Erläuterungen

Allgemeiner Teil

1. Hauptgesichtspunkte des Entwurfs:

Mit dieser Novelle soll 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.

Andererseits hat 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.

Weiters soll 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, wenn die bestehenden Ermittlungsmaßnahmen zur Vorbeugung des befürchteten verfassungsgefährdenden Angriffs aussichtslos sind.

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.

Außerdem handelt 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.

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

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

2. Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung eines diesem Entwurf entsprechenden Bundesgesetzes gründet sich auf Art. 10 Abs. 1 Z 1 („Verwaltungsgerichtsbarkeit“), Z 6 („Strafrechtswesen“), Z 7 („Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit“), Z 9 („Post- und Fernmeldewesen“) und Z 16 („Dienstrecht und Personalvertretungsrecht der Bundesbediensteten“) des Bundes-Verfassungsgesetzes – B-VG, BGBl. Nr. 1/1930.

3. Besonderheiten des Normerzeugungsverfahrens:

Da in den §§ 15a ff die Zuständigkeit des Bundesverwaltungsgerichtes zur Entscheidung über Anträge in sonstigen Angelegenheiten im Sinne des Art. 130 Abs. 2 Z 4 B-VG vorgesehen wird, darf das vorgeschlagene Bundesgesetz gemäß Art. 131 Abs. 4 Z 2 lit. d iVm Abs. 4 letzter Satz B-VG nur mit Zustimmung aller neun Länder kundgemacht werden.

Besonderer Teil

Zu Art. 1 (Änderung des Staatsschutz- und Nachrichtendienst-Gesetzes)

Zu Z 1 (§ 2a Abs. 1):

Im Rahmen des Begutachtungsverfahrens wurden wiederholt Bedenken hinsichtlich der Doppelstellung der Direktion einerseits als ermittelnde Stelle und andererseits als überprüfende Stelle hinsichtlich der Durchführung der Vertrauenswürdigkeitsprüfungen des Rechtsschutzbeauftragten sowie der betroffenen Bundesverwaltungsrichter, denen künftig unter anderem die Kontrolle beziehungsweise Bewilligung von Nachrichtenüberwachungen nach § 11 Abs. 1 Z 8 und 9 obliegen soll, geäußert. Um diesem Spannungsverhältnis Rechnung zu tragen, soll nunmehr ausdrücklich angeordnet werden, dass sämtliche Vertrauenswürdigkeitsprüfungen durch eine Organisationseinheit der Direktion, die von den operativen Organisationseinheiten der Aufgabenbereiche Staatsschutz sowie Nachrichtendienst getrennt ist, vorzunehmen sind. Durch diese strikte organisatorische Trennung wird das Risiko einer allfälligen Einflussnahme auf die Rechtsstellung und das Tätigwerden des Rechtsschutzbeauftragten sowie des Bundesverwaltungsgerichts durch die von deren Kontrolle betroffenen Organisationseinheiten der Direktion minimiert.

Zu Z 2 und 3 (§ 6 Abs. 3 Z 3 und 4):

Es handelt sich um Ergänzungen des Deliktskatalogs der Z 3 und 4 um die für den Verfassungsschutz relevanten Tatbestände des Strafgesetzbuches „Religiös motivierte extremistische Verbindung“ in § 247b StGB und „Überlieferung an eine ausländische Macht“ in § 103 StGB, um die Qualifikation des § 50 Abs. 1a des Waffengesetzes 1996, welcher insbesondere den illegalen Waffenhandel unter Strafe stellt, sowie § 25 Abs. 1 und 2 des Investitionskontrollgesetzes – InvKG, BGBl. I Nr. 87/2020, der im Wesentlichen die Deliktstatbestände, die vor Inkrafttreten des InvKG in § 79 Abs. 1 Z 25 und 26 des Außenwirtschaftsgesetzes 2011 – AußWG 2011, BGBl. I Nr. 26/2011, abgebildet waren, ersetzt hat.

Zu Z 4 (§ 6 Abs. 4 und 5):

Zu § 6 Abs. 4:

Bislang sah § 6 Abs. 4 nur die Möglichkeit eines besonderen Aufschubs kriminalpolizeilicher Berichtspflichten für Organe des öffentlichen Sicherheitsdienstes im Bereich des Verfassungsschutzes vor. Nicht geregelt war jedoch, wie bei Zusammentreffen einer Aufgabe nach § 6 Abs. 1 oder 2 mit (sonstigen) sicherheits- oder kriminalpolizeilichen Aufgaben vorzugehen ist. Die bestehenden Regelungen zum Aufschub sicherheitspolizeilichen Einschreitens nach § 23 SPG oder kriminalpolizeilicher Ermittlungen nach § 99 Abs. 4 StPO, welche nach einer Interessenabwägung einen Aufschub gemäß § 23 SPG nur zur Abwehr krimineller Verbindungen oder Verhinderung von bestimmten bereits geplanten Verbrechen bzw. gemäß § 99 Abs. 4 Z 1 StPO zur Aufklärung einer wesentlich schwerer wiegenden Straftat oder Ausforschung eines führend Beteiligten erlauben, berücksichtigen die relevanten Aufgaben des Verfassungsschutzes nicht und erschweren damit eine effiziente Bekämpfung verfassungsgefährdender Strukturen. Aus diesem Grund soll § 6 Abs. 4 eine Überarbeitung erfahren, um auch hinsichtlich der Aufgaben des Verfassungsschutzes das sicherheitspolizeiliche Einschreiten oder kriminalpolizeiliche Ermittlungen aufschieben zu können.

Künftig sollen daher nach dem Vorbild der maßgeblichen Bestimmungen in § 23 SPG sowie § 99 Abs. 4 f StPO die Organe des öffentlichen Sicherheitsdienstes der Organisationseinheiten gemäß § 1 Abs. 3 von sicherheitspolizeilichem Einschreiten Abstand nehmen oder kriminalpolizeiliche Ermittlungen aufschieben können, soweit jeweils ein überwiegendes Interesse an der Erfüllung der Aufgabe nach § 6 Abs. 1 oder 2 besteht; das Interesse an der Aufgabenerfüllung nach § 6 Abs. 1 oder 2 muss dabei eindeutig und offenkundig überwiegen (vgl. *Pilnacek*/*Pleischl* in *Fuchs*/*Ratz*, WK StPO, Vorverfahren § 99 Rz 402). Es kommt immer auf die Abwägung und Beurteilung im Einzelfall an (vgl. *Vogl* in *Fuchs*/*Ratz*, WK StPO § 99 Rz 13).

Das sicherheitspolizeiliche Einschreiten (Vorbeugung oder Beendigung gefährlicher Angriffe) durch Organe des öffentlichen Sicherheitsdienstes darf jedenfalls nur aufgeschoben werden, solange keine Gefahr für Leben und Gesundheit Dritter besteht und dafür Vorsorge getroffen ist, dass ein aus der Tat entstehender Schaden zur Gänze gutgemacht wird (§ 23 Abs. 2 SPG). § 23 Abs. 3 SPG gilt.

Ein Aufschub kriminalpolizeilicher Ermittlungen setzt voraus, dass – bei gebotener ex-ante Betrachtung – mit dem Aufschub keine ernste Gefahr für Leben, Gesundheit, körperliche Unversehrtheit oder Freiheit Dritter verbunden ist (vgl. § 99 Abs. 4 StPO).

Die Gründe für die Abstandnahme von sicherheitspolizeilichem Einschreiten oder den Aufschub kriminalpolizeilicher Ermittlungen sind zu dokumentieren und im zweiten Fall unverzüglich der

Staatsanwaltschaft als Bericht gemäß § 100 StPO zu übermitteln. Denn wenngleich die Befugnis zum Aufschub kriminalpolizeilicher Ermittlungen der Kriminalpolizei grundsätzlich aus eigenem zusteht, kann mit dem Aufschub zumindest ein vorläufiger Verzicht auf die Strafverfolgung verbunden sein (vgl. EBRV StPRG 131; *Pilnacek*/*Pleischl* in *Fuchs*/*Ratz*, WK StPO, Vorverfahren § 99 Rz 404), sodass eine Information der Staatsanwaltschaft unverzüglich zu erfolgen hat, um ihr die Wahrnehmung ihrer Leitungsfunktion zu ermöglichen. In diesem Sinne kann die Staatsanwaltschaft nach erfolgtem Bericht, 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 aufzunehmen (*Vogl* in *Fuchs*/*Ratz*, WK StPO § 99 Rz 15).

Zu § 6 Abs. 5:

Gemäß der strikten Aufgabenzuweisung in § 1 Abs. 4 obliegt die Aufgabe der erweiterten Gefahrenerforschung zur Beobachtung einer Gruppierung (§ 6 Abs. 1) der für den Aufgabenbereich Nachrichtendienst zuständigen Organisationseinheit der Direktion und der vorbeugende Schutz vor verfassungsgefährdenden Angriffen durch Einzelpersonen (§ 6 Abs. 2) den für den Aufgabenbereich Staatsschutz zuständigen Organisationseinheiten (§ 1 Abs. 3). Zur Koordinierung dieser beiden Aufgabenbereiche ist innerhalb der Direktion eine Informationsschnittstelle eingerichtet, welcher insbesondere der tagesaktuelle und anlassbezogene Informations- und Lageaustausch, die Bewertung von Informationen sowie die Abstimmung strategischer und operativer Maßnahmen obliegt (§ 2 Abs. 1).

Allerdings hat die Praxis seit Inkrafttreten des SNG gezeigt, dass diese strikte Aufgabenzuweisung trotz Einrichtung der Informationsschnittstelle eine rasche, zweckmäßige und effiziente Aufgabenerfüllung in gewissen Fallkonstellationen erschweren kann (vgl. auch *Salimi*, Gefährliche Gruppierungen, Rz. 60), weshalb der Direktor im Einzelfall unter gesetzlich festgelegten Kriterien den Aufgabenbereich Nachrichtendienst mit der Wahrnehmung einer Aufgabe nach § 6 Abs. 2 ermächtigen dürfen soll.

Um eine Ermächtigung nach Z 1 erteilen zu können, muss durch den Aufgabenbereich Nachrichtendienst bereits eine Aufgabe der erweiterten Gefahrenerforschung wahrgenommen werden, im Zuge derer sich für eine Einzelperson – aus der Gruppierung gemäß § 6 Abs. 1 – auch die Voraussetzungen des § 6 Abs. 2 ergeben. Wenn eine Übergabe dieser sich neu stellenden Aufgabe gemäß § 6 Abs. 2 an den Aufgabenbereich Staatsschutz im konkreten Anlassfall die Aufgabenerfüllung etwa aufgrund besonderer Dringlichkeit beeinträchtigen oder zu Doppelgleisigkeiten der Ermittlungen führen würde, kann der Direktor im Einzelfall von dieser Ermächtigung Gebrauch machen.

Die Erteilung einer Ermächtigung gemäß Z 2 ist dann zulässig, wenn dem Aufgabenbereich Nachrichtendienst Informationen von Dienststellen inländischer Behörden, ausländischen Sicherheitsbehörden oder Sicherheitsorganisationen übermittelt werden, die eine Aufgabe nach § 6 Abs. 2 begründen, die genannten Informationen aber einer Verarbeitungsbeschränkung unterliegen, sodass diese nach den Vorgaben der übermittelnden Stelle nur von mit nachrichtendienstlichen Aufgaben betrauten Organisationseinheiten verarbeitet werden dürfen. Die Verarbeitungsbeschränkung kann sich unmittelbar aus § 9 PolKG ergeben, aber auch aus vergleichbaren nationalen, internationalen oder bilateralen Verpflichtungen. Die Informationen können sowohl von ausländischen oder internationalen übermittelnden Stellen (zB. ausländische Partnerdienste) als auch von inländischen Behörden (etwa Heeres-Nachrichtenamt oder Abwehramt) stammen.

Voraussetzung für jede Erteilung einer Ermächtigung gemäß Z 1 oder 2 ist es überdies, dass die Wahrnehmung der Aufgabe nach § 6 Abs. 2 durch den Aufgabenbereich Nachrichtendienst im jeweiligen Fall im Interesse der Raschheit und Zweckmäßigkeit geboten ist (vgl. auch § 14 Abs. 3 SPG).

Jede Aufgabenübertragung gemäß Abs. 5 bedarf einer eigenen Ermächtigung des Direktors. Der Direktor hat sowohl den Leiter der Informationsschnittstelle (§ 2 Abs. 1) als auch den Rechtsschutzbeauftragten sogleich bei Beginn und Ende jeder Aufgabenwahrnehmung zu informieren. Dies ist erforderlich, damit einerseits der Leiter der Informationsschnittstelle insbesondere die allenfalls erforderlichen Abstimmungen strategischer und operativer Maßnahmen wahrnehmen kann, andererseits der Rechtsschutzbeauftragte bereits vor einem Ansuchen um Ermächtigung für die Aufgabe informiert ist und diese Information auch in den jährlichen Bericht gemäß § 15 Abs. 4, der auch dem Ständigen Unterausschuss zu übermitteln ist (§ 17 Abs. 4), einfließen lassen kann.

Wird eine entsprechende Ermächtigung durch den Direktor erteilt, ist seitens der für den Aufgabenbereich Nachrichtendienst zuständigen Organisationseinheit nach den herkömmlichen Regelungen des SNG vorzugehen und insbesondere die Ermächtigung des Rechtsschutzbeauftragten für die konkrete Aufgabe nach § 6 Abs. 2 einzuholen (vgl. § 14). In der Meldung an den Rechtsschutzbeauftragten sollte – unter Anführung der einschlägigen Ziffer – auf die erteilte Ermächtigung des Direktors gemäß Abs. 5 Z 1 oder Z 2 hingewiesen werden.

Die Möglichkeit der Ermächtigung der für den Aufgabenbereich Nachrichtendienst zuständigen Organisationseinheit der Direktion zur einzelfallbezogenen Wahrnehmung von Aufgaben des Staatsschutzes ändert nichts an der bestehenden strikten personellen Trennung der Aufgabenbereiche Staatsschutz und Nachrichtendienst. Überdies kommt weiterhin ausschließlich dem Staatsschutz die Wahrnehmung der Aufgaben nach dem SPG und der StPO im Zusammenhang mit verfassungsgefährdenden Angriffen zu (§ 1 Abs. 4). Die Verarbeitung von bereits ermittelten Daten erfolgt auch im Rahmen der Aufgabenübertragung nach den bestehenden Datenverarbeitungsregelungen, vgl. insbesondere § 10 Abs. 2 bzw. § 12.

Zu Z 5 (§ 9 Abs. 1):

Anregungen aus dem Begutachtungsverfahren folgend soll das Ermittlungsverbot für personenbezogene Daten, für die gemäß § 157 Abs. 1 Z 2 bis 4 StPO ein Recht auf Aussageverweigerung besteht, auf Daten, die gemäß § 155 Abs. 1 Z 1 StPO der geistlichen Amtsverschwiegenheit unterliegen, erstreckt werden.

Zu Z 6 (§ 10 Abs. 4):

Durch die gegenständliche Klarstellung soll es den Organisationseinheiten gemäß § 1 Abs. 3 ermöglicht werden, gemäß § 10 Abs. 4 von Rechtsträgern des öffentlichen oder privaten Bereichs mittels Einsatzes von Bild- und Tonaufzeichnungsgeräten übergebene Daten, auch dann zu verarbeiten, wenn darauf neben Bild- auch Tondaten, wie es bei Videoaufnahmen zunehmend üblich ist, enthalten sind; vgl. auch die diesbezüglich korrespondierende Norm in § 53 Abs. 5 SPG.

Zu Z 7, 8 und 9 (§ 11 Abs. 1):

Mit der Ergänzung der Ermittlungsmaßnahme nach Z 5 soll eine Anpassung an die korrespondierende Bestimmung der StPO (§ 134 Z 2a StPO) erfolgen, in der mit BGBl. I Nr. 27/2018 eine Legaldefinition zur Lokalisierung einer technischen Einrichtung eingeführt wurde. Durch die Einführung einer Legaldefinition sollte klargestellt werden, dass es sich bei der Lokalisierung einer technischen Einrichtung um den Einsatz technischer Mittel zur Feststellung von geografischen Standorten und der zur internationalen Kennung des Benutzers dienenden Nummer ohne Mitwirkung des Anbieters (oder sonstigen Diensteanbieters) handelt. Diese Klarstellung soll nunmehr auch für den Bereich des Staatsschutzes und Nachrichtendienstes nachgezogen werden.

Mit der gegenständlichen Änderung der Z 7 soll außerdem eine Rechtsgrundlage für den Einsatz von technischen Mitteln, insbesondere WLAN-Catchern, geschaffen werden, mit deren Hilfe die Ermittlung von Verkehrs-, Zugangs- und Standortdaten ohne Einbeziehung von Betreibern öffentlicher Telekommunikationsdienste (§ 160 Abs. 3 Z 1 TKG 2021) und sonstigen Diensteanbietern (§ 3 Z 2 ECG) ermöglicht werden soll.

Für den Einsatz technischer Mittel nach Z 5 und Z 7 ist nach den herkömmlichen Regelungen des SNG eine Ermächtigung des Rechtsschutzbeauftragten einzuholen (vgl. § 14).

Zu Z 10 und 11 (§ 11 Abs. 1 Z 8 und 9 sowie Abs. 2 und 3):

Bislang ermöglicht das SNG den Verfassungsschutzbehörden im Hinblick auf Telekommunikation lediglich die Ermittlung von Verkehrsdaten, Kommunikationsinhaltsdaten können dahingegen nicht ermittelt werden. Praktische Erfahrungen im Zusammenhang mit dem vorbeugenden Schutz vor verfassungsgefährdenden Angriffen – insbesondere im Hinblick auf die Abwehr geplanter terroristischer Anschläge – sowie der internationale Vergleich haben allerdings gezeigt, dass das Fehlen einer Möglichkeit zur Überwachung des Kommunikationsverkehrs eine effiziente Aufgabenerfüllung der Verfassungsschutzbehörden unmöglich macht. So steht etwa in Deutschland die Überwachung der Inhalte sowohl von konventioneller wie auch verschlüsselter Kommunikation nicht nur den Strafverfolgungsbehörden, sondern auch den Sicherheitsbehörden und Nachrichtendiensten zur Verfügung. Da ohne die Überwachung von Inhaltsdaten keine konkreten Hinweise auf bevorstehende verfassungsgefährdende Angriffe – etwa hinsichtlich potentieller (Mit-)Täter, Art und Weise des drohenden Angriffs, Begehungsorte oder -zeitpunkte – gewonnen werden können, sind die österreichischen Verfassungsschutzbehörden, mangels Substituierbarkeit der Inhaltsüberwachung durch bestehende Ermittlungsmaßnahmen, in vielen Fällen auf Informationen von Partnerdiensten angewiesen, die mitunter aufgrund ihrer Klassifizierung nur eingeschränkt für Strafverfolgungszwecke verwendet werden können.

Aus diesen Gründen sollen nunmehr die Rechtsgrundlagen 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 auch eine Rechtsgrundlage

für die Überwachung verschlüsselter Nachrichten zur effektiven Bekämpfung von verfassungsschutzrelevanten Bedrohungslagen geschaffen werden. In diesem Sinne betont auch die Richtlinie (EU) 2017/541 zur Terrorismusbekämpfung und zur Ersetzung des Rahmenbeschlusses 2002/475/JI des Rates und zur Änderung des Beschlusses 2005/671/JI des Rates, ABl. Nr. L 88 vom 31.3.2017 S. 6, (im Folgenden: Terrorismus-RL) die Bedeutung der Zurverfügungstellung wirksamer Ermittlungsinstrumente, wie insbesondere der Überwachung des Kommunikationsverkehrs, für die Bekämpfung terroristischer Straftaten (Art. 20 sowie Erwägungsgrund 21 der Terrorismus-RL). In dem rezenten Erkenntnis des VfGH zur Sicherstellung und Auswertung von Datenträgern trägt das Höchstgericht ebenso dem Umstand Rechnung, dass „*staatliches Handeln durch die rasche Verbreitung der Nutzung neuer Kommunikationstechnologien in vielerlei Hinsicht vor besondere Herausforderungen gestellt wurde und wird.*“ Dieses geänderte Umfeld ist nach der Rechtsprechung des VfGH auch maßgeblich bei der Beurteilung der Befugnisse zu berücksichtigen (VfGH vom 14. Dezember 2023, G 352/2021 Rn 2.2.8.).

In Anbetracht dieser Erwägungen und unter Berücksichtigung jener Argumentationslinien, die den Verfassungsgerichtshof mit Erkenntnis vom 11. Dezember 2019, G 72-74/2019, G 181-182/2019, zur Aufhebung der strafprozessualen Ermittlungsmaßnahme der „Überwachung verschlüsselter Nachrichten“ gemäß § 135a StPO idF BGBl. I Nr. 27/2018 aufgrund die Verhältnismäßigkeit nicht wahrender Ausgestaltung (*Schmoller* zu OGH 15 Os 13/23k, JBl 2023, 145, 744) veranlasst haben, soll zur Vorbeugung bestimmter, besonders schwerwiegender verfassungsgefährdender Angriffe durch die Einführung von § 11 Abs. 1 Z 8 und 9 die Überwachung sowohl unverschlüsselter als auch verschlüsselter Nachrichten im Rahmen dieses Gesetzes ermöglicht werden. Der im zitierten Erkenntnis geäußerten Ansicht des VfGH, eine derartige verdeckte Überwachung verschlüsselter Nachrichten dürfe nur in Bezug auf Straftaten erfolgen, die im Einzelfall eine gravierende Bedrohung der in Art. 8 Abs. 2 EMRK genannten Ziele darstellen und die einen solchen schwerwiegenden Eingriff rechtfertigen (vgl. Rn. 190), wird durch folgende Vorkehrungen Rechnung getragen:

Bereits durch die Verortung gegenständlicher Ermittlungsmaßnahmen im SNG wird eine Beschränkung ihres Anwendungsbereichs auf die Zwecke des Verfassungsschutzes erzielt. Dabei soll die Überwachung sowohl von unverschlüsselten als auch verschlüsselten Nachrichten auf die Vorbeugung gesetzlich determinierter, besonders schwerwiegender verfassungsgefährdender Angriffe durch einen Betroffenen nach § 6 Abs. 2 beschränkt sein. Unter derartigen Angriffen sind ausschließlich verfassungsgefährdende Angriffe, die im Falle ihrer Verwirklichung zumindest mit bis zu zehn Jahren Freiheitsstrafe bedroht wären oder den Tatbestand des § 256 StGB („Geheimer Nachrichtendienst zum Nachteil Österreichs“) erfüllen würden, zu verstehen. Die sachliche Notwendigkeit für die Aufnahme des Tatbestandes des § 256 StGB gründet sich – unabhängig von dessen Strafdrohung – auf den besonderen Deliktstypus und ist vor dem Hintergrund der geopolitischen Entwicklungen – etwa dem Angriffskrieg Russlands auf die Ukraine – besonders bedeutend. In den vergangenen zwei Jahren konnte eine Zunahme von Spionageaktivitäten in Österreich festgestellt werden. Überdies können Spionageaktivitäten auch transnationale Repressionen – insbesondere politische Verfolgung, die von autoritären Staaten außerhalb ihres Staatsgebietes ausgeübt wird – zum Ziel haben, womit eine Gefahr für Leib, Leben und Freiheit der Betroffenen verbunden sein kann. Klassisches Anwendungsbeispiel der vorgeschlagenen Ermittlungsmaßnahmen gemäß § 11 Abs. 1 Z 8 und 9 wäre etwa die Vorbeugung von Tötungs- oder schweren Körperverletzungsdelikten, die geeignet sind, eine schwere oder längere Zeit anhaltende Störung des öffentlichen Lebens herbeizuführen, und mit dem Vorsatz begangen werden, die Bevölkerung auf schwerwiegende Weise einzuschüchtern, öffentliche Stellen oder eine internationale Organisation zu einer Handlung, Duldung oder Unterlassung zu nötigen oder die politischen, verfassungsrechtlichen, wirtschaftlichen oder sozialen Grundstrukturen eines Staates oder einer internationalen Organisation ernsthaft zu erschüttern oder zu zerstören (vgl. § 278c Abs. 1 Z 1 und 2 StGB). Durch diese hohe Schwelle ist gewährleistet, dass eine Überwachung von Nachrichten nach dem SNG nur dann erfolgt, wenn sie zur Vorbeugung von verfassungsgefährdenden Angriffen dient, deren Verwirklichung im Einzelfall eine gravierende Bedrohung der in Art. 8 Abs. 2 EMRK genannten Ziele darstellt und einen solchen Eingriff rechtfertigt. Wenngleich dem Erkenntnis des Verfassungsgerichtshofs zu G 72-74/2019, G 181-182/2019, zu entnehmen ist, dass die Schwelle für die Zulässigkeit der Überwachung konventioneller Kommunikation geringer sein kann als bei Überwachung verschlüsselter Kommunikation, sollen in Anbetracht der in diesem Bereich gänzlich Neuland betretenden sicherheitspolizeilichen Ermittlungsmaßnahmen die engen Voraussetzungen sowohl für die Überwachung verschlüsselter (Z 9) als auch unverschlüsselter Kommunikation (Z 8) gelten.

Die Definition der neuen Ermittlungsmaßnahmen knüpft an die Legaldefinition der „Überwachung von Nachrichten“ in § 134 Z 3 StPO an und orientiert sich damit an den für den strafprozessualen Bereich bereits etablierten Begriffsbestimmungen, angepasst an den Bedarf des Verfassungsschutzes. Gegenstand der Überwachung nach Z 8 und 9 dürfen demnach lediglich über ein Kommunikationsnetz (§ 4 Z 1

TKG 2021) oder einen Dienst der Informationsgesellschaft (§ 1 Abs. 1 Z 2 des Notifikationsgesetzes) (unverschlüsselt oder verschlüsselt) gesendete, übermittelte oder empfangene Nachrichten und Informationen sein. Abweichend von §134 Z 3 StPO ist vom Begriff der „Nachricht“ auch die autonome Kommunikation zweier Endgeräte ohne menschliches Zutun (M2M-Kommunikation) inklusive der Datenübermittlung an Server im Rahmen von automatisierten Backups erfasst.

Eine Online-Durchsuchung des gesamten Computersystems inklusive lokal abgespeicherter Daten ist sowohl aufgrund der ausdrücklichen Eingrenzung auf Nachrichten, die mit einem Übertragungsvorgang in Zusammenhang stehen, als auch der in § 15a Abs. 3 festgelegten Beschränkung der gerichtlichen Bewilligung der Maßnahme auf jene Applikationen sowie jenen künftigen Zeitraum, der zur Erfüllung der Aufgabe nach § 6 Abs. 2 voraussichtlich erforderlich ist, nicht zulässig. In diesem Sinne ist auch im Rahmen der Durchführung einer Ermittlungsmaßnahme nach Z 9 gemäß § 15b Abs. 1 Z 1 technisch sicherzustellen, dass von der eingesetzten Software ausschließlich innerhalb des seitens des Bundesverwaltungsgerichtes festgelegten Bewilligungsumfangs und -zeitraums gesendete, übermittelte oder empfangene Nachrichten und Informationen iSd § 134 Z 3 StPO überwacht werden können.

Von der Überwachung erfasst sind daher neben der herkömmlichen (Sprach- und SMS-)Telekommunikation sowohl sämtliche Nachrichten und Informationen, die über internetbasierte Apps wie WhatsApp, Telegram etc. übermittelt werden, als auch über einen Cloud-Diensteanbieter an einen Cloud-Server übermittelte Datenpakete, zumal auch hier eine Übermittlung an einen anderen Server stattfindet. Durch das ausdrückliche Abstellen auf einen Übertragungsvorgang ist hingegen die Überwachung von lokal gespeicherten Daten nicht umfasst.

Hinsichtlich der technischen Durchführung der Überwachung unverschlüsselt kommunizierter Nachrichten gemäß Z 8 kann auf die im Rahmen des Vollzugs der Ermittlungsmaßnahme nach § 134 Z 3 StPO gesammelten Erfahrungswerte und die hierfür geschaffenen technischen Strukturen zurückgegriffen werden. Die Ausleitung der im Rahmen der Kommunikationsverbindung bei dem Betreiber des verwendeten Kommunikationsnetzes oder sonstigen Dienstes der Informationsgesellschaft anfallenden Nachrichten und Informationen erfordert bei unverschlüsselten Nachrichten keinen zusätzlichen Eingriff in das Kommunikationsmedium der zu überwachenden Person. Für die Überwachung verschlüsselter Datenströme gemäß Z 9 bedarf es dahingegen zusätzlich des Einbringens eines Programms in das betreffende Computersystem, um end-to-end verschlüsselt gesendete, übermittelte oder empfangene Nachrichten und Informationen noch vor deren Verschlüsselung bzw. nach deren Entschlüsselung ermitteln zu können. Durch das Programm werden somit ausschließlich jene Kommunikationsinhalte und damit in Zusammenhang stehende Daten lesbar gemacht, die auch bisher schon im Rahmen einer Überwachung von Nachrichten nach § 134 Z 3 StPO ermittelt werden können. Ziel der Ermittlungsmaßnahme nach Z 9 ist daher die Überwachung von via „Messengerdiensten“ (z.B.: WhatsApp, Telegram etc.) verschlüsselt übermittelten Nachrichten. Unter „Computersystem“ im Sinne des § 74 Abs. 1 Z 8 StGB sind sowohl einzelne als auch verbundene Vorrichtungen, die der automationsunterstützten Datenverarbeitung dienen, zu subsumieren. Die Ermittlungsmaßnahmen erfassen somit nicht nur den klassischen Computerbegriff, sondern auch andere Geräte, die eine Internetverbindung ermöglichen, wie insbesondere Smartphones und Tablets. Durch den Verweis auf die Definition des StGB soll insbesondere die Schaffung verwechslungsanfälliger neuer Terminologien vermieden werden.

Bei dem zur Überwindung der Transportverschlüsselung einzubringenden Programm handelt es sich um eine Software, die Nachrichten und Informationen noch vor deren Verschlüsselung bzw. nach der Entschlüsselung im Rahmen der Vorgänge des Sendens, Übermittelns und Empfangens ausleiten kann. Vor ihrer Einbringung ist die Software individuell auf das zu überwachende Computersystem – insbesondere unter dem Gesichtspunkt, die Überwachung auf das zur Erfüllung der Aufgabe unbedingt erforderliche Ausmaß zu beschränken und die Einhaltung der Beschränkungen des § 15b Abs. 1 sicherzustellen – abzustimmen. Zu diesem Zweck ist vorab insbesondere eine Eingrenzung der Zugriffsmöglichkeiten der Software auf bestimmte Kommunikationsapplikationen zu prüfen. Zur anschließenden Einbringung des Programms ohne Kenntnisnahme des Betroffenen dürfen technische Mittel eingesetzt werden, nicht jedoch neue Sicherheitslücken durch die Direktion geschaffen. Ebenso wenig gibt es – mangels Mitwirkungsverpflichtung der Anbieter im Rahmen von § 11 Abs. 1 Z 9 – eine Verpflichtung für Anbieter, bestehende Sicherheitslücken offenzuhalten. Im Rahmen einer remote-Einbringung, bei der kein physischer Zugriff auf das zu überwachende Gerät stattfindet, kommt insbesondere der eindeutigen Zuordnung des Zielcomputersystems zum Betroffenen vor und während der Maßnahme, beispielsweise durch entsprechende begleitende Ermittlungsmaßnahmen wie Observation oder eindeutige Identifikation durch Mac-Adresse, Seriennummer, Geräte-ID, IMSI- oder IMEI-Nummer oder individuelle IP-Adresse, besondere Bedeutung zu. Durch diese vorbereitenden Maßnahmen soll vorab eruiert werden, mit welchem Zielgerät und über welche Kommunikationskanäle der Betroffene

primär kommuniziert. Das Computersystem gemäß Abs. 1 Z 9, in das ein Programm zur Überwindung der Verschlüsselung eingebracht werden soll, muss sich demnach längerfristig (zumindest) in der Verfügungsgewalt des Betroffenen nach § 6 Abs. 2 befinden, sodass eine Überwachung öffentlich zugänglicher Computersystem oder solcher von unbeteiligten Dritten ausgeschlossen ist. Die einzubringende Software ist technisch regulierbar, sodass nur gezielte und von der Bewilligung umfasste Nachrichten aus bestimmten Applikationen ausgeleitet werden können. Zum Zweck der Eruierung dieser Identifikationsdaten wird dem Einsatz einer Ermittlungsmaßnahme nach Z 8 oder 9 regelmäßig die Ermittlung personenbezogener Daten insbesondere durch Observation und Anfrage an Betreiber öffentlicher Telekommunikationsdienste und sonstige Diensteanbieter nach Maßgabe der Z 5 und 7 vorangehen. Ein Eindringen in vom Hausrecht geschützte Räume oder Durchsuchen von Behältnissen zwecks Installation des Programms ist nicht zulässig.

Die Überwachung konventioneller wie auch verschlüsselt kommunizierter Nachrichten ist überdies nur zulässig, wenn die Erfüllung der Aufgabe durch Einsatz anderer Ermittlungsmaßnahmen aussichtslos wäre. Diesbezüglich gilt nach den allgemeinen Verhältnismäßigkeitsgrundsätzen (vgl. § 29 SPG) – wie auch für sämtliche bestehende Ermittlungsbefugnisse des § 11 Abs. 1 – dass eine Ermittlungsmaßnahme jeweils nur dann zulässig ist, wenn sämtliche weniger eingriffsintensiven Maßnahmen aussichtslos erscheinen. Die Überwachung von Nachrichten ist gegenüber den bestehenden Ermittlungsmaßnahmen jedenfalls als eingriffsintensivste Maßnahme zu betrachten, sodass sie nur als ultima ratio, mithin nur im Falle der Aussichtslosigkeit aller anderen Ermittlungsmaßnahmen, zum Einsatz kommt. Die Zulässigkeit der Überwachung von Nachrichten gemäß Z 8 zur Durchführung einer Maßnahme nach Z 9 stellt insofern eine notwendige Einschränkung des ultima-ratio-Erfordernisses dar, als die Überwachung nach Z 8 für die Eruierung, welche Kommunikationskanäle der Betroffene nutzt, und somit die treffsichere Einbringung des Programms zur Überwachung verschlüsselt gesendeter, übermittelter oder empfangener Nachrichten unbedingt erforderlich ist. Diese Ausnahme ermöglicht es somit nur, die Maßnahme nach Z 8 auch in jenen Fällen einzusetzen, in denen sie selbst hinsichtlich der Inhaltsüberwachung von Nachrichten zwar nicht erfolgsversprechend erscheint, weil beispielsweise durch (verdeckte) Observation bereits festgestellt werden konnte, dass der Betroffene ausschließlich verschlüsselt kommuniziert, aber Voraussetzung für die erfolgreiche Überwachung verschlüsselter Nachrichten ist. Eine über die Feststellung der verwendeten Kommunikationskanäle zum zielgerichteten Einsatz der Nachrichtenüberwachung nach Z 9 hinausgehende Grundlage für den Einsatz einer Nachrichtenüberwachung wird durch den letzten Halbsatz der Z 8 ebenso wenig bezweckt, wie eine allfällige Mitwirkungsverpflichtung der Anbieter an der Durchführung einer Überwachung nach Z 9, da diese gemäß § 11 Abs. 2 auf die Überwachung nach Z 8 beschränkt ist.

Aufgrund der Einführung der neuen Ermittlungsmaßnahme gemäß Abs. 1 Z 8 sind auch die Abs. 2 und 3, die die Mitwirkungs- und Verschwiegenheitspflichten der ersuchten Stellen sowie die einschlägigen Kostenersatzbestimmungen enthalten, anzupassen. Wie auch schon im Rahmen der bestehenden Ermittlungsmaßnahmen des § 11 Abs. 1 sind Kosten, die Anbietern im Rahmen einer Mitwirkung an der Überwachung von Nachrichten entstehen, nach Maßgabe der Überwachungskostenverordnung – ÜKVO, BGBl. II Nr. 322/2004, vom Bundesministerium für Inneres zu ersetzen. Überdies haben die Erfahrungen der Vergangenheit gezeigt, dass die Verpflichtung der ersuchten Stelle, mit der Ermächtigung verbundene Tatsachen und Vorgänge gegenüber Dritten geheim zu halten, auch auf die Einholung von Auskünften nach § 11 Abs. 1 Z 5 erstreckt werden muss.

Zu Z 12 (§ 14 Abs. 2):

Die bislang in § 11 Abs. 1 Z 7 für die Ermächtigung des Rechtsschutzbeauftragten zur Ermittlung personenbezogener Daten angeordnete Beschränkung auf jenen künftigen oder vergangenen Zeitraum, der zur Erreichung des Zwecks voraussichtlich erforderlich ist, wurde aufgrund systematischer Erwägungen zu den übrigen die Ermächtigung des Rechtsschutzbeauftragten betreffenden Bestimmungen in § 14 Abs. 2 verschoben und anlässlich der Ergebnisse des Begutachtungsverfahrens sprachlich adaptiert.

Zu Z 13 bis 17 (§ 14 Abs. 4, 5 und 6, § 15 Abs. 2 und 3, § 15a, § 15b, § 15c, § 15d sowie § 16 Abs. 2 und 3):

In Anbetracht der spezifischen Eingriffsintensität der neuen Ermittlungsmaßnahmen nach § 11 Abs. 1 Z 8 und 9 sowie der technischen Besonderheiten, die mit der Überwachung verschlüsselter Nachrichten verbunden sind, sollen durch die folgenden Anpassungen – insbesondere die Einführung der besonderen Rechtsschutzbestimmungen der §§ 15a bis 15d – engmaschig flankierende Regelungen, die den Persönlichkeitsschutz und das Grundrecht auf Datenschutz angemessen würdigen, geschaffen werden. Um einen besonders hohen Schutzstandard zu gewährleisten und dem mit diesen Ermittlungsmaßnahmen erstmals verbundenen Eingriff in das unter Richtervorbehalt stehende Fernmeldegeheimnis gemäß

Art. 10a Staatsgrundgesetz – StGG, RGBl. Nr. 142/1867, (die Ermittlung von Verkehrsdaten gemäß § 11 Abs. 1 Z 7 stellt keinen Eingriff in das Fernmeldegeheimnis dar, vgl. auch Pkt. 8.2. des Erkenntnisses des VfGH vom 29. November 2017, G 223/2016) unter formellen Gesichtspunkten entsprechend Rechnung zu tragen, soll im Zuge der Einführung dieser Ermittlungsmaßnahmen ein innerhalb dieses Gesetzes neuartiges Rechtsschutzsystem im Sinne eines besonderen Bewilligungs- und Kontrollverfahrens unter Einbindung des Bundesverwaltungsgerichts (§§ 15a und 15c) sowie des gemäß § 91a SPG beim Bundesminister für Inneres eingerichteten Rechtsschutzbeauftragten (§ 14 Abs. 4 bis 6, § 15c Abs. 1 und 2 sowie § 16) etabliert werden. Die Antragstellung für die Bewilligung und die Durchführung der Maßnahmen obliegt ausschließlich der Direktion, um die Einheitlichkeit des Vollzugs und die Qualitätssicherung durch Bündelung des (technischen) Know-Hows zu gewährleisten sowie die begleitende Kontrolle der Maßnahme durch den Rechtsschutzbeauftragten angesichts deren örtlicher Zentralisierung zu erleichtern.

Beabsichtigt die Direktion die Durchführung einer Überwachung von (verschlüsselten) Nachrichten, hat sie – noch vor ihrem Antrag auf gerichtliche Bewilligung der Maßnahme – den Rechtsschutzbeauftragten zu befassen (§ 14 Abs. 4). Diesem ist durch Mitteilung jener Informationen, die gemäß § 15a Abs. 2 auch einem Antrag an das BVwG zugrunde zu legen wären, binnen einer Frist von drei Werktagen, wobei Samstage nicht als Werktage gelten, Gelegenheit zur Äußerung zu geben (vgl. auch § 91c Abs. 2 SPG). Mit seiner zustimmenden oder ablehnenden Äußerung kann der Rechtsschutzbeauftragte seine Sicht in den Entscheidungsfindungsprozess der Beantragung einer Nachrichtenüberwachung einbringen. Wenngleich seine Äußerung keine direkte Verbindlichkeit hinsichtlich der Entscheidung über die gerichtliche Antragstellung entfaltet, kommt insbesondere einer ablehnenden Stellungnahme im Regelfall normative Kraft aus ihrer Faktizität zu (vgl. *Vogl* in *Thanner/Vogl,* SPG[2] § 91c Rz 15). Durch dieses vorgeschaltete Äußerungsrecht des Rechtsschutzbeauftragten, anstelle seiner bloßen Einbindung im Rahmen des kommissarischen Rechtsschutzes, wird gewährleistet, dass der Rechtsschutzbeauftragte nicht nur die konkrete Durchführung einer Nachrichtenüberwachung kontrollieren und allenfalls ein Rechtsmittel zugunsten des Betroffenen erheben, sondern bereits Bedenken gegen deren Durchführung vorbringen kann und damit zu einer besonderen Wahrung der Verhältnismäßigkeit beiträgt. Gleichzeitig wird durch die Etablierung eines Vier-Augen-Prinzips ein gewisser Qualitätsstandard hinsichtlich der an das BVwG ergehenden Anträge sichergestellt.

Zu § 15a (Bewilligung der Überwachung von Nachrichten):

Nach Äußerung des Rechtsschutzbeauftragten oder Ablauf der Drei-Tages-Frist kann die Direktion einen, zumindest die in § 15a Abs. 2 angeführten Informationen enthaltenden, Antrag auf Bewilligung der Maßnahme an das BVwG stellen. Die mit der Antragstellung und Bewilligung in Zusammenhang stehende Kommunikation zwischen der Direktion und dem BVwG erfolgt im elektronischen Weg über einen sicheren Kommunikationskanal, um ein möglichst hohes Datensicherheitsniveau zu gewährleisten (§ 15c Abs. 5).

Der Antrag hat jedenfalls folgende Bestandteile zu umfassen:

1. den Namen oder sonstige Identifizierungsmerkmale des zu überwachenden Betroffenen nach § 6 Abs. 2, wie etwa Geburtsdatum, Geburtsort, Staatsangehörigkeit oder Wohnanschrift, sowie allenfalls einen Hinweis darauf, dass es sich bei diesem um eine in § 155 Abs. 1 Z 1 oder § 157 Abs. 1 Z 2 bis 4 StPO angeführte Person handelt;
2. die nach § 14 Abs. 2 grundsätzlich erforderliche Ermächtigung des Rechtsschutzbeauftragten für die Aufgabe nach § 6 Abs. 2 und den Zeitraum, für den diese Ermächtigung erteilt wurde, sowie eine allfällige Äußerung des Rechtsschutzbeauftragten nach § 14 Abs. 4. Sofern keine Äußerung des Rechtsschutzbeauftragten vorliegt, muss im Antrag ein Hinweis darauf aufgenommen werden;
3. den befürchteten verfassungsgefährdenden Angriff im Sinne § 11 Abs. 1 Z 8 – somit ein verfassungsgefährdender Angriff nach § 256 StGB oder ein solcher, dessen Verwirklichung zumindest mit bis zu zehn Jahren Freiheitsstrafe bedroht ist – sowie jene Tatsachen, aus denen sich ein begründeter Gefahrenverdacht ergibt;
4. sofern erforderlich die Tatsachen, aus denen sich ergibt, dass die Erfüllung der Aufgabe durch Einsatz anderer Ermittlungsmaßnahmen aussichtslos wäre. Ist eine Ermittlungsmaßnahme nach § 11 Abs. 1 Z 8 zur Durchführung einer Überwachung von Nachrichten nach § 11 Abs. 1 Z 9 unbedingt erforderlich, ist gleichfalls im Antrag ein Hinweis darauf aufzunehmen; ergänzend kann der Antrag auch Informationen zu erforderlichen begleitenden oder vorangegangenen Ermittlungsmaßnahmen, wie etwa Observationen, enthalten;
5. die Identifizierungsmerkmale der gemäß § 11 Abs. 1 Z 8 zu überwachenden technischen Einrichtung (etwa Rufnummer, IMSI- oder IMEI-Nummer oder individuelle IP-Adresse) oder

des gemäß § 11 Abs. 1 Z 9 zu überwachenden Computersystems, aus denen auch auf die Verfügungsgewalt des Betroffenen nach § 6 Abs. 2 geschlossen werden kann. Hinsichtlich des zu überwachenden Computersystems sind jene Parameter zu nennen, die vorab zwecks Einbringung des Programms (beispielsweise durch Einsatz einer Ermittlungsmaßnahme nach § 11 Abs. 1 Z 5 oder 7) in Erfahrung gebracht wurden, wie insbesondere Gerätetyp, Betriebssystem, Mac-Adresse, Seriennummer, Geräte-ID, IMSI- oder IMEI-Nummer oder individuelle IP-Adresse;

6. die begehrte Dauer der Überwachung, wobei diese jedenfalls auf jenen Zeitraum, der für die Erfüllung der Aufgabe unbedingt erforderlich erscheint, längstens jedoch auf drei Monate begrenzt sein sollte (vgl. zur zulässigen Bewilligungsdauer § 15a Abs. 3);
7. die Art der Nachrichtenübertragung (zB. Internet-Kommunikation, E-Mail, Sprachtelefonie, Funk, Fax);
8. bei einer Überwachung gemäß § 11 Abs. 1 Z 9 zusätzlich die beabsichtigte Art des Einsatzes technischer Mittel, deren Einsatz die Einbringung des Programms in das zu überwachende Computersystem ermöglichen soll und die zu überwachenden Applikationen. Das Programm, das in das zu überwachende Computersystem eingebracht werden soll, sowie die Möglichkeit zur Einschränkung desselben auf bestimmte Kommunikationsapplikationen (wie zB. Signal oder WhatsApp) im Sinne des § 15b Abs. 1 sind bereits durch den Rechtsschutzbeauftragten gemäß § 14 Abs. 6 vorab zu prüfen;
9. allenfalls die Tatsachen, aus denen sich ergibt, dass Gefahr im Verzug gemäß Abs. 1 letzter Satz vorliegt und somit eine Bewilligung der Nachrichtenüberwachung durch den Einzelrichter des Bundesverwaltungsgerichtes in Betracht kommt, sowie
10. sofern gemäß § 15d Abs. 1 letzter Satz erforderlich die besonders schwerwiegenden Gründe, die den Eingriff in das Verbot gemäß § 155 Abs. 1 Z 1 StPO oder die nach § 157 Abs. 1 Z 2 bis 4 StPO geschützten Rechte verhältnismäßig erscheinen lassen.

Bei allfälligem Ergänzungsbedarf des Antrags ermöglicht die ausdrückliche Anwendbarkeit des § 13 Abs. 3 AVG die Erteilung von Verbesserungsaufträgen durch das Bundesverwaltungsgericht an die DSN.

Für die Bewilligung der Ermittlungsmaßnahme ist aufgrund bundesgesetzlicher Anordnung in § 15a Abs. 1 gemäß Art. 131 Abs. 4 Z 2 lit. d B-VG das Bundesverwaltungsgericht zuständig. Durch diese im Bereich der Sicherheitspolizei neuartige verwaltungsgerichtliche Bewilligung soll eine unabhängige gerichtliche Kontrolle sowie ein verstärkter Rechtsschutz zur Gewährleistung der Verhältnismäßigkeit und des Grundrechtsschutzes, insbesondere des unter Richtervorbehalt stehenden Fernmeldegeheimnisses gemäß Art. 10a StGG, etabliert werden.

Die Bewilligung der Maßnahme durch das Bundesverwaltungsgericht darf nur in jenem Umfang und für jenen künftigen Zeitraum, der zur Erfüllung der Aufgabe voraussichtlich erforderlich ist, höchstens aber für drei Monate erteilt werden (§ 15a Abs. 3). Im Rahmen des Bewilligungsumfangs ist durch das Bundesverwaltungsgericht – basierend auf der seitens der Direktion im Antrag gemäß Abs. 2 Z 7 angeführten Art der Nachrichtenübertragung und der gem. Z 8 genannten Applikationen – insbesondere festzulegen, welche konkreten Übertragungsarten und Applikationen (z.B. Telegram, WhatsApp etc.) die Nachrichtenüberwachung umfassen soll. Bei der Festlegung des Bewilligungszeitraums hat das BVwG insbesondere die Schwere des befürchteten verfassungsgefährdenden Angriffs sowie die Bestimmtheit jener Anhaltspunkte, die dessen Befürchtung rechtfertigen, zu erwägen. Ist innerhalb des Bewilligungszeitraums eine erneute Einbringung des Programms – insbesondere aus technischen Gründen – erforderlich, muss kein diesbezüglicher neuer Antrag gestellt werden. Verlängerungen der Bewilligung sind zulässig, wobei jeweils erneute, im Sinne des § 15a Abs. 2 begründete Anträge erforderlich sind. Der Beschluss ist in diesem Stadium sowohl der Direktion als auch dem Rechtsschutzbeauftragten zuzustellen, um diesem die ihm nach § 14 Abs. 5 im Rahmen des kommissarischen Rechtsschutzes zukommende Prüfung der Bewilligung sowie die allfällige Erhebung einer Revision zugunsten des Betroffenen nach § 15c Abs. 1 unter den Voraussetzungen des § 25a Verwaltungsgerichtshofgesetz 1985 – VwGG, BGBl. Nr. 10/1985, binnen einer Frist von sechs Wochen, zu ermöglichen; einer allfälligen Revision kommt keine aufschiebende Wirkung zu (§ 30 VwGG). Ein Revisionsrecht gegen den Beschluss des Bundesverwaltungsgerichtes kommt zudem dem Bundesminister für Inneres zu, wobei die Revisionsfrist diesfalls mit der Zustellung des Beschlusses an die Direktion beginnt.

Zu § 14 Abs. 5 und 6 (Rechtsschutz durch den Rechtsschutzbeauftragten):

Dem Rechtsschutzbeauftragten obliegt gemäß § 14 Abs. 5 überdies die Prüfung der gerichtlichen Bewilligung und die begleitende Kontrolle der Durchführung der Nachrichtenüberwachung gemäß § 11 Abs. 1 Z 8 und 9. Im Rahmen dieser begleitenden Kontrolltätigkeit hat er insbesondere darauf zu achten, dass die Grenzen der Bewilligung in zeitlicher Hinsicht eingehalten werden, mithin keine Nachrichten

und Informationen ermittelt werden, die von der Bewilligung nicht gedeckt sind, und die Ermittlungsmaßnahme nur solange durchgeführt wird, als die Verhältnismäßigkeit gewahrt ist. Zur effektiven Ausübung der Kontrolle ist dem Rechtsschutzbeauftragten gemäß § 15 Abs. 1 insbesondere jederzeit Einblick in alle erforderlichen Unterlagen und Aufzeichnungen zu gewähren und umfassend Auskunft zu erteilen; umfasst von dieser technologieneutralen Formulierung sind jedenfalls auch alle erforderlichen Daten und Datenverarbeitungen. Durch diese begleitende Kontrolle soll die Wahrung der Rechte des von der Nachrichtenüberwachung Betroffenen zu einem Zeitpunkt, in dem dieser noch keine Kenntnisse von deren Durchführung hat, gewährleistet werden. Darüber hinaus stehen dem Rechtsschutzbeauftragten weiterhin die herkömmlichen Rechtsschutzmöglichkeiten zur Verfügung.

Ergänzend hat die Direktion gemäß Abs. 5 vor der erstmaligen Inbetriebnahme jenes Programms, das im Rahmen einer Maßnahme nach § 11 Abs. 1 Z 9 in ein Computersystem eingebracht wird, um die Verschlüsselung der Nachrichten und Informationen zu überwinden, den Bundeminister für Inneres zu verständigen. Dieser hat sodann den Rechtsschutzbeauftragten zu informieren, um ihm die Möglichkeit zu geben, vorab zu prüfen, ob das Programm die rechtlichen Anforderungen, insbesondere die technischen Spezifikationen nach § 15b Abs. 1, erfüllt. Hierbei wird insbesondere darauf Bedacht zu nehmen sein, dass die Nachrichtenüberwachung gemäß der Vorgabe des §15b Abs. 1 Z 1 auf die Ausleitung von Nachrichten und Informationen aus einzelnen Applikationen des Zielcomputersystems beschränkt werden kann. Die erstmalige Inbetriebnahme des Programms ist erst nach Ablauf der dem Rechtsschutzbeauftragten eingeräumten dreimonatigen Äußerungsfrist oder einer entsprechenden Äußerung des Rechtsschutzbeauftragten zulässig. Bei Änderungen der technischen Funktionsweise des Programms, insbesondere im Hinblick auf die Anforderungen nach § 15b Abs. 1, ist der Rechtsschutzbeauftragte erneut zu befassen.

Zu § 15b (Besondere Bestimmungen für die Durchführung der Überwachung von Nachrichten):

Neben diesen Rechtsschutzgarantien sind angesichts der mit der Einbringung einer Software zur Überwachung verschlüsselter Kommunikation nach § 11 Abs. 1 Z 9 verbundenen technischen Besonderheiten dieser Ermittlungsmaßnahme ergänzende Schutzvorkehrungen gemäß § 15b Abs. 1 zu treffen. So ist durch entsprechende Programmierung der Software zu gewährleisten, dass ausschließlich innerhalb des Bewilligungsumfangs und -zeitraums gesendete, übermittelte oder empfangene Nachrichten und Informationen überwacht werden können. Um die Überwachung möglichst treffsicher auf ermittlungsrelevante Kommunikationsinhalte zu begrenzen, ist überdies technisch sicherzustellen, dass nur Nachrichten und Informationen aus jenen Applikationen des Zielcomputersystems ausgeleitet werden, die gemäß der gerichtlichen Bewilligung überwacht werden dürfen. Es ist sicherzustellen, dass mit der Durchführung der Überwachung keine über die Installation und die mit der Überwachung notwendigerweise einhergehenden Eingriffe hinausgehenden Veränderungen des zu überwachenden Computersystems inklusive der auf ihm gespeicherten Daten und keine dauerhaften Beschädigungen verbunden sind. Nach Beendigung der Ermittlungsmaßnahme muss sichergestellt sein, dass die eingebrachte Software ohne dauerhafte Beschädigung oder Beeinträchtigung des Computersystems vollständig entfernt oder funktionsunfähig wird. Dies kann in der Praxis durch die Ausgestaltung des Programms mit einem sogenannten „Kill-Switch“ sichergestellt werden, der nach Ablauf der vorgegebenen Frist oder bereits zuvor durch remote-Betätigung (beispielsweise, wenn die Maßnahme vorzeitig zu beenden ist, etwa weil das Gerät weitergegeben wurde und von einer anderen als der Zielperson verwendet wird) die vollständige sichere Löschung der Überwachungssoftware gewährleistet. Ebenso kann in die Software eine laufende Datumsprüfung eingebaut werden, sodass diese bei Erreichen eines bestimmten Datums automatisch gelöscht wird, unabhängig davon, ob eine Verbindung mit dem Internet besteht.

Um die Authentizität und Integrität der erhobenen Nachrichten sowie die Nachverfolgbarkeit deren Ermittlung zu gewährleisten, sieht § 15b Abs. 2 spezifische, technisch bei jedem Einsatz sicherzustellende Dokumentationspflichten vor. Durch die automationsunterstützte, lückenlose Dokumentation dieser Parameter soll insbesondere sichergestellt werden, dass die Installation des Programms sowie jede sonstige durch die Software an dem Computersystem vorgenommene Veränderung nachvollziehbar bleibt. Die Dokumentation ist – im Sinne von § 37 Abs. 1 Z 6 DSG – nach dem Stand der Technik vor Veränderung, Verlust, Zerstörung oder Schädigung zu schützen. Die bestehenden Protokollierungspflichten nach § 50 DSG bleiben von diesen erweiterten Dokumentationspflichten unberührt.

Der Bundesminister für Inneres ist 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 und hat als solcher für das Überwachungsprogramm ein Verzeichnis von Verarbeitungstätigkeiten zu führen (vgl. §§ 4, 49 DSG), mit der Datenschutzbehörde nach Maßgabe des § 51 DSG zusammenzuarbeiten und eine Datenschutz-Folgenabschätzung durchzuführen (§ 52 DSG).

Gemäß § 15b Abs. 3 sind sämtliche ermittelte Nachrichten samt Informationen iSd § 134 Z 3 StPO bereits während der Durchführung der Maßnahme zu prüfen und nur diejenigen Nachrichten und Informationen weiterzuverarbeiten, die für die Vorbeugung jenes verfassungsgefährdenden Angriffs, für den die Maßnahme bewilligt wurde, erforderlich sind oder die nach § 15b Abs. 4 weiterverarbeitet werden dürfen, wobei durch den Verweis auf § 9 Abs. 1 klargestellt wird, dass die Weiterverarbeitung von Nachrichten und Informationen, die der von § 155 Abs. 1 Z 1 StPO erfassten geistlichen Amtsverschwiegenheit oder einem von § 157 Abs. 1 Z 2 bis 4 StPO geschützten Berufsgeheimnis unterliegen, nicht zulässig ist (vgl. hinsichtlich des Schutzes der geistlichen Amtsverschwiegenheit und von Berufsgeheimnissen bei der Überwachung von Nachrichten überdies auch § 15d Abs. 2 erster Satz). Daten, die demnach nicht weiterverarbeitet werden dürfen, sind nach den im Sicherheitspolizeibereich einschlägigen Bestimmungen (§ 63 SPG) zu löschen.

Sofern aus ermittelten Nachrichten und Informationen, die nach Maßgabe des § 15b Abs. 3 erster Fall mangels Erforderlichkeit für die Vorbeugung jenes verfassungsgefährdenden Angriffs, für den die Maßnahme bewilligt wurde, prinzipiell zu löschen wären, Anhaltspunkte für eine begangene Straftat oder deren geplante Begehung zu Tage treten, eröffnet sich eine besondere Herausforderung im Spannungsverhältnis zwischen Offizialprinzip einerseits und dem Interesse an einer umfassenden Geheimhaltung der verdeckten Nachrichtenüberwachung andererseits. Um dem staatlichen Strafverfolgungsanspruch sowie der Verhinderung gefährlicher oder verfassungsgefährdender Angriffe dennoch Rechnung tragen zu können, soll die Direktion bei Bekanntwerden eines begründeten Gefahrenverdachts für einen anderen verfassungsgefährdenden Angriff als jenen, für den die Überwachung von Nachrichten bewilligt wurde, oder von Hinweisen auf eine im Rahmen der erweiterten Gefahrenerforschung zu beobachtende Gruppierung im Sinne des § 6 Abs. 1, unverzüglich um die Ermächtigung des Rechtsschutzbeauftragten für die Aufgabe nach § 6 Abs. 1 oder 2 ansuchen. Bis zur Erteilung der Ermächtigung sind die betreffenden Nachrichten und Informationen gesondert von den für die konkrete Aufgabenerfüllung erforderlichen Nachrichten und Informationen zu verwahren. Sollte die Ermächtigung durch den Rechtsschutzbeauftragten verwehrt werden, sind die Nachrichten und Informationen in nicht rückführbarer Weise zu löschen. Die Einbeziehung von Hinweisen auf Gruppierungen in die bedingte Weiterverarbeitungsermächtigung bezieht ihre Rechtfertigung – neben dem Interesse an der frühzeitigen Erkennung verfassungsgefährdender Strukturen – nicht zuletzt aus dem Umstand, dass gemäß § 6 Abs. 1 Gruppierungen nur insofern der Beobachtung unterliegen, als im Hinblick auf ihre bestehenden Strukturen und auf zu gewärtigende Entwicklungen in ihrem Umfeld damit zu rechnen ist, dass es zu mit schwerer Gefahr für die öffentliche Sicherheit verbundener Kriminalität kommt. Da bei Vergehen in der Regel nicht von einer schweren Gefahr für die öffentliche Sicherheit auszugehen ist (vgl. AB 812 BlgNR 20. GP 6) wird auch für Hinweise auf Gruppierungen die – für Z 2 ausdrücklich normierte – Verbrechensschwelle gewürdigt.

Sollten sich aus den ermittelten Nachrichten und Informationen Anhaltspunkte für ein geplantes (§ 16 Abs. 3 SPG) oder begangenes Verbrechen (§ 17 StGB), wovon auch strafbare Versuche (§ 15 StGB) umfasst sind, ergeben, so ist darüber im Falle eines geplanten Verbrechens die zuständige Sicherheitsbehörde, im Falle eines bereits begangenen die Staatsanwaltschaft, der die Entscheidung über Weiterführung, Beendigung oder Einstellung des Verfahrens obliegt, ehestmöglich zu verständigen, sofern nicht das sicherheitspolizeiliche Einschreiten oder kriminalpolizeiliche Ermittlungen gemäß § 6 Abs. 4 aufgeschoben werden. Sofern sich der Hinweis auf eine strafbare Handlung gegen fremdes Vermögen nach dem sechsten Abschnitt des StGB bezieht, ist ein Vorgehen nach Z 2 nicht zulässig, sodass die den Hinweis enthaltenden Nachrichten nicht weiterverarbeitet werden dürfen und zu löschen sind. Durch den Verweis auf § 16 Abs. 3 SPG soll klargestellt werden, dass auch gefährliche Angriffe, die sich noch im Vorbereitungsstadium befinden, von der Verständigungspflicht nach § 15b Abs. 4 Z 2 umfasst sind.

Die Schadenersatzbestimmung in § 15b Abs. 5 orientiert sich weitestgehend an der korrespondierenden strafprozessualen Bestimmung des § 148 StPO.

Zu § 15 Abs. 3 und § 15c (Besonderer Rechtsschutz bei der Überwachung von Nachrichten):

Angesichts der Etablierung eines neuartigen Rechtsschutzsystems für die Überwachung (un)verschlüsselter Kommunikation nach § 11 Abs. 1 Z 8 und 9, im Rahmen dessen eine Bewilligung des BVwG sowie ein kommissarischer Rechtsschutz gegen die Bewilligung und die laufende Kontrolle der Maßnahme durch den Rechtsschutzbeauftragten vorgesehen sind, sind begleitende Verfahrensbestimmungen, insbesondere hinsichtlich der Bewilligungsmodalitäten für entsprechende Anträge der Direktion nach § 15a Abs. 1, erforderlich. Sämtliche Rechtsschutzbestimmungen, die einerseits die Bewilligung der Ermittlungsmaßnahme, andererseits die Möglichkeit ihrer vorzeitigen Beendigung betreffen, sollen gebündelt in § 15c abgebildet werden. Gemäß § 15c Abs. 1 kommt dem Rechtsschutzbeauftragten das Recht zu, stellvertretend für den Betroffenen einer Maßnahme nach § 11

Abs. 1 Z 8 oder 9 zu einem Zeitpunkt, zu dem dieser selbst noch keine Kenntnis von der verdeckten Maßnahme erlangt hat, beim Verwaltungsgerichtshof Revision gegen den bewilligenden Beschluss des BVwG zu erheben. Ab Zustellung des Beschlusses (vgl. § 15a Abs. 3) kommt dem Rechtsschutzbeauftragten gem. § 15 Abs. 3 im Zusammenhang mit der Überwachung von Nachrichten vor den Gerichtshöfen des öffentlichen Rechts im Rahmen eines vom Bundesminister für Inneres angestrengten Rechtsmittelverfahrens die Stellung einer mitbeteiligten Amtspartei zu. Ab diesem Zeitpunkt kann er unter den Voraussetzungen des § 25a Verwaltungsgerichtshofgesetzes 1985 – VwGG, BGBl. Nr. 10/1985, binnen einer Frist von sechs Wochen Revision gegen den Beschluss erheben, wobei diesem Rechtsmittel keine aufschiebende Wirkung zukommt (§ 30 VwGG). Der Beginn der Parteistellung des Rechtsschutzbeauftragten mit Zustellung des Beschlusses hindert das Gericht allerdings nicht daran, den Rechtsschutzbeauftragten auch schon im Rahmen des Verfahrens auf Erlassung der Bewilligung als Auskunftsperson zu Rate zu ziehen.

Im Zuge der Durchführung der Maßnahme kommt dem Rechtsschutzbeauftragten gem. § 15c Abs. 2 überdies das Recht zu, jederzeit die nach § 11 Abs. 1 Z 8 oder 9 ermittelten Nachrichten und Informationen, die nicht bereits nach § 15b Abs. 3 letzter Satz gelöscht wurden, vollumfänglich und direkt vor Ort in den Räumlichkeiten der Direktion, in denen die Nachrichtenüberwachung stattfindet, einzusehen und anzuhören, die Löschung von Nachrichten und Informationen oder Teilen von ihnen, insbesondere bei Überschreitung der Bewilligung, zu verlangen und sich von der ordnungsgemäßen Löschung zu überzeugen. Als ultima ratio steht es ihm überdies jederzeit frei, seine Ermächtigung gemäß § 14 Abs. 2 für die Aufgabe nach § 6 Abs. 2 zu entziehen und damit sämtliche Ermittlungsmaßnahmen nach § 11 Abs. 1 inklusive der Nachrichtenüberwachung sofort zu stoppen. Sollte der Rechtsschutzbeauftragte im Zuge seiner begleitenden Kontrolle Anhaltspunkte wahrnehmen, die ihn an der Verhältnismäßigkeit der Fortführung der Ermittlungsmaßnahme zweifeln lassen – etwa weil sich trotz bereits länger andauernder Überwachung aus den Nachrichten und Informationen keine inkriminierenden Hinweise auf jenen verfassungsgefährdenden Angriff, für dessen Vorbeugung die Maßnahme bewilligt wurde, ergeben – hat der Rechtsschutzbeauftragte unverzüglich einen begründeten Antrag auf Aufhebung der Bewilligung (§ 15a Abs. 1) beim nach der Geschäftsverteilung zuständigen Senat des BVwG zu stellen. Bei diesem Antrag handelt es sich nicht um ein Rechtsmittel gegen den bewilligenden Beschluss des BVwG, sondern einen selbständigen, ein neues (erstinstanzliches) Verfahren auslösenden Antrag. Zugleich mit der Beantragung der Aufhebung hat der Rechtsschutzbeauftragte die Direktion von seinem Antrag durch Übermittlung desselben in Kenntnis zu setzen. Um dem BVwG eine fundierte Entscheidungsgrundlage unter Berücksichtigung aller für und wider eine vorzeitige Beendigung der Ermittlungsmaßnahme sprechenden Gründe zu ermöglichen, wird der Direktion im Verfahren auf Aufhebung des bewilligenden Beschlusses ausdrücklich das Recht auf Stellungnahme eingeräumt. Sofern dem Antrag des Rechtsschutzbeauftragten auf Aufhebung des die Ermittlungsmaßnahme bewilligenden Beschusses durch Erlassung eines neuerlichen Beschlusses seitens des BVwG Folge gegeben wird, ist die Erhebung einer Revision gegen diesen Beschluss durch den Bundesminister für Inneres ausgeschlossen. Damit soll unter Berücksichtig von Effizienzerwägungen dem Umstand Rechnung getragen werden, dass eine durch den Rechtsschutzbeauftragten und das BVwG für unverhältnismäßig erachtete Ermittlungsmaßnahme keiner zusätzlichen höchstgerichtlichen Überprüfung zu unterziehen ist. Das gilt umso mehr, als es der Direktion unbenommen bleibt, einen erneuten – auf ergänzende Zulässigkeitsargumente oder Sachverhaltsdarstellungen gestützten – Antrag gemäß § 15a Abs. 1 zu stellen, sofern sie die Voraussetzungen des Einsatzes einer Maßnahme nach § 11 Abs. 1 Z 8 oder 9 weiterhin als erfüllt erachtet, um deren rasche Wiederaufnahme unabhängig von einem langwierigen Revisionsverfahren zu ermöglichen.

Die Absätze 3 bis 4 normieren Verfahrensbestimmungen für die Behandlung des Antrags auf Bewilligung einer Ermittlungsmaßnahme nach § 11 Abs. 1 Z 8 oder 9 durch das BVwG. Die Entscheidung über die Anträge der Direktion gem. § 15a Abs. 1 oder des Rechtsschutzbeauftragten gem. § 15c Abs. 2 erfolgt durch den nach der Geschäftsverteilung zuständigen Dreirichtersenat des Bundesverwaltungsgerichtes (§ 7 Abs. 1 BVwGG) mittels begründetem Beschluss (§ 15c Abs. 4). Durch die Befassung eines Richtergremiums soll ein erhöhtes Prüfniveau gegenüber der Entscheidung durch einen Einzelrichter gewährleistet werden und ein möglichst hoher Schutzstandard für die neuen Ermittlungsmaßnahmen der Nachrichtenüberwachung etabliert werden. Ausschließlich bei Gefahr im Verzug kann – wenn nicht davon auszugehen ist, dass die Bewilligung durch den Dreirichtersenat rechtzeitig zur Vorbeugung des verfassungsgefährdenden Angriffs eingeholt werden kann – die Bewilligung auch durch den Einzelrichter des Bundesverwaltungsgerichtes (§ 6 BVwGG) erfolgen. Das Vorliegen einer Gefahr-im-Verzug-Situation ist seitens der Direktion gemäß § 15a Abs. 1 Z 9 im Rahmen des Antrags auf Bewilligung der Nachrichtenüberwachung anzuführen und zu begründen. Die Beurteilung, ob Gefahr im Verzug tatsächlich vorliegt, obliegt der richterlichen Würdigung basierend auf einer ex-ante Beurteilung der zum Zeitpunkt der Antragstellung bekannten Tatsachen. Sämtliche Richter und sonstige Bedienstete des

BVwG, die mit der Bearbeitung der Anträge betraut sind und denen demnach klassifizierte Informationen im Sinne des § 2 Abs. 2 des Informationssicherheitsgesetzes – InfoSiG, BGBl. I Nr. 23/2002, aus dem hochsensiblen Bereich des Verfassungsschutzes zur Kenntnis gelangen könnten, haben sich zuvor einer Vertrauenswürdigkeitsprüfung (§ 2a) zu unterziehen und diese – vergleichbar Art. 43 des schweizer Bundesgesetzes über die Informationssicherheit hinsichtlich der dortigen erweiterten Personensicherheitsprüfung – alle fünf Jahre zu wiederholen. Bei Vorliegen von Anhaltspunkten, welche die Vertrauenswürdigkeit in Zweifel ziehen lassen, ist diese unverzüglich zu wiederholen. Im Falle eines negativen Ergebnisses der Vertrauenswürdigkeitsprüfung ist eine Befassung mit Anträgen im Zusammenhang mit einer Ermittlungsmaßnahme nach § 11 Abs. 1 Z 8 oder 9 gemäß § 15 Abs. 3a BVwGG ausgeschlossen (vgl. die Ausführungen zu Art. 4 Z 1).

Um dem BVwG eine fundierte Entscheidung hinsichtlich des auf Bewilligung der Ermittlungsmaßnahme nach § 11 Abs. 1 Z 8 oder 9 gerichteten Antrags der Direktion oder des auf vorzeitige Aufhebung der Bewilligung gerichteten Antrags des Rechtsschutzbeauftragten zu ermöglichen, kommen den in diesen Angelegenheiten betrauten Richtern des BVwG die Rechte des Rechtsschutzbeauftragten nach § 15 Abs. 1 und 2 erster Satz zu. Ihnen ist demnach insbesondere von den Organisationseinheiten nach § 1 Abs. 3 jederzeit Einblick in alle erforderlichen Unterlagen und Aufzeichnungen sowie in die Datenverarbeitungen nach § 12 Abs. 1 und 1a zu gewähren und die erforderliche Auskunft zu erteilen. Die Ausübung dieser Rechte beschränkt sich in zeitlicher Hinsicht auf die Dauer des Bewilligungsverfahrens beziehungsweise eines allfälligen Aufhebungsverfahrens und begründet keine Kontrollpflichten des BVwG hinsichtlich der Durchführung der Maßnahme.

Das BVwG hat über den Antrag der Direktion oder des Rechtsschutzbeauftragten unverzüglich zu erkennen. Abhängig von der – im Rahmen des Antrags auf Bewilligung seitens der Direktion darzulegenden – Dringlichkeit des Einsatzes der Ermittlungsmaßnahme, wird das Erfordernis der Unverzüglichkeit variabel zu beurteilen sein. Angesichts der Schwere der die Maßnahme rechtfertigenden, drohenden verfassungsgefährdenden Angriffe, sollte die Entscheidungsdauer allerdings sieben Werktage nicht übersteigen. Der Dringlichkeit des Einsatzes der Maßnahme ist auch der ausdrückliche Ausschluss der Durchführung einer mündlichen Verhandlung in Verfahren auf Beantragung der Bewilligung sowie einem allfälligen Verfahren auf Aufhebung derselben geschuldet. Durch die Möglichkeit der Beiziehung des Rechtsschutzbeauftragten als Auskunftsperson im Bewilligungsverfahren (vgl. die Ausführungen zu § 15 Abs. 3) sowie die ausdrückliche Einräumung eines Stellungnahmerechts der Direktion im Aufhebungsverfahren (§ 15c Abs. 2) handelt es sich trotz Unterbleibens einer mündlichen Verhandlung um kein reines Aktenverfahren und werden hinreichende Garantien zur Gewährleistung des Parteiengehörs etabliert.

Im Zusammenhang mit der Beantragung einer Maßnahme nach § 11 Abs. 1 Z 8 oder 9 ergehende Beschlüsse des BVwG haben die wesentlichen Entscheidungsgründe zu enthalten und sind gemäß § 20 Z 6 BVwGG – um dem Interesse an Geheimhaltung der konkreten Durchführungsparameter einer Nachrichtenüberwachung nachzukommen – nicht im Rechtsinformationssystem des Bundes (RIS) zu veröffentlichen (vgl. die Ausführungen zu Art. 4 Z 3).

Schließlich hält Abs. 5 fest, dass sämtliche Kommunikation im Zusammenhang mit einer Ermittlungsmaßnahme nach § 11 Abs. 1 Z 8 und 9 oder einem diesbezüglichen Rechtsmittel zwischen dem BVwG oder sonstigen Rechtsschutzeinrichtungen (insb. VwGH, VfGH oder DSB) einerseits und der Direktion sowie dem Rechtsschutzbeauftragten andererseits im elektronischen Weg über einen sicheren Kommunikationskanal zu erfolgen hat, um ein möglichst hohes Datensicherheitsniveau zu gewährleisten. Dabei handelt es sich um eine lex specialis zu den bestehenden materienspezifischen Rechtsgrundlagen zur (elektronischen) Einbringung von Schriftsätzen. Das BVwG und die sonstigen Rechtsschutzeinrichtungen haben überdies sämtliche damit in Zusammenhang stehende Daten getrennt vom sonstigen Aktenbestand zu verwahren und auf geeignete Art und Weise gegen unbefugte Einsichtnahme zu sichern.

Zu § 15d (Schutz der geistlichen Amtsverschwiegenheit und von Berufsgeheimnissen bei der Überwachung von Nachrichten):

Da das Ermittlungsverbot gemäß § 9 Abs. 1 dritter Satz nur für jene Fälle einen Schutz von Verschwiegenheitspflichten bietet, in denen der Geistliche oder der Berufsgeheimnisträger nicht selbst Betroffener nach § 6 Abs. 2 ist, sollen mit § 15d – Anregungen aus dem Begutachtungsverfahren folgend und im Lichte rezenter Judikatur des EGMR (vgl. EGMR 03.04.2025, 57748/21 [Kulák gg. Slowakei]) – Sonderbestimmungen für den Schutz der geistlichen Amtsverschwiegenheit sowie von Berufsgeheimnissen bei der Überwachung von Nachrichten geschaffen werden.

In Anlehnung an § 144 Abs. 3 iVm § 147 Abs. 2 StPO soll für jene Fälle, in denen ein Computersystem einer in § 155 Abs. 1 Z 1 oder § 157 Abs. 1 Z 2 bis 4 StPO angeführten Person überwacht werden soll,

entsprechend der unterschiedlichen Eingriffsintensität der Maßnahme eine Kaskade an zusätzlichen Erfordernissen für die Bewilligung der Nachrichtenüberwachung etabliert werden, je nachdem, ob das zu überwachende Computersystem rein privat oder auch beruflich bzw. in Ausübung des geistlichen Amtes genutzt wird. Sofern es sich um eine ausschließlich private Nutzung handelt, soll die Bewilligung der Maßnahme in jedem Fall dem gemäß § 7 Abs. 1 BVwGG aus drei Mitgliedern bestehendem nach der Geschäftsverteilung zuständigen Senat obliegen. Die gemäß § 15a Abs. 1 letzter Satz grundsätzlich vorgesehene Einschränkung, dass im Falle von Gefahr im Verzug die Bewilligung der Nachrichtenüberwachung auch durch den nach der Geschäftsverteilung zuständigen Einzelrichter des Bundesverwaltungsgerichtes erfolgen kann, kommt im Falle der Betroffenheit des Computersystems eines Geheimnisträgers nicht zur Anwendung. Sofern nicht ausgeschlossen werden kann, dass das zu überwachende Computersystem auch im Rahmen amtlicher oder beruflicher Kommunikation verwendet wird, ist – in Anlehnung an § 115l StPO – zusätzlich zu der Senatsentscheidung im Rahmen des Antrages auf Bewilligung der Nachrichtenüberwachung darzulegen, dass besonders schwerwiegende Gründe vorliegen, die den Eingriff in die berufliche Kommunikation verhältnismäßig erscheinen lassen (vgl. § 15a Abs. 2 Z 10). Derartige Gründe können insbesondere in einer gesteigerten Dichte oder Schwere der für die Nachrichtenüberwachung ausschlaggebenden Verdachtsmomente begründet liegen.

Durch die Bezugnahme in Abs. 2 auf das Ermittlungsverbot gemäß § 9 Abs. 1 dritter Satz soll ausdrücklich klargestellt werden, dass Nachrichten und Informationen, die an eine in § 155 Abs. 1 Z 1 oder § 157 Abs. 1 Z 2 bis 4 StPO angeführte Person oder von dieser gesendet, übermittelt oder empfangen werden, unverzüglich zu löschen sind, wenn nicht ein Computersystem dieser Person Gegenstand der Nachrichtenüberwachung ist. Das Verarbeitungsverbot gilt diesfalls umfassend, sodass auch allfällige Hinweise auf einen anderen verfassungsgefährdenden Angriff als jenen, für den die Maßnahme bewilligt wurde, eine Gruppierung nach § 6 Abs. 1 oder auf geplante bzw. bereits begangene Verbrechen (sog. Zufallsfunde) unverzüglich zu löschen sind. Um die Umsetzung dieses strengen Verarbeitungsverbotes sicherzustellen, kommt insbesondere der begleitenden Kontrolle durch den Rechtsschutzbeauftragten, die im Falle der Betroffenheit eines Geheimnisträgers besonders intensiv zu erfolgen haben wird, gesteigerte Bedeutung zu.

Zu § 16 Abs. 2 und 3 (Information der Betroffenen):

Die Information des von der Durchführung einer Überwachung von (verschlüsselten) Nachrichten Betroffenen der Aufgabe nach § 6 Abs. 2 hat nach Maßgabe des § 16 Abs. 2 mit Ablauf der Ermächtigung des Rechtsschutzbeauftragten nachweislich zu erfolgen. Gemeinsam mit der Information über die Durchführung einer Überwachung von Nachrichten nach § 11 Abs. 1 Z 8 oder 9 ist dem Betroffenen der Beschluss des Bundesverwaltungsgerichtes (§ 15a Abs. 3) zuzustellen, soweit dies nicht gemäß Abs. 3 aufzuschieben ist oder zu unterbleiben hat. Mit dieser Zustellung beginnt auch die sechswöchige Frist zur Erhebung einer Revision durch den Betroffenen. Darüber hinaus wird die Informationspflicht, um auch dem Rechtsschutz sonstiger, von der Nachrichtenüberwachung betroffener Dritter ausreichend Rechnung zu tragen, auf jene Personen erstreckt, an die oder von denen Nachrichten gesendet, übermittelt oder empfangen wurden, die aufgrund ihrer Erforderlichkeit für die Aufgabenerfüllung weiterverarbeitet wurden, sofern ihre Identität sich ohne erheblichen Verfahrensaufwand, somit lediglich durch leicht durchführbare zusätzliche Erhebungen, feststellen lässt (vgl. zur vergleichbaren strafprozessualen Regelung § 139 Abs. 2 StPO). Im Übrigen stehen dem Betroffenen oder sonstigen betroffenen Dritten weiterhin sämtliche sonstige 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. Dem Betroffenen einer Nachrichtenüberwachung steht es schließlich auch ab der Zustellung des Beschlusses des Bundesverwaltungsgerichtes frei, eine Revision an den Verwaltungsgerichtshof zu erheben.

Zu Z 18, 19 und 20 (§ 17 Abs. 3, 3a, 3b und 5):

Der Bundesminister für Inneres hat dem Ständigen Unterausschuss des Ausschusses für innere Angelegenheiten zur Überprüfung von Maßnahmen zum Schutz der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit (Art. 52a B-VG) über jene Fälle, in denen gemäß § 6 Abs. 4 Z 1 davon Abstand genommen wurde, einem gefährlichen Angriff vorzubeugen oder ein Ende zu setzen, über erteilte Ermächtigungen des Direktors gemäß § 6 Abs. 5, um dem Aufgabenbereich Nachrichtendienst im Einzelfall die Wahrnehmung einer Aufgabe des Staatschutzes zu ermöglichen und über die Durchführung

von Nachrichtenüberwachungen nach § 11 Abs. 1 Z 8 oder 9 sowie die damit im Zusammenhang stehende Information Betroffener nach § 16 jedenfalls halbjährlich zu berichten.

Zusätzlich hat der Bundesminister für Inneres dem Ständigen Unterausschuss vor der erstmaligen Inbetriebnahme eines Programms gemäß § 11 Abs. 1 Z 9 über dessen Anschaffungskosten und die standardisierende Leistungsbeschreibung, die insbesondere auch allgemeine Angaben hinsichtlich der Softwarearchitektur und des Anbieters des Programms enthält, zu berichten. Anschließend hat der Bundesminister für Inneres jährlich bis spätestens 31. März des Folgejahres über die innerhalb des vergangenen Kalenderjahres angefallenen Gesamtkosten im Zusammenhang mit der Überwachung von Nachrichten nach § 11 Abs. 1 Z 9 an den Ständigen Unterausschuss zu berichten.

Schließlich soll eine anlassbezogene unverzügliche Berichtspflicht des Bundesministers für Inneres gegenüber dem Ständigen Unterausschuss vorgesehen werden, wenn die Anzahl der Anwendungsfälle der Überwachung von Nachrichten nach § 11 Abs. 1 Z 9 innerhalb eines Kalenderjahres 30 überschreitet.

Außerdem soll ausdrücklich festgehalten werden, dass die Verpflichtung des Rechtsschutzbeauftragten gemäß § 17 Abs. 5, dem Ständigen Unterausschuss für Auskünfte über wesentliche Entwicklungen zur Verfügung zu stehen, insbesondere auch Auskünfte über Umfang und Ergebnis seiner Vorabkontrolle des Programms zur Überwachung verschlüsselter Nachrichten gemäß § 14 Abs. 6 umfasst.

Zu Z 21 (§ 17a Abs. 3):

In Anlehnung an § 2a Abs. 6 des Staatsanwaltschaftsgesetzes – StAG, BGBl. Nr. 164/1986, soll eine ausdrückliche gesetzliche Grundlage für die Einrichtung eines internetbasierten Hinweisgebersystems, über das der unabhängigen Kontrollkommission Verfassungsschutz Vorwürfe gegen die Tätigkeiten der Organisationseinheiten nach § 1 Abs. 3 auch anonym gemeldet werden können, geschaffen werden. Das System soll durch Ausschluss der Rückverfolgbarkeit der verwendeten IP-Adresse sowie einer ausschließlich auf Freiwilligkeit basierenden Möglichkeit zur Preisgabe der Identität die Anonymität des Hinweisgebers wahren und zugleich eine Nachfragemöglichkeit der Kontrollkommission beim Hinweisgeber unter Wahrung dessen Anonymität zur Objektivierung der Begründetheit des gemeldeten Vorwurfs ermöglichen.

Zu Z 22 (§ 18 Abs. 10 und 11):

Es handelt sich um die Inkrafttretensbestimmung sowie die Verankerung einer verpflichtenden Evaluierung der Anwendung der Ermächtigung zur einzelfallbezogenen Aufgabenübertragung gemäß § 6 Abs. 5 drei Jahre nach ihrem Inkrafttreten. Über das Ergebnis der Evaluierung ist dem Ständigen Unterausschuss zu berichten.

Zu Z 23 (§ 18a):

Es handelt sich um die Außerkrafttretensbestimmung für § 6 Abs. 5.

Zu Art. 2 (Änderung des Sicherheitspolizeigesetzes)

Zu Z 1 (§ 53 Abs. 3b):

Durch den Entfall der Kurzbezeichnung „IMSI“ soll klargestellt werden, dass von der internationalen Mobilteilnehmerkennung, deren Feststellung beziehungsweise Beauskunftung nach § 53 Abs. 3b zulässig ist, nicht bloß die „International Mobile Subscriber Identity“, sondern beispielsweise auch der im 5G-Netz einschlägige Identifizierungsparameter „Subscription Permanent Identifier (SUPI)“ umfasst ist, um eine Lokalisierung unabhängig vom konkreten Netz zu ermöglichen.

Zu Z 2 (§ 91b Abs. 1a):

Vor dem Hintergrund, dass dem Rechtsschutzbeauftragten sowie seinen Stellvertretern im Rahmen ihrer Aufgaben nach dem SPG sowie SNG klassifizierte Informationen im Sinne des § 2 Abs. 2 InfoSiG – insbesondere auch aus dem hochsensiblen Bereich des Verfassungsschutzes – zur Kenntnis gelangen können, soll deren Verpflichtung, sich vor Beginn ihrer Tätigkeit einer Vertrauenswürdigkeitsprüfung nach § 2a SNG zu unterziehen, vorgesehen werden. Ebenso wie hinsichtlich der Richter und Bediensteten des Bundesverwaltungsgerichts gemäß § 15c Abs. 3 SNG soll die Vertrauenswürdigkeitsprüfung für den Rechtsschutzbeauftragten sowie seine Stellvertreter alle fünf Jahre zu wiederholen sein. Sofern sich vor Ablauf dieser Frist Anhaltspunkte, wonach der Rechtsschutzbeauftragte oder einer seiner Stellvertreter nicht mehr vertrauenswürdig sein könnte, ergeben, ist die Prüfung aufgrund der sinngemäßen Geltung von § 2a Abs. 8 zweiter Satz SNG unverzüglich zu wiederholen.

Zu Z 3 (§ 91b Abs. 2a):

In Anlehnung an § 9a Abs. 8 des Gesetzes über das Bundesamt zur Korruptionsprävention und Korruptionsbekämpfung – BAK-G, BGBl. I Nr. 72/2009, sowie § 15 Abs. 6 des

Volksanwaltschaftsgesetzes 1982 – VolksanwG, BGBl. Nr. 433/1982, soll auch für den Rechtsschutzbeauftragten sowie seine Stellvertreter die Möglichkeit einer Abberufung vor Ablauf der Funktionsperiode geschaffen werden. In Betracht kommt eine Abberufung einerseits sofern der Rechtsschutzbeauftragte oder einer seiner Stellvertreter die mit seiner Funktion verbundenen Pflichten grob verletzt hat oder dauernd vernachlässigt und andererseits bei einer nachträglichen Unvereinbarkeit mit den Ernennungsvoraussetzungen nach Abs. 1 oder dem Nichterfüllen des Erfordernisses einer Vertrauenswürdigkeitsprüfung nach Abs. 1a. Eine Unvereinbarkeit mit Abs. 1 kann sich insbesondere im Falle eines nachträglich eintretenden Ausschlusses der Eignung als Geschworener oder Schöffe gemäß § 2 des Geschworenen- und Schöffengesetzes 1990 – GSchG, BGBl. Nr. 256/1990, etwa wenn die Pflichten des Amtes infolge des körperlichen oder geistigen Zustands nicht mehr erfüllt werden können, ergeben. Im Falle der Verweigerung einer Vertrauenswürdigkeitsprüfung oder bei im Rahmen der Überprüfung zu Tage geförderten Anhaltspunkten, die die Vertrauenswürdigkeit ausschließen, fehlt es wiederum an der erforderlichen Berechtigung zur Ausübung der Tätigkeit, weil gemäß § 3 Abs. 1 Z 1 lit c InfoSiG kein Zugang zu entsprechend klassifizierten Informationen gewährt werden darf. In beiden Alternativen ist eine pflichtgemäße Erfüllung der Aufgaben des Rechtsschutzbeauftragten und seiner Stellvertreter nicht mehr möglich, sodass eine Abberufung indiziert ist. Die Abberufung soll im Sinne eines actus contrarius im Wesentlichen spiegelbildlich zu den Bestellungsmodalitäten gemäß § 91a Abs. 2 erfolgen: Bei Vorliegen eines entsprechenden Vorschlages der Bundesregierung kann der Bundespräsident demnach – sofern dem Rechtsschutzbeauftragten sowie sämtlichen Stellvertretern zuvor das Recht auf Äußerung in der Sache eingeräumt wurde – die Abberufung verfügen.

Zu Z 4 (§ 91b Abs. 3):

Dem Rechtsschutzbeauftragten und seinen Stellvertretern sollen künftig neben den zur Bewältigung ihrer administrativen Tätigkeit notwendigen Personal- und Sacherfordernissen ausdrücklich auch die notwendigen technischen Ressourcen zur Verfügung gestellt werden. Hierdurch soll insbesondere auch die Effektivität der begleitenden Kontrolle der neu zu schaffenden Ermittlungsmaßnahme der Überwachung von Nachrichten durch den Rechtsschutzbeauftragten gemäß § 14 Abs. 4, 5 und 6 SNG gewährleistet werden. Die voraussichtlich erforderliche Ausstattung des Rechtsschutzbeauftragten lässt sich im Detail der Wirkungsorientierten Folgenabschätzung entnehmen, in der insbesondere festgelegt ist, dass ihm die erforderliche Anzahl an wissenschaftlichen Mitarbeitern zur Verfügung zu stellen ist, um auch auf personeller Ebene die entsprechende technische Expertise des Rechtsschutzbeauftragten sicherzustellen.

Da auch den Mitarbeitern des Rechtsschutzbeauftragten, die gemäß § 91b Abs. 3 mit der Bewältigung seines administrativen Aufwandes befasst sind, im Rahmen ihrer Tätigkeit klassifizierte Informationen zur Kenntnis gelangen können, sind auch sie einer Vertrauenswürdigkeitsprüfung nach § 2a SNG zu unterziehen. Die Überprüfungsmodalitäten entsprechen jenen für den Rechtsschutzbeauftragten, sodass diesbezüglich auf die Ausführungen zu Z 2 verwiesen werden kann.

Zu Z 5 (§ 94 Abs. 57):

Es handelt sich um die Inkrafttretensbestimmung.

Zu Z 6 (§ 96 Abs. 11 und 12):

Es handelt sich um die erforderliche Übergangsbestimmung, damit die Bestimmungen betreffend die Durchführung einer Vertrauenswürdigkeitsprüfung des Rechtsschutzbeauftragten sowie seiner Stellvertreter erst auf Bestellungen, die nach Inkrafttreten dieses Bundesgesetzes erfolgen, Anwendung finden. Für Personen, die zur Bewältigung des administrativen Aufwandes des Rechtsschutzbeauftragten eingesetzt werden, soll dahingegen eine sechsmonatige Übergangsfrist vorgesehen werden, nach deren Ablauf die Vertrauenswürdigkeitsprüfungen erstmals durchzuführen sind. Sofern bereits vor diesem Zeitpunkt Anhaltspunkte, die die Vertrauenswürdigkeit in Zweifel ziehen, vorliegen, ist die Überprüfung unverzüglich durchzuführen.

Zu Art. 3 (Änderung des Telekommunikationsgesetzes 2021)

Zu Z 1 bis 4 (§ 161 Abs. 3 und § 162 Abs. 1, 2 sowie 3):

Mit der Anpassung der Bestimmungen des Telekommunikationsgesetzes 2021 soll die Ausnahme vom Kommunikationsgeheimnis auf die neue Ermittlungsmaßnahme nach § 11 Abs. 1 Z 8 SNG erweitert und die erforderliche Mitwirkung der (Kommunikationsdienste)Anbieter an der Nachrichtenüberwachung gemäß § 11 Abs. 1 Z 8 SNG sichergestellt werden. Ergänzend soll die Verordnung gemäß § 162 Abs. 2, mit der ein angemessener Kostenersatz für die Mitwirkung der Anbieter im Rahmen diverser Ermittlungsmaßnahmen nach StPO, SNG, FinStrG und MBG, vorgesehen wird, künftig auch im

Einvernehmen mit dem Bundesminister für Inneres, der die im Zusammenhang mit Ermittlungsmaßnahmen nach § 11 Abs. 1 Z 7 und 8 entstehenden Kosten zu tragen hat, erlassen werden.

Zu Z 5 (§ 217):

Die Bestimmungen des TKG 2021 sollen gleichzeitig mit der Novelle des SNG in Kraft treten.

Zu Art. 4 (Änderung des Bundesverwaltungsgerichtsgesetzes)

Zu Z 1 (§ 15 Abs. 3a):

Nach § 15c Abs. 3 des Staatsschutz- und Nachrichtendienst-Gesetzes (SNG), BGBl. I Nr. 5/2016, ist vorgesehen, dass sich die Richterinnen und Richter des Bundesverwaltungsgerichts, denen Anträge nach § 15a Abs. 1 SNG oder § 15c Abs. 2 SNG zugewiesen sind, vor der Wahrnehmung dieser Angelegenheiten einer Vertrauenswürdigkeitsprüfung nach § 2a SNG zu unterziehen haben. Mit dem vorgeschlagenen Abs. 3a wird nunmehr für den Geschäftsverteilungsausschuss bindend sichergestellt, dass nur jene Richterinnen und Richter des Bundesverwaltungsgerichts mit derart sensiblen Angelegenheiten nach dem SNG befasst werden dürfen, die als vertrauenswürdig im Sinne der zuvor durchgeführten Vertrauenswürdigkeitsprüfung gelten. Dies gilt naturgemäß auch im Fall einer Senatszuständigkeit nach § 15a Abs. 1 SNG insoweit, als die Zuweisung nur an Senate erfolgen darf, die sich ausschließlich aus nach § 15c Abs. 3 SNG vertrauenswürdigen Richterinnen und Richtern zusammensetzen.

Zu Z 2 (§ 16a samt Überschrift):

Auch am Bundesverwaltungsgericht sind in bestimmten Eilverfahren nach dem Staatsschutz- und Nachrichtendienst-Gesetz (SNG), BGBl. I Nr. 5/2016, rasch Entscheidungen zu treffen, weshalb vergleichbar den für Strafsachen zuständigen Landesgerichten fortan beim Bundesverwaltungsgericht zumindest eine Rufbereitschaft, allenfalls ein Journaldienst einzurichten ist. Die Regelungen orientieren sich an den §§ 38, 39 GOG, wobei eine verpflichtende Anwesenheit im Amt angesichts der zunehmenden Digitalisierung, insbesondere der durch den digitalen Gerichtsakt und moderne Telekommunikationsmöglichkeiten eröffneten Möglichkeit, von zuhause aus den Dienst zu versehen, nicht mehr zeitgemäß und erforderlich erscheint. Für den Journaldienst gilt daher der allgemeine Grundsatz der §§ 60, 211 Abs. 1 RStDG. Zur erforderlichen besoldungsrechtlichen Anpassung siehe Art. 5 Z 1 zu § 66 Abs. 3 RStDG.

Auch wenn § 38 GOG zutreffend als allgemeiner Rechtsgrund für die Einrichtung einer Rufbereitschaft bzw. eines Journaldienstes und nicht als zahlenmäßige Festlegung auf „eine Richterin oder einen Richter“ zu verstehen ist, soll zur Vermeidung von Missverständnissen semantisch sauber klargestellt werden, dass, so wie das in der ordentlichen Gerichtsbarkeit bei den für Strafsachen zuständigen Gerichtshöfen erster Instanz gelebte Praxis ist, im Bedarfsfall auch mehrere Richterinnen und Richter Rufbereitschaft bzw. Journaldienst versehen können.

Zu Z 3 (§ 20):

Bislang hatte das Bundesverwaltungsgericht alle Erkenntnisse und Beschlüsse, die nicht bloß verfahrensleitender Natur waren, in anonymisierter Form im Rechtsinformationssystem des Bundes (RIS) zu veröffentlichen. Seit Bestehen des Bundesverwaltungsgerichts wurden auf Basis dieser Bestimmung bis dato weit über 170.000 Erkenntnisse und Beschlüsse anonymisiert und kundgemacht.

Um eine Entlastung der Evidenzstelle des Bundesverwaltungsgerichts, die für die Anonymisierung jeder einzelnen zu veröffentlichenden Entscheidung zuständig ist, zu erreichen, soll künftig die Verpflichtung zur Veröffentlichung jener Entscheidungen entfallen, die keine (zusätzlichen) rechtsrelevanten Informationen enthalten. Damit wird auch einer Überfrachtung des RIS mit Entscheidungen, denen kein inhaltlicher Informationsmehrwert zukommt, vorgebeugt.

In diesem Sinne sollen etwa gekürzte Ausfertigungen von Entscheidungen, die im Wesentlichen lediglich den Spruch der Entscheidung sowie den Hinweis auf den Verzicht auf die Erhebung von Rechtsmitteln bzw. den Verzicht auf die Ausfertigung des Erkenntnisses enthalten, nicht mehr der Veröffentlichungspflicht unterliegen. Ebenfalls ausgenommen von einer Pflicht zur Veröffentlichung werden jene Entscheidungen, die in einer Vielzahl faktisch gleichlautend ergehen, wie etwa in Verfahren mit zahlreichen Beschwerdeführerinnen und Beschwerdeführern bzw. mitbeteiligten Parteien oder asylrechtlichen Familienverfahren, in denen mehrere Familienmitglieder inhaltlich gleichlautende Entscheidungen erhalten. Berichtigungsbeschlüsse und Beschlüsse über die Gebühren der nichtamtlichen Sachverständigen, Dolmetscherinnen und Dolmetscher werden ebenfalls von der Veröffentlichungspflicht ausgenommen wie Beschlüsse betreffend Einstellung oder Gegenstandslosigkeit des Verfahrens.

Die künftig von der Veröffentlichungspflicht auszunehmenden Erkenntnisse und Beschlüsse stellen ausdrücklich keine Informationen von allgemeinem Interesse im Sinne des Art. 22a Abs. 1 B-VG idF BGBl. I Nr. 5/2024 dar.

Ebenso sollen im Zusammenhang mit der Beantragung einer Maßnahme nach § 11 Abs. 1 Z 8 oder 9 SNG ergehende Beschlüsse des BVwG im Interesse an Geheimhaltung der konkreten Durchführungsparameter einer Nachrichtenüberwachung nicht im Rechtsinformationssystem des Bundes (RIS) veröffentlicht werden. Auch wenn nach Art. 22a Abs. 1 B-VG und dem IFG ab 1. September 2025 Informationen von allgemeinem Interesse zu veröffentlichen sind, sieht § 6 Abs. 1 Z 4 IFG im Interesse der Aufrechterhaltung der öffentlichen Ordnung und Sicherheit eine Ausnahme von der Veröffentlichungspflicht vor. Dieser Ausnahmetatbestand ist in den gegenständlichen Verfahren jedenfalls immer anzunehmen.

Zu Z 4 (§ 27 Abs. 10):

Es handelt sich um die Inkrafttretensbestimmung.

Zu Art. 5 (Änderung des Richter- und Staatsanwaltschaftsdienstgesetzes)

Zu Z 1 (§ 66 Abs. 3):

Da nach Art. 4 Z 2 des vorgeschlagenen Entwurfs mit § 16a BVwGG eine Rufbereitschaft, allenfalls ein Journaldienst einzurichten ist, bedarf es auch der besoldungsrechtlichen Anpassung in § 66 Abs. 3.

Zu Z 2 (§ 212 Abs. 83):

Es handelt sich um die Inkrafttretensbestimmung.