrichten in § 11 Abs. 1 Z 8 und 9 SNG ausdrücklich begrüßt.

7. Abschließend wird festgehalten, dass das Bundesministerium für Justiz die Notwendigkeit der Diskussion hinsichtlich einer allf. Lücke in den innerstaatlichen Überwachungsmöglichkeiten durch die Veränderung des Kommunikationsverhaltens und die Verlagerung auf end-to-end-verschlüsselte Messengerdienste selbstverständlich genauso erkennt (siehe Ausführungen in der Stellungnahme des Bundesministeriums für Justiz 94/SN-350/ME, 12).

Zu Ziffer 7 (§ 14 Abs. 2):

Wie bereits in der Stellungnahme des Bundesministeriums für Justiz 94/SN-350/ME dargelegt stellt sich aus datenschutzrechtlicher Sicht die Frage nach dem Mehrwert der aus § 11 Abs. 1 Z 7 letzter Satz SNG in § 14 Abs. 2 SNG verschobenen 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.

Zu Ziffer 8 (§ 14 Abs. 6):

Die Einräumung eines Äußerungsrechts des Rechtsschutzbeauftragten zum Überwachungsprogramm vor der erstmaligen Inbetriebnahme wird ausdrücklich begrüßt. In den Erläuterungen ist zudem festgehalten, dass bei nicht bloß unerheblichen Änderungen der technischen Funktionsweise des Programms im Hinblick auf die Anforderungen nach § 15b Abs. 1 der Rechtsschutzbeauftragte erneut zu befassen ist; dieser Aspekt sollte jedoch auch Eingang in den Gesetzestext finden. Anzumerken ist zudem, dass die Dauer der Äußerungsfrist von zwei Wochen äußerst knapp bemessen scheint.

Zudem wird angeregt eine Ergänzung (zumindest in den Erläuterungen) dahingehend zu prüfen, dass der Rechtsschutzbeauftragte, der in der Regel über einen juristischen Hintergrund verfügt, geeignete Hilfskräfte für diese Prüftätigkeit beiziehen kann, um diese auch effektiv ausüben zu können.

Weiters wird darauf hingewiesen, dass in den Erläuterungen zu § 134 Z 3a StPO idF BGBl. I Nr. 27/2018, ErlRV 17 BgNR 26. GP, 13, auf ein geplantes unabhängiges Audit verwiesen wurde: *„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."

Der gegenständliche Ministerialentwurf sollte in dieser Hinsicht jedenfalls nicht hinter diesen Kautelen zurückbleiben und an Stelle eines (bloßen) Äußerungsrechts des Rechtsschutzbeauftragten ein derartiges unabhängiges Audit der Programmarchitektur in Aussicht genommen werden.

Zu Ziffer 11 (§§ 15a bis 15c):

1. Allgemein wird festgehalten, dass die Aufteilung dieser Bestimmungen auf mehrere übersichtliche Paragraphen begrüßt wird (im Vgl. zu 350/ME XXVVII. GP).

2. Wie bereits in der Stellungnahme des Bundesministeriums für Justiz 94/SN-350/ME ausgeführt sollte aus datenschutzrechtlicher Sicht in den Erläuterungen näher dargelegt werden, welche Angaben in § 15a Abs. 2 Z 8 SNG mit Angaben über „*die beabsichtigte Art des Einsatzes technischer Mittel*" konkret gemeint und wie detailliert diese zu gestalten sind.

3. Zu § 15b Abs. 1: Einleitend wird angemerkt, dass die technische Umsetzbarkeit der gesetzlichen Vorgaben vornehmlich vom do. Bundesministerium zu beurteilen ist.

Um - einen allf. Eindruck von - Missbrauchspotential hintanzustellen wird angeregt weitere gesetzliche Vorgaben zu prüfen, zB Verschlüsselung auf dem Übertragungsweg (zwischen überwachtem Endgerät und DSN) oder weitere Vorkehrungen zur Verhinderung unberechtigter Zugriffe auf erlangte Daten (vgl. § 115k StPO oder detaillierte Regelungen in der TKG-DSVO).

Weiters wird in diesem Zusammenhang angeregt, eine Auseinandersetzung mit dem System der österreichischen Cybersicherheit vorzunehmen, gesetzliche Vorgaben zu treffen und Kriterien festzulegen, die die Auflösung des Spannungsverhältnisses bzw. des Zielkonflikts einer allf. notwenigen Nutzbarmachung von IT-Sicherheitslücken ermöglichen.

Die vorgeschlagene Regelung in § 14 Abs. 6 (Äußerungsrecht des RSB vor der ersten Inbetriebnahme) wird in diesem Zusammenhang ausdrücklich begrüßt.

4. Zu § 15b Abs. 1 Z 3 SNG, demzufolge bei der Durchführung der Ermittlungsmaßnahme nach § 11 Abs. 1 Z 9 SNG technisch sicherzustellen ist, dass das eingebrachte Programm nach Beendigung der Ermittlungsmaßnahme entfernt oder funktionsunfähig wird, wird ebenfalls auf die Stellungnahme des Bundesministeriums für Justiz 94/SN-350/ME hingewiesen.

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. Weiterhin unklar sind zudem die rechtlichen Konsequenzen, wenn sich dies im Zuge einer bereits laufenden Ermittlungsmaßnahme nachträglich als faktisch nicht (mehr) möglich erweisen sollte. § 11 Abs. 1 letzter Satz SNG ordnet zwar an, dass die Ermittlung personenbezogener Daten zu beenden ist, sobald ihre Voraussetzungen wegfallen; § 15b Abs. 1 SNG regelt aber keine Voraussetzungen, sondern Modalitäten der Durchführung der Überwachung von Nachrichten. Für den Fall, dass diese nicht mehr im Einklang mit den in § 15b Abs. 1 SNG geregelten Vorgaben steht, bedürfte es einer dem § 11 Abs. 1 letzter Satz SNG vergleichbaren Regelung.

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

6. Zur in § 15b Abs. 4 Z 1 SNG 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 Stellungnahme des Bundesministeriums für Justiz 94/SN-350/ME verwiesen.

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 allerdings weiterhin keine derartige Verpflichtung zur umgehenden Einholung einer entsprechenden Ermächtigung (und somit Klärung der Zulässigkeit der Weiterverarbeitung) 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.

7. Zu § 15c Abs. 1: Es wird angeregt zu prüfen, ob eine Beschwerdelegitimation des Betroffenen gegen die gerichtliche Bewilligung einzuräumen ist. Gem. § 15c Abs. 1 steht (nur) dem RSB das Recht zu, beim VwGH Revision gegen die Bewilligung des BVwG zu

erheben. Dem Betroffenen oder sonstigen betroffenen Dritten steht – entgegen den EB zu 350/ME XXVVII.GP [1] - kein Beschwerderecht gegen die gerichtliche Bewilligung der Maßnahmen (mehr) zu. Dem Betroffenen stehen lediglich Auskunftsrechte zur Verfügung. Ab dem Zeitpunkt der Verständigung beziehungsweise einer allenfalls bereits zuvor erfolgten Kenntnisnahme steht es dem Betroffenen oder sonstigen betroffenen Dritten frei, eine Beschwerde wegen Verletzung der Bestimmungen über den Datenschutz nach § 90 SPG aufgrund einer behaupteten Verletzung seiner Rechte durch Verarbeiten personenbezogener Daten entgegen den Bestimmungen des DSG geltend zu machen. Ebenso kommt diesen das Recht zur Erhebung einer Beschwerde wegen Verletzung subjektiver Rechte nach § 88 Abs. 2 SPG zu, sofern sie sich, insbesondere durch die Modalitäten der Durchführung der Ermittlungsmaßnahme, in ihren Rechten verletzt erachten. Es sollte geprüft werden, ob daneben noch eine Beschwerdelegitimation weiteren Rechtsschutz böte.

Zu Z 12 (§ 16 Abs. 2 und 3 SNG):

Nach § 16 Abs. 3 iVm Abs. 2 SNG kann die Information von Betroffenen einer Aufgabe nach § 6 Abs. 1 oder 2 SNG bzw. von einer Überwachung von Nachrichten gemäß § 11 Abs. 1 Z 8 oder 9 SNG betroffener Personen 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*“.

Diese Formulierung 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. Nach § 43 Abs. 4 DSG kann die Unterrichtung der betroffenen Person über die Verarbeitung ihrer personenbezogenen Daten bei Vorliegen der dort geregelten Gründe aber stets nur „*soweit und solange aufgeschoben, eingeschränkt oder unterlassen werden, wie dies im Einzelfall unbedingt erforderlich und verhältnismäßig ist*“. Insoweit wäre die Information bei Wegfall von zunächst vorliegenden Gründen des § 43 Abs. 4 DSG umgehend nachzuholen. Hervorzuheben ist, dass die Information der betroffenen Person über die Verarbeitung ihrer personenbezogenen Daten Grundvoraussetzung für die Geltendmachung ihrer Betroffenenrechte ist und daher auch

[1] Aus den Erläuterungen zu 350/ME, 27. GP, Seite 8: „Letztlich kann der Betroffene auch unmittelbar auf Art. 133 Abs. 6 Z 1 B-VG gestützt gegen den bewilligenden Beschluss des BVwG Revision an den Verwaltungsgerichtshof nach Maßgabe der §§ 25a ff VwGG erheben.“

entsprechend gewährleistet sein muss (vgl. idS auch VfGH 14.12.2023, G 352/2021, Rn. 101).

§ 16 Abs. 2 SNG sollte insoweit überarbeitet werden.

Zu Ziffer 14 (§ 17 Abs. 3):

Die vorgeschlagene Berichtspflicht gegenüber dem Ständigen Unterausschuss des Ausschusses für innere Angelegenheiten wird begrüßt, weil sie die Transparenz der Maßnahme erhöht. Der Vollständigkeit wegen wird angemerkt, dass laut WFA jährlich mit nur rund 5 bis 15 Verfahren mit Überwachungen verschlüsselter Nachrichten gerechnet wird.

Zu § 9 SNG:

In § 9 Abs. 1 SNG wird lediglich auf § 157 Abs. 1 Z 2 bis 4 und § 157 Abs. 2 StPO verwiesen. Es wird angeregt zu prüfen, ob die Verweise auf § 144 StPO (Umgehungsverbot) und § 155 StPO (Vernehmungsverbote) auszuweiten sind.

Zur datenschutzrechtlichen Rollenverteilung iZm der Überwachung verschlüsselter Nachrichten:

Zur datenschutzrechtlichen Rollenverteilung iZm der Überwachung verschlüsselter Nachrichten wird auf die Ausführungen in der Stellungnahme des Bundesministeriums für Justiz 94/SN-350/ME verwiesen.

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 gesetzliche Benennung eines Verantwortlicher (siehe Rn. 23-35 des Urteils) auseinandersetzt und auch die Möglichkeit eines allenfalls hinzutretenden faktisch (Mit-)Verantwortlichen (vgl. Rn. 48 des Urteils) anspricht.

Zu Artikel 3 (TKG 2021):

Laut den Erläuterungen sollen mit der Anpassung der Bestimmungen des TKG 2021 die Ausnahmen vom Kommunikationsgeheimnis auf die neuen Ermittlungsmaßnahmen nach

§ 11 Abs. 1 Z 8 und 9 SNG (Überwachung verschlüsselter und unverschlüsselter Nachrichten) erweitert und die erforderliche Mitwirkung der (Kommunikationsdienste)Anbieter an der Nachrichtenüberwachung sichergestellt werden.

Dabei fällt auf, dass die Überwachungsmaßnahmen nach § 11 Abs. 1 Z 8 und 9 SNG in § 162 Abs. 1, 2 und 3 gleichförmig ergänzt werden sollen. Während die Überwachung (unverschlüsselter) Nachrichten in § 162 Abs. 1, 2 und 3 TKG 2021 ergänzt werden soll, soll die Überwachung verschlüsselter Nachrichten nach § 11 Abs. 1 Z 9 SNG nicht in § 162 Abs. 1 TKG 2021 (betreffend die IKEV) und auch nicht in § 162 Abs. 3 TKG 2021 (betreffend die ÜVO) ergänzt werden (nur in § 162 Abs. 2 TKG 2021 – betreffend die ÜKVO).

Es wird angeregt zu prüfen, ob eine Ergänzung von § 11 Abs. 1 Z 9 auch in § 162 Abs. 1 und 3 TKG 2021 zweckmäßig erscheint bzw. notwendig ist.

Zudem bleibt offen, wie die erforderliche Mitwirkung nach § 162 Abs. 2 TKG 2021 mit der Einschränkung auf die eindeutige Zuordnung des Computersystems des Betroffenen erfolgen soll.

Zu Artikel 4 und Artikel 5 (BVwGG und RStDG):

Es fällt auf, dass kein fixes Datum für das Inkrafttreten dieser Bestimmungen, sondern das Inkrafttreten mit dem der Kundmachung folgenden Tag vorgesehen ist. Dagegen ist im Grunde nichts einzuwenden, lediglich im Bereich Sicherheitsüberprüfung könnte eine fehlende Legisvakanz bzw. Übergangsregelung zu Problemen führen. Der Vollständigkeit halber bleibt darauf hinzuweisen, dass sich derzeit bereits das BBG 2025 im Stadium des Begutachtungsverfahrens befindet und darin ebenfalls Änderungen im RStDG enthalten sind. Es könnten daher in Artikel 5 (Änderung des RStDG) möglicherweise noch Änderungen im Einleitungssatz bei der Fundstelle der letzten Änderung sowie bei der Absatzbezeichnung der Inkrafttretensbestimmung notwendig werden, sollte das BBG 2025 früher beschlossen werden als das gegenständliche Vorhaben.

Zur WFA:

Hinsichtlich der WFA ist festzuhalten, dass diese soweit ersichtlich weiterhin auch im Bereich des Bundesministeriums für Inneres keine Zusatzkosten für den Kostenersatz an die Telekomunternehmen für deren Mitwirkung an der Nachrichtenüberwachung gemäß § 11 Abs. 2 SNG ausweist.

Zudem fällt auf, dass bei der Darstellung des Personalaufwandes die 0,5 VBÄ im Bereich v2/4 erst ab dem Jahr 2026 berücksichtigt werden, während die übrigen Personalaufwendungen bereits ab 2025 dargestellt werden.

Dabei handelt es sich möglicherweise um ein Versehen, zumal diese bei der Darstellung der Ausgaben im DB 13.02.07 durchaus berücksichtigt zu sein scheinen. Unter Abzug der nunmehr ausgewiesenen Kosten für den Bereitschaftsdienst sind nämlich dort noch genau die im vorangegangenen Entwurf ausgewiesenen Kosten dargestellt (etwa 2025: im Vorentwurf 134 tsd. Euro zzgl. Bereitschaftsdienst 44 Tsd. Euro = 178 Tsd. Euro).

Das BMF hat bereits im Rahmen des Begutachtungsverfahrens zu 350/ME kritisch angemerkt (37/SN-350/ME), dass in der WFA unter anderem auch die „Zusatzkosten für den Kostenersatz an die Telekomunternehmen für deren Mitwirkung an der Nachrichtenüberwachung *gemäß § 11 Abs. 2 SNG*“ auszuweisen wären.

In diesem Zusammenhang darf angemerkt werden, dass es für den Bereich der Justiz UG 13 wesentlich erscheint, dass dahingehend Einvernehmen besteht, dass weder Kosten*tragung* noch Kosten*ersatz* im Zusammenhang mit der gegenständlichen Novelle Budgetwirksamkeit für die Justiz entfalten und dies in der WFA unmissverständlich zum Ausdruck kommt.

4. Juni 2025
Für die Bundesministerin:
Dr. Fritz Zeder

Elektronisch gefertigt

REPUBLIK ÖSTERREICH BMJ SIGNATUR	**Datum/Zeit**	2025-06-04T10:07:15+02:00
	Hinweis	Dieses Dokument wurde elektronisch signiert. Auch ein Ausdruck dieses Dokuments hat die Beweiskraft einer öffentlichen Urkunde.
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: www.justiz.gv.at/amtssignatur