REPUBLIK ÖSTERREICH DATENSCHUTZRAT

An das
Bundesministerium für Inneres

Per E-Mail:
bmi-III-1-stellungnahmen@bmi.gv.at
team.s@bmj.gv.at

BMJ - DSR (Geschäftsstelle des Datenschutzrates)
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: 2021-0.332.342

GZ des Begutachtungsentwurfes: 2021-0.206.281

Entwurf eines Bundesgesetzes, mit dem das Polizeiliche Staatsschutzgesetz, das Sicherheitspolizeigesetz, das Strafgesetzbuch, die Strafprozessordnung 1975 und das Tilgungsgesetz 1972 geändert werden; Stellungnahme des Datenschutzrates

Der **Datenschutzrat** hat in seiner 257. Sitzung am 6. Mai 2021 **einstimmig beschlossen**, zu der im Betreff genannten Thematik folgende Stellungnahme abzugeben:

I. Allgemeines

1 **Laut den Erläuterungen** habe sich aufgrund internationaler Vorgaben sowie den Vorkommnissen in den letzten Jahren rund um das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung gezeigt, dass es einer organisatorischen Neustrukturierung und inhaltlichen Professionalisierung im Bereich des österreichischen Verfassungsschutzes bedarf. Der österreichische Verfassungsschutz soll daher organisatorisch neu strukturiert und inhaltlich professionalisiert werden. Zur Vornahme einer entsprechenden Reformierung wurde im BMI das Projekt „BVT neu“ geschaffen, welches den polizeilichen Nachrichtendienst und Staatsschutz nach Maßgabe internationaler Standards neu ausrichten soll. Zweck des Entwurfes sei daher **laut den Erläuterungen** die Reformierung des polizeilichen Nachrichtendienstes und des österreichischen Verfassungsschutzes nach

Maßgabe internationaler Standards durch Änderung des Polizeilichen Staatsschutzgesetzes, des Sicherheitspolizeigesetzes, des Strafgesetzbuches, der Strafprozessordnung und des Tilgungsgesetzes. Das vormalige Bundesamt für Verfassungsschutz und Terrorismusbekämpfung soll künftig den Namen „Direktion Staatsschutz und Nachrichtendienst“ tragen. Den bisherigen Landesämtern für Verfassungsschutz und Terrorismusbekämpfung soll künftig in erster Linie die Aufgabe des Staatsschutzes zukommen, weshalb dies auch in ihrer Bezeichnung ersichtlich sein soll. Anstelle des bisher verwendeten Terminus „polizeilicher Staatsschutz“ soll künftig der Begriff „Verfassungsschutz“ als Überbegriff die beiden Aufgabenbereiche „Staatsschutz“ und „Nachrichtendienst“ zusammenfassen.

II. Datenschutzrechtliche Bemerkungen

Zu Art. 1 (Änderung des Polizeilichen Staatsschutzgesetzes):

Zu Z 10 (§ 4 Z 5):

2 **§ 4 Z 5** sieht vor, dass die Leistung von **Amtshilfe an ausländische Sicherheitsbehörden**, denen ausschließlich die Gefahrenerforschung obliegt, „unabhängig von den sonstigen Aufgabenzuweisungen nach diesem Bundesgesetz“ ausschließlich der für den Aufgabenbereich Nachrichtendienst zuständigen Organisationseinheit der Direktion zukommt.

3 Aus datenschutzrechtlicher Sicht stellt sich die Frage, ob aufgrund dieser **Konzentration der Zuständigkeit zur internationalen Amtshilfeleistung** die für den Aufgabenbereich Nachrichtendienst zuständigen Organisationseinheit der Direktion im Rahmen der Amtshilfe ggf. auch **personenbezogene Daten übermittelt, die sie nicht selbst als Verantwortlicher verarbeitet**. Diesfalls wäre eine **Übermittlungsregelung** vom ursprünglichen Verantwortlichen zur für den Aufgabenbereich Nachrichtendienst zuständigen Organisationseinheit der Direktion erforderlich. Es wird angeregt, auf diesen Aspekt in den Erläuterungen einzugehen und gegebenenfalls erforderliche ergänzende Regelungen zu treffen.

Zu Z 13 (§ 6a):

4 Nach **§ 6a Abs. 1 und 2** ist im Rahmen der Fallkonferenz Staatsschutz die **Übermittlung personenbezogener Daten**, die im Rahmen der Sicherheitspolizei verarbeitet wurden, **an die Teilnehmer der Fallkonferenz** (dh. Behörden und „Einrichtungen, die mit dem Vollzug öffentlicher Aufgaben, insbesondere zum Zweck der Deradikalisierung, Extremismusprävention oder der sozialen Integration von Menschen betraut sind“) vorgesehen.

5 Im vorliegenden Zusammenhang („Gefahrenverdacht“) handelt es sich um **strafrechts-relevante Daten**, deren Verarbeitung erheblich in die Rechte der betroffenen Personen eingreift. Die Übermittlung personenbezogener Daten an die Teilnehmer der Fallkonferenz Staatsschutz durch die für den Aufgabenbereich Staatsschutz zuständigen Organisationseinheiten gemäß § 1 Abs. 3 erfolgt im Rahmen der **Hoheitsverwaltung** und bedarf daher jedenfalls einer **gesetzlichen Grundlage**, die den **Anforderungen des § 1 Abs. 2 DSG** entsprechen muss. Im Hinblick auf § 1 Abs. 2 DSG iVm Art. 18 B-VG und die Anforderungen an den Grad der Bestimmtheit gesetzlicher Eingriffe in das Grundrecht auf Datenschutz hat der Verfassungsgerichtshof festgehalten, dass eine Ermächtigungsnorm iSd § 1 Abs. 2 DSG **ausreichend präzise, also für jedermann vorhersehbar, bezeichnen muss, unter welchen Voraussetzungen die Ermittlung bzw. die Verarbeitung der Daten für die Wahrnehmung konkreter Verwaltungsaufgaben zulässig ist** (VfSlg. 18.146/2007; 16.369/2001; zuletzt Erkenntnis vom 11.12.2019, G 72-74/2019 ua., Rz 64 ff).

6 Um diesen Vorgaben zu genügen, bedarf es näherer Determinierungen in § 6a:

7 Zunächst ist zu bemerken, dass der **Kreis der in § 6a Abs. 1 angesprochenen Einrichtungen** unbestimmt ist und jedenfalls näher eingeschränkt werden sollte. Während die Betrauung mit dem Vollzug öffentlicher Aufgaben zum Zweck der Deradikalisierung oder Extremismusprävention hinreichend klar abgrenzbar sein dürfte, sollte der Zweck der „**sozialen Integration von Menschen**“ näher **erläutert** werden.

8 Der Vollzug öffentlicher Aufgaben ist zudem nicht auf die genannten Bereiche beschränkt („insbesondere“), weshalb nach dem Wortlaut des § 6a Abs. 1 potentiell jegliche mit der Vollziehung hoheitlicher Aufgaben betraute Einrichtung als Teilnehmer der Fallkonferenz in Frage käme. Der **Kreis der in Frage kommenden Einrichtungen** sollte vor diesem Hintergrund jedenfalls **im Gesetzestext** selbst **auf das erforderliche Maß eingeschränkt werden**.

9 Den Erläuterungen zufolge werden durch die Fallkonferenz Staatsschutz **keine hoheitlichen Aufgaben an Dritte übertragen**, sondern erfolgt lediglich ein Informationsaustausch mit den im Einzelfall relevanten Behörden und Einrichtungen.

10 Ungeachtet dessen stellt die Formulierung „die mit dem Vollzug öffentlichen Aufgaben […] betraut sind“ in § 6a Abs. 1 dennoch klar auf **Private** ab, **die bereits im Rahmen der Hoheitsverwaltung herangezogen werden** (wenngleich diese nicht zusätzlich mit hoheitlichen Aufgaben im Rahmen der Fallkonferenz betraut werden). Da es sich hierbei um ein wesentliches (einschränkendes) Kriterium hinsichtlich des potentiellen

Teilnehmerkreises an der Fallkonferenz handelt, sollte dieser Umstand in den Erläuterungen klargestellt werden.

11 Die **Datenarten**, die für Zwecke der Fallkonferenz übermittelt werden dürfen, sollten – zumindest beispielhaft – näher präzisiert werden.

12 In den Erläuterungen zu § 6a wird auf den allgemein geltenden Grundsatz der Verhältnismäßigkeit und Erforderlichkeit (§§ 51 f SPG, § 9 Abs. 2) verwiesen, aus dem sich ergebe, dass die Datenübermittlung für Zwecke der Fallkonferenz Staatsschutz ohnedies nur im unbedingt erforderlichen Ausmaß erfolgen darf. Damit würde jedoch die **Verhältnismäßigkeitsprüfung** zur Gänze der **Vollzugsebene überlassen**. Im Sinne des datenschutzrechtlichen Determinierungsgebots sind zur Sicherstellung der Verhältnismäßigkeit des Eingriffs in das Grundrecht auf Datenschutz **Einschränkungen bereits auf gesetzlicher Ebene geboten.**

13 **§ 6a Abs. 2** verpflichtet die Teilnehmer der Fallkonferenz – sofern sie nicht ohnehin der Amtsverschwiegenheit unterliegen – zur **vertraulichen Behandlung** der übermittelten Daten. Abseits dieser Vertraulichkeitsverpflichtung enthält das SNG, soweit ersichtlich, **keine Regelungen über die Verarbeitung personenbezogener Daten durch die empfangenden Einrichtungen**. Insbesondere regelt das 3. Hauptstück des SNG nur die Verarbeitung personenbezogener Daten durch Organisationseinheiten gemäß § 1 Abs. 3.

14 Aufgrund des Verhältnismäßigkeitsgrundsatzes sowie der Grundsätze der Zweckbindung und Datenminimierung (Art. 5 Abs. 1 lit. b und c DSGVO) sollte grundsätzlich schon aus dem **Gesetz** hervorgehen, **welche personenbezogenen Daten zu welchen konkreten Zwecken benötigt werden und zu verarbeiten sind**. Überdies sollte ein ausdrückliches **Verarbeitungsverbot für andere Zwecke** verankert werden, um unzulässige Weiterverarbeitungen innerhalb der Einrichtungen (die nicht zwangsläufig gegen die Vertraulichkeitsverpflichtung verstoßen müssen und diesfalls auch nicht unter den diesbezüglichen Verwaltungsstraftatbestand in § 17e Abs. 1 Z 1 fallen würden) hintanzuhalten.

15 Soweit die **Erläuterungen** im Zusammenhang mit einer allfälligen Weiterverarbeitung zu anderen Zwecken durch Teilnehmer auf die entsprechenden Bestimmungen der **DSGVO** verweisen, ist festzuhalten, dass im vorliegenden Zusammenhang aufgrund der besonderen Sensibilität der betroffenen Daten (Gefahrenverdacht, personenbezogene Daten aus der Hoheitsverwaltung) und der Intensität des damit verbundenen

Grundrechtseingriffs **spezifische Schranken für die Weiterverarbeitung** aus datenschutzrechtlicher Sicht geboten erscheinen.

16 Es wird darauf hingewiesen, dass die **Teilnehmer der Fallkonferenz Staatsschutz** hinsichtlich der in diesem Rahmen erhaltenen Daten selbst **Verantwortliche** (Art. 4 Z 7 DSGVO bzw. § 36 Abs. 2 Z 8 DSG) werden. In diesem Zusammenhang wäre zu prüfen, ob – insbesondere zur Vermeidung einer Umgehung von Auskunftsbeschränkungen, die den für den Aufgabenbereich Staatsschutz zuständigen Organisationseinheiten der Direktion zur Verfügung stehen – allfällige **Beschränkungen der Betroffenenrechte** (Information, Auskunft, Richtigstellung, Löschung) gegenüber den Teilnehmern der Fallkonferenz Staatsschutz erforderlich sind. Die in den §§ 43, 44 und 45 DSG unmittelbar vorgesehenen Einschränkungen von Betroffenenrechten gelten nur für zuständige Behörden iSd § 36 Abs. 2 Z 7 DSG; soweit die einbezogenen Behörden und Einrichtungen keine solchen zuständigen Behörden sind (und daher der DSGVO unterliegen), wäre dafür eine gesetzliche **Regelung nach Art. 23 DSGVO** erforderlich, die die **Erfordernisse des Art. 23 Abs. 2 DSGVO** zu erfüllen hätte.

Zu den Z 15 und 34 (§ 7 Abs. 2 und § 12 Abs. 4):

17 **§ 7 Abs. 2** ermächtigt die Organisationseinheiten gemäß § 1 Abs. 3 dazu, näher bezeichnete Deradikalisierungseinrichtungen über deren Ersuchen „**bei ihrer Entscheidungsfindung**, ob eine bestimmte Personen vom Zweck der Einrichtung umfasst ist, im Einzelfall zu **unterstützen**“. Korrespondierend dazu werden in § 12 Abs. 4 Übermittlungen an Einrichtungen (§ 7 Abs. 2) ermöglicht, „soweit dies für die Erfüllung der Aufgaben der Einrichtung unbedingt erforderlich ist und die Einrichtung sich zur vertraulichen Behandlung verpflichtet hat“.

18 Diesbezüglich wird auf das zu § 6a Gesagte hingewiesen, das auch **im Zusammenhang mit der Übermittlung personenbezogener Daten an Deradikalisierungseinrichtungen** sowie die **weitere Verarbeitung** der erhaltenen personenbezogenen Daten **durch diese** – insbesondere auch dann, wenn die Betreuung der betroffenen Person in der Folge übernommen wird – gilt.

Zu den Z 16 und 21 (§ 8 Abs. 1 und § 10 Abs. 1):

19 Gemäß **§ 8 Abs. 1** obliegt der für den Aufgabenbereich Nachrichtendienst zuständigen Organisationseinheit der Direktion für Zwecke des § 1 Abs. 2 die Gewinnung und Analyse von Information zur Beurteilung von verfassungsschutzrelevanten Bedrohungslagen. Gemäß **§ 10 Abs. 1** dürfen die **„Organisationseinheiten gemäß § 1 Abs. 3“ personenbezogene Daten für die in den Z 1 bis 4 genannten Zwecke verarbeiten**. Den

Erläuterungen zufolge ermöglicht § 10 Abs. 1 die Verarbeitung zu Zwecken des Nachrichtendienstes (§ 8 Abs. 1) – wenngleich diese Aufgabe nur der Direktion zukommen soll – weiterhin durch alle Organisationseinheiten gemäß § 1 Abs. 3, somit auch durch die für Staatsschutz zuständigen Organisationseinheiten der Landespolizeidirektionen. Dies sei insbesondere erforderlich, um die Weiterleitung von bei den für den Staatsschutz zuständigen Organisationseinheiten der Landespolizeidirektionen einlangenden Informationen, die die Aufgabe des § 8 betreffen, an die Direktion zu ermöglichen.

20 Diese Ausführungen stehen in klarem **Widerspruch zu § 9 Abs. 2**, demzufolge personenbezogene Daten von den Organisationseinheiten gemäß § 1 Abs. 3 gemäß dem 3. Hauptstück nur verarbeitet werden dürfen, soweit dies **zur Erfüllung der ihnen übertragenen Aufgaben erforderlich** ist, und sollten schon aus diesem Grund entfallen bzw. durch einen Verweis auf den sich aus § 9 Abs. 2 ergebenden Aufgabenbezug ersetzt werden.

21 Aus datenschutzrechtlicher Sicht wird die grundsätzliche Trennung zwischen Staatsschutz und Nachrichtendienst begrüßt, aus der gesetzlichen Regelung des § 10 Abs. 1 scheint aber eine pauschale Ermächtigung von Behörden zur Datenverarbeitung für Zwecke außerhalb ihres Aufgabenbereiches hervorzugehen. Dies wäre auch **mit den allgemeinen grund- und unionsrechtlichen Anforderungen des Datenschutzes**, insbesondere mit dem aus dem **Grundrecht auf Datenschutz (§ 1 Abs. 2 DSG)** erfließenden datenschutzrechtlichen Determinierungsgebot, **nicht in Einklang zu bringen**. Eine Datenverarbeitung kann für die Erfüllung einer von der zuständigen Behörde wahrgenommenen Aufgabe (§ 38 DSG) von vornherein nur dann erforderlich und verhältnismäßig sein, wenn dieser eine entsprechende Aufgabe zukommt.

22 Dies bedeutet nicht, dass das in den Erläuterungen angesprochene **Weiterleiten** von Informationen an andere Organisationseinheiten für deren Bereich in jedem Fall unzulässig wäre. Eine solche Datenübermittlung **müsste aber im Gesetz – unter Beachtung der datenschutzrechtlichen Erfordernisse – explizit vorgesehen und geregelt werden**. Dies könnte zB im Rahmen von Ermittlungen vom Staatsschutz erlangte Informationen betreffen, die an den Nachrichtendienst übermittelt werden, weil diese in seinen Aufgabenbereich fallen.

Zu Z 22 (§ 10 Abs. 3):

23 Mit der Ausdehnung des Verweises in **§ 10 Abs. 3** auf die Erfüllung der **Aufgaben nach § 10 Abs. 1 Z 4 (Analyse und Information nach § 8)** wird die in Abs. 3 verankerte Berechtigung, von den dort genannten Stellen Auskünfte – deren Verweigerung nur in

engen Grenzen zulässig ist – zu verlangen, erheblich erweitert. Die – in den Erläuterungen lediglich abstrakt postulierte – **Erforderlichkeit und Verhältnismäßigkeit der Auskunftspflicht** in diesem Zusammenhang wäre in den **Erläuterungen** näher darzulegen und entsprechend zu begründen.

Zu Z 31 (§ 12 Abs. 1a):

24 Die Datenverarbeitungsermächtigung in § 12 Abs. 1a umfasst auch „sachverhalts-, tat- und fallbezogene Informationen“ sowie „Verwaltungsdaten, die [die Direktion] rechtmäßig ermittelt hat oder verarbeiten darf“. Im Hinblick auf die potentielle Reichweite dieser Ermächtigung sollten die genannten Begriffe nach Möglichkeit näher eingeschränkt, zumindest aber in den Erläuterungen näher präzisiert werden.

25 Die in **§ 12 Abs. 1a** vorgesehene Festlegung der **Höchstspeicherfrist** mit zehn Jahren sollte in den Erläuterungen begründet werden.

Zu Z 34 (§ 12 Abs. 4 SNG):

26 Im Hinblick auf **§ 12 Abs. 4,** demzufolge die **Übermittlung an „Einrichtungen (§ 7 Abs. 2**), soweit dies für die Erfüllung der Aufgabe der Einrichtung unbedingt erforderlich ist und die Einrichtung sich zur vertraulichen Behandlung verpflichtet hat“, **sowie „an Betreiber kritischer Infrastrukturen**, soweit dies für den Betrieb von wesentlicher Bedeutung ist“, wird auf die **Anmerkungen zu § 6a (Fallkonferenz Staatsschutz)** verwiesen. Zudem bestehen, soweit ersichtlich, keine Regelungen über die Verarbeitung der übermittelten personenbezogenen Daten durch die Betreiber kritischer Infrastrukturen; auch diesbezüglich wird auf die Anmerkungen zu § 6a verwiesen.

Zu Z 45 (4a. Hauptstück):

27 Im Hinblick auf die neu geschaffene **Unabhängige Kontrollkommission Verfassungsschutz** bedarf es eines **Regelungsregimes für Datenverarbeitungen**. Soweit ersichtlich, enthält das 4a. Hauptstück lediglich eine Amtsverschwiegenheits- und Geheimhaltungspflicht (§ 17a Abs. 3), ein Recht auf Einsicht und Kopien (§ 17c Abs. 2) sowie eine Löschungspflicht hinsichtlich dieser Kopien nach Berichterstattung (§ 17c Abs. 4). Im Hinblick daraus, dass es sich um höchst sensible Daten aus der Hoheitsverwaltung handelt und die Kontrollkommission als Verantwortlicher der DSGVO unterliegt, wären vorliegend zahlreiche Begleitregelungen zur Verarbeitung personenbezogener Daten durch die Kontrollkommission geboten (etwa betreffend Datensicherheit, Weiterverarbeitungsverbote usw.).

Zur Wirkungsorientierten Folgenabschätzung

28 Nachdem der Entwurf unzweifelhaft die **Verarbeitung zahlreicher personenbezogener Daten** regelt, wäre im Rahmen der (vereinfachten) wirkungsorientierten Folgenabschätzung zumindest darzulegen, ob für Datenverarbeitungen (insbesondere im Rahmen des SNG) eine **Datenschutz-Folgenschätzung gemäß § 52 DSG iVm Art. 35 DSGVO erforderlich ist** oder nicht. Dem vorliegenden Entwurf ist jedoch keine (vereinfachte) wirkungsorientierte Folgenabschätzung beigeschlossen.

29 Eine Datenschutz-Folgenabschätzung ist gemäß § 52 DSG iVm Art. 35 Abs. 1 DSGVO insbesondere in den Fällen des Art. 35 Abs. 3 DSGVO – und damit etwa für die umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 Abs. 1 DSGVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO – erforderlich.

30 Grundsätzlich trifft diese Verpflichtung zur Durchführungen der Datenschutz-Folgenabschätzung gemäß § 52 DSG iVm Art. 35 DSGVO den **Verantwortlichen** der Datenverarbeitung. Eine allfällige **Vorwegnahme** der Datenschutz-Folgenabschätzung müsste gemäß § 52 DSG iVm Art. 35 Abs. 10 DSGVO bereits **im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass dieser Rechtsgrundlage** erfolgen. Soweit dies (etwa für einzelne Datenverarbeitungen) nicht erfolgt, würde die Verpflichtung zur Durchführung der Datenschutz-Folgenabschätzung in diesem Umfang (wieder) den jeweiligen Verantwortlichen treffen.

Für den Datenschutzrat
Der Vorsitzende:
OFENAUER
10. Mai 2021

Elektronisch gefertigt