REPUBLIK ÖSTERREICH DATENSCHUTZRAT

An das
Bundesministerium für Inneres
Herrengasse 7
1010 Wien

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

BMJ - Kompetenzstelle GDSR (Geschäftsstelle des Datenschutzrates)

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

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

Geschäftszahl: 2024-0.679.067

GZ des Begutachtungsentwurfes:
2024-0.148.142

Entwurf eines Bundesgesetzes, mit dem das Staatsschutz- und Nachrichtendienstgesetz geändert wird; Stellungnahme des Datenschutzrates

Der Datenschutzrat hat in seiner 279. Sitzung am 23. September 2024 einstimmig beschlossen, zu der im Betreff genannten Thematik folgende Stellungnahme abzugeben:

I. Materialien zum Entwurf

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

2 Andererseits habe die Praxis laut den Erläuterungen seit Inkrafttreten des Staatsschutz- und Nachrichtendienst-Gesetzes (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.

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

4 Schließlich würde es sich um Ergänzungen des Deliktskatalogs der verfassungsgefährdenden Angriffe um für den Verfassungsschutz relevante Tatbestände des Strafgesetzbuches und des Waffengesetzes sowie um eine redaktionelle Verschiebung handeln.

II. Inhaltliche Bemerkungen

A. Grundsätzliches:

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

6 Konkrete Angaben zur Erforderlichkeit sowie zur Eignung dieser Maßnahme sind aus den vorliegenden Erläuterungen nicht ausreichend erkennbar. Seitens des informierten Vertreters der DSN wurden in der Sitzung des DSR zwar Anwendungsfälle zur Begründung der Erforderlichkeit genannt, die Erläuterungen müssten aber um entsprechende Begründungen und Datenmaterial ergänzt werden. Ebenso sollten Ausführungen zur erwartbaren Häufigkeit der Anwendung der Maßnahme aufgenommen werden.

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

8 b. Dem Begutachtungsentwurf ist kein Vorblatt und keine (vereinfachte) wirkungsorientierte Folgenabschätzung angeschlossen. Nachdem der Entwurf unzweifelhaft die Verarbeitung zahlreicher personenbezogener Daten regelt, wäre – neben den allgemeinen Ausführungen in den Erläuterungen – auch im Rahmen der (vereinfachten) wirkungsorientierten Folgenabschätzung darzulegen, ob für die betreffenden Datenverarbeitungen eine Datenschutz-Folgenschätzung gemäß Art. 35 DSGVO erforderlich ist oder nicht.

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

B. Zum Entwurf:

Zu Z 4 (§ 6 Abs. 5):

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

11 In datenschutzrechtlicher Hinsicht stellt sich die Frage, welche Konsequenzen die Möglichkeit zur punktuellen Wahrnehmung von Aufgaben des Staatsschutzes durch die für den Aufgabenbereich Nachrichtendienst zuständige Organisationseinheit der Direktion in Bezug auf die Weiterverarbeitung personenbezogener Daten für andere Zwecke als jenen, zu dem sie ermittelt wurden, hat.

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

13 Die mit einer punktuellen Ermächtigung iSd § 6 Abs. 5 verbundenen Auswirkungen in Bezug auf Datenverarbeitungen sollten in den Erläuterungen näher dargestellt werden.

Zu Z 5 (§ 9 Abs. 2a):

14 Den Erläuterungen zufolge handelt es sich im Wesentlichen um eine redaktionelle Verschiebung des § 11 Abs. 1a zur Klarstellung, dass sich bereits die genannte Regelung grundsätzlich auf die Verarbeitung personenbezogener Daten im Nachrichtendienst bezieht.

15 Unklar ist jedoch der normative Gehalt dieser (im Wortlaut geringfügig veränderten) Regelung, zumal das 3. Hauptstück bereits konkrete, aufgabenbezogene und begrenzte Ermächtigungsnormen zur Verarbeitung personenbezogener Daten enthält. Eine zusätzliche horizontale Datenverarbeitungsermächtigung (die dem Wortlaut des vorgeschlagenen § 9 Abs. 2a grundsätzlich entnommen werden könnte) stünde in einem klaren Spannungsverhältnis zur datenschutzrechtlich gebotenen Zweckbindung (vgl. § 37 Abs. 1 Z 2 DSG) sowie zum aus dem Grundrecht auf Datenschutz (§ 1 DSG) erfließenden datenschutzrechtlichen Determinierungsgebot.

16 Soweit die Regelung auf ein Gebot des Einsatzes geeigneter und besonders geschulter Bediensteter abzielt, wäre dies nicht als bloße „Kann“-Bestimmung (und somit optional) zu formulieren, sondern müsste in Form einer Verpflichtung angeordnet werden (etwa „Zur Verarbeitung personenbezogener Daten nach diesem Hauptstück durch die für den Aufgabenbereich Nachrichtendienst zuständige Organisationseinheit der Direktion sind geeignete und besonders geschulte Bedienstete heranzuziehen.“).

Allerdings stellt sich in diesem Zusammenhang allgemein die Frage, ob das Kriterium der „Eignung“ überhaupt gesonderter Erwähnung bedarf (auch im Hinblick auf die logische Folgefrage, was das Fehlen einer solchen Vorgabe in den anderen Bereichen bedeutet; ein Einsatz ungeeigneter Bediensteter sollte auch sonst nicht in Betracht gezogen werden).

Zu Z 6 (§ 11 Abs. 1):

17 a. Mit den vorgeschlagenen Änderungen in den Z 1, 2, 3, 5 und 7 werden die Zulässigkeitsschwellen für die dort geregelten Ermittlungsmaßnahmen gesenkt; die Erläuterungen verweisen in diesem Zusammenhang nur pauschal auf die bisweilige Erforderlichkeit des gleichzeitigen Einsatzes mehrerer Ermittlungsmaßnahmen.

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

19 b. Mit der in den Z 8 und 9 neu vorgesehenen Ermächtigung zur Überwachung von (verschlüsselten) Nachrichten (§ 134 Z 3 StPO) werden weitreichende Eingriffe in das Grundrecht auf Datenschutz ermöglicht.

20 Die Erforderlichkeit und Verhältnismäßigkeit der betreffenden Grundrechtseingriffe zu den damit verfolgen Zwecken ist vornehmlich vom Bundesministerium für Inneres zu beurteilen. Auf die Anmerkungen unter Pkt. II.A. wird in diesem Zusammenhang verwiesen.

21 Die Überwachung verschlüsselter Nachrichten nach Z 9 erfolgt „durch Einbringen eines Programms in ein Computersystem“ eines Betroffenen nach § 6 Abs. 2. Inwieweit derartige Programme technisch so gestaltet werden können, dass tatsächlich nur von der konkreten Bewilligung umfasste personenbezogene Daten verarbeitet werden, kann in technischer und datenschutzrechtlicher Hinsicht nicht abschließend beurteilt werden. In datenschutzrechtlicher Hinsicht setzt dies aber jedenfalls voraus, dass die Abgrenzung bereits unmittelbar bei der Ermittlung der personenbezogenen Daten (und nicht etwa erst bei deren Ausleitung) erfolgt. Fraglich ist, ob auch die technischen Vorgänge vor der Ausleitung eine Verarbeitung personenbezogener Daten iSd § 36 Abs. 2 Z 2 DSG darstellen und davon auch Daten umfasst sind, die nicht zur Ausleitung bestimmt sind.

22 Durch die (remote-)Einbringung und Nutzung von Überwachungsprogrammen in Computersystemen im Rahmen der Z 9 könnten Sicherheitslücken geschaffen werden, die in der Folge auch von Dritten (insbesondere Kriminellen, aber zB auch ausländischen Nachrichtendiensten) genutzt werden könnten. § 15a Abs. 5 zweiter Satz ordnet an, dass das eingebrachte Programm „nach dem Stand der Technik" gegen unbefugte Nutzung zu schützen ist, womit eine solche wohl nicht von vornherein ausgeschlossen werden kann. Die damit verbundenen Gefahren und Risiken für die Betroffenen nach § 6 Abs. 2, deren Kommunikationspartner sowie gegebenenfalls auch Dritte bzw. die Allgemeinheit sind für die Beurteilung der abstrakten Verhältnismäßigkeit der Ermittlungsmaßnahme nach § 11 Abs. 1 Z 9 wesentlich, weshalb auf diesen Aspekt in den Erläuterungen näher eingegangen werden sollte.

23 Den Erläuterungen zufolge dürfen Gegenstand der Überwachung nach Z 8 und 9 auch „mit dem Übertragungsvorgang unmittelbar in Zusammenhang stehende Stamm-, Zugangs- und Verkehrsdaten" sein. Dies scheint nicht dem Gesetzestext zu entsprechen, zumal die Z 8 und 9 an das Konzept der Überwachung von Nachrichten iSd § 134 Z 3 StPO anknüpfen. Stamm-, Zugangs- und Verkehrsdaten sind gerade keine „Nachrichten", sondern wären erforderlichenfalls im Wege einer (ggf. parallel angeordneten) Ermittlungsmaßnahme nach Z 7 zu ermitteln. Die Erläuterungen sollten entsprechend überarbeitet werden.

Zu Z 9 (§ 14 Abs. 2):

24 Wenngleich die vorgesehene Verschiebung des bisherigen § 11 Abs. 1 Z 7 letzter Satz betreffend die Ermächtigung des Rechtsschutzbeauftragten in § 14 Abs. 2 in systematischer Hinsicht nachvollziehbar erscheint, stellt sich die Frage nach dem Mehrwert der betreffenden Regelung gegenüber den bereits jetzt in § 14 Abs. 2 geregelten, auch für andere Ermittlungsmaßnahmen geltenden Vorgaben für die Ermächtigung. Insbesondere stellt sich die Frage, ob die voraussichtliche Erforderlichkeit zur „Erreichung des Zwecks" etwas Anderes ist als die voraussichtliche Erforderlichkeit zur „Erfüllung der Aufgabe" (letztere Formulierung findet sich auch im neuen § 15a Abs. 3) und 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. Eine Konsolidierung sollte geprüft werden. Die informierten Vertreter sagten zu, die Praktikabilität der Fristen mit dem Rechtsschutzbeauftragten abzuklären.

Zu Z 12 (§ 15a):

25 a. Gemäß Abs. 2 Z 8 hat der Antrag auf Bewilligung bei einer Überwachung gemäß § 11 Abs. 1 Z 9 „die beabsichtigte Art des Einsatzes technischer Mittel" zu enthalten.

In den Erläuterungen sollte näher dargelegt werden, welche konkreten Angaben damit gemeint und wie detailliert diese zu gestalten sind.

26 b. Gemäß Abs. 5 Z 3 ist bei der Durchführung der Ermittlungsmaßnahme nach § 11 Abs. 1 Z 9 technisch sicherzustellen, dass das eingebrachte Programm nach Beendigung der Ermittlungsmaßnahme entfernt oder funktionsunfähig wird. Unbeschadet der Frage, inwieweit dies in technischer Hinsicht – auch mit Blick auf allfällige spätere Veränderungen des Computersystems durch den/die Benutzer – vorweg sichergestellt werden kann, sind die rechtlichen Konsequenzen, wenn sich dies im Zuge einer bereits laufenden Ermittlungsmaßnahme nachträglich als nicht (mehr) möglich erweisen sollte (etwa, weil eine vorzeitig erforderliche „remote"-Betätigung wegen Weitergabe des Geräts [vgl. das Beispiel in den Erläuterungen] mangels Internetverbindung nicht mehr möglich ist), unklar. Die Fortführung einer Ermittlungsmaßnahme, die nicht mehr im Einklang mit den in § 15a Abs. 5 geregelten Anforderungen an die Durchführung steht, sollte jedenfalls unzulässig sein.

27 c. Im Hinblick auf Abs. 6 Z 3 ist fraglich, ob der Begriff der „nicht nur flüchtigen" Veränderungen ausreichend klar abgrenzbar ist.

28 d. In Bezug auf die in Abs. 8 Z 1 vorgesehene (gesonderte) Aufbewahrung ermittelter Nachrichten bis zur Erteilung einer Ermächtigung des Rechtsschutzbeauftragten für die Weiterverwendung für eine andere Aufgabe nach § 6 Abs. 2 stellt sich die Frage, inwieweit hier eine Verpflichtung zur umgehenden Einholung einer entsprechenden Ermächtigung (und somit Klärung der Zulässigkeit der Weiterverarbeitung) besteht. Eine Aufbewahrung ermittelter Nachrichten „auf Vorrat", wenn zwar ein begründeter Gefahrenverdacht für einen anderen verfassungsgefährdenden Angriff, aber kein unmittelbarer Handlungsbedarf besteht, sollte jedenfalls vermieden werden.

29 Zur datenschutzrechtlichen Rollenverteilung iZm der Überwachung verschlüsselter Nachrichten:

30 Den Erläuterungen (S. 8, vorletzter Absatz) zufolge ist der Bundesminister für Inneres datenschutzrechtlich Verantwortlicher „der Software sowie der im Rahmen des § 15a Abs. 6 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)."

31 Eine solche der datenschutzrechtlichen Rollenverteilung kann dem Gesetzestext nicht entnommen werden und scheint auch nicht den Kriterien des § 36 Abs. 2 Z 8 DSG zu entsprechen:

32 Die datenschutzrechtliche Verantwortlichenrolle bezieht sich grundsätzlich auf konkrete Verarbeitungsvorgänge und nicht auf ein abstraktes Verarbeitungssystem. Verantwortlicher ist gemäß § 36 Abs. 2 Z 8 DSG „die zuständige Behörde, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“.

33 Die zitierten Erläuterungen erwecken den Eindruck, dass für Datenverarbeitungen nach § 11 Abs. 1 Z 9 eine (alleinige) Verantwortlichkeit des Bundesministers für Inneres bestehen könnte. Dies entspricht aber nicht dem datenschutzrechtlichen Rollenkonzept im Lichte der faktischen Abläufe:

34 Verantwortlicher einer Überwachung von Nachrichten iSd § 11 Abs. 1 Z 8 und 9 ist grundsätzlich jene zuständige Behörde (§ 36 Abs. 2 Z 7 DSG), die die Entscheidung über die Durchführung der Ermittlungsmaßnahme trifft. Der Umstand, dass die Überwachung von Nachrichten im Falle der Z 9 „durch Einbringen eines Programms in ein Computersystem“ erfolgt, ändert an deren Verantwortlichkeit grundsätzlich nichts. Eine faktische Entscheidungsingerenz des Bundesministers für Inneres im Zusammenhang mit dem eingesetzten Überwachungsprogramm (die dem Gesetzestext allerdings nicht zu entnehmen ist) könnte nur dazu führen, dass dieser ggf. als gemeinsam Verantwortlicher für die betreffenden Datenverarbeitungen hinzutritt.

35 Im Falle einer solchen gemeinsamen Verantwortlichkeit wären gemäß § 47 DSG in einer Vereinbarung in transparenter Form die jeweiligen Aufgaben der jeweiligen gemeinsam Verantwortlichen nach dem DSG festzulegen, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß § 43 DSG nachkommt, sofern und soweit diese nicht gesetzlich festgelegt sind, und eine Anlaufstelle für die betroffenen Personen anzugeben.

36 Zur Vermeidung von Rechtsunklarheiten und Vollzugsproblemen wird – soweit es sich nicht um eine alleinige Verantwortlichkeit der zuständigen Behörde, die die Ermittlungsmaßnahme einsetzt, handelt – empfohlen, die datenschutzrechtliche Rollenverteilung iZm Datenverarbeitungen nach § 11 Abs. 1 Z 9 bereits im Gesetzestext klar zu regeln.

37 Zu beachten ist, dass eine von den allgemeinen Kriterien des § 36 Abs. 2 Z 8 DSG abweichende Festlegung nur zulässig ist, soweit die Zwecke und Mittel der Verarbeitung im Gesetz geregelt werden. Überdies muss sichergestellt sein, dass im Falle einer gesetzlichen Festlegung des Verantwortlichen dieser in der Lage ist, den datenschutzrechtlichen Verantwortlichenpflichten vollinhaltlich nachzukommen.

Für den Datenschutzrat:
Der Vorsitzende
OFENAUER
24. September 2024

Elektronisch gefertigt