BUNDESKANZLERAMT VERFASSUNGSDIENST

GZ ● BKA-603.729/0001-V/5/2017
ABTEILUNGSMAIL ● **V@BKA.GV.AT**
BEARBEITER ● FRAU DR. MARTINA LAIS
HERR MAG. LORENZ DOPPLINGER (DATENSCHUTZ)
PERS. E-MAIL ● MARTINA.LAIS@BKA.GV.AT
LORENZ.DOPPLINGER@BKA.GV.AT
TELEFON ● **+43 1 53115-**202843
-202372
IHR ZEICHEN ●BMI-LR1340/0004-III/1/2017

An das
Bundesministerium für Inneres

Herrengasse 7
1010 Wien

Antwort bitte unter Anführung der GZ an die Abteilungsmail

Entwurf eines Bundesgesetzes, mit dem das Bundesgesetz über die internationale polizeiliche Kooperation (Polizeikooperationsgesetz – PolKG) geändert wird;
Begutachtung; Stellungnahme

Zu dem mit der do. oz. Note übermittelten Gesetzesentwurf nimmt das Bundeskanzleramt-Verfassungsdienst wie folgt Stellung:

I. Allgemeines

Es wird darauf hingewiesen, dass die Übereinstimmung des im Entwurf vorliegenden Bundesgesetzes mit dem Recht der Europäischen Union vornehmlich vom do. Bundesministerium zu beurteilen ist.

II. Inhaltliche Bemerkungen

Zu Z 3 (§ 8a):

Die Erläuterungen führen aus, dass sich der subjektive Rechtsschutz „im Übrigen“ (gemeint wohl: abgesehen von den Befugnissen des Rechtsschutzbeauftragten) nach den Bestimmungen des SPG richtet. Das PolKG enthält jedoch – ausgenommen § 17 für den besonderen Rechtsschutz beim Einschreiten der Sicherheitsbehörden im Ausland und ausländischer Sicherheitsbehörden im Inland – an keiner Stelle eine Regelung, welche die Anwendbarkeit der entsprechenden Bestimmungen des SPG anordnet, sodass sich dies aus dem SPG selbst ergeben müsste. Dies sollte für die im SPG enthaltenen Rechtsschutzvorrichtungen im

Einzelnen gesondert geprüft und in den Erläuterungen entsprechend dargelegt werden.

Zu Z 3 (§ 8a) aus Sicht des Datenschutz:

1. Die Ermächtigung zur Teilnahme an internationalen Informationsverbundsystemen ist in ihrer vorgeschlagenen Form zu pauschal, da sie nicht jenen Grad an Determinierung aufweist, der grundrechtlich geboten (Art. 18 B-VG, Art. 1 DSG 2000) und durch die Judikatur zur Ausgestaltung und Vorhersehbarkeit eines Grundrechtseingriffs gefordert ist (vgl. etwa VfSlg. 18.146/2007).

Zunächst sollten die Zwecke, zu denen Daten in internationalen Informationsverbundsystemen verwendet werden dürfen, deutlich enger und genauer festgelegt werden. Unklar erscheint hier auch die Abgrenzung zur Datenverwendung zu nachrichtendienstlichen Zwecken. Determinierungsbedürftig ist zudem, welche Arten von Daten verwendet – einerseits eingespeist und andererseits abgerufen – werden dürfen.

Zu unbestimmt erscheint die Ermächtigung ferner im Hinblick auf die unterschiedlichen Systemarchitekturen der hiervon erfassten Informationsverbundsysteme: So ermächtigt die Bestimmung anscheinend gleichermaßen zur Teilnahme an Systemen, die bloß mit gemeinsamen Indexdateien („Hit/No-Hit"-Verfahren) arbeiten, wie zur Teilnahme an Systemen, bei denen umfassende zentrale Datenbanken zum Zweck einer Direktabfrage angelegt werden.

Überdies ist nicht hinreichend sichergestellt, dass die im Rahmen eines Datenverbundes verwendeten Daten durchgehend (also auch bei den beteiligten ausländischen Stellen) einem angemessenen Datenschutzregime unterliegen. Dies ist insbesondere dann unerlässlich, wenn – wie hier – ein institutionalisierter und automatisierter Informationsaustausch angestrebt wird. Keinesfalls ausreichend ist es, darauf zu verweisen, dass ausländische Stellen ihre jeweiligen nationalen Gesetze und internationale Vereinbarungen einhalten – ergibt sich aus der systematischen Verankerung der vorgeschlagenen Bestimmung im PolKG und der umfassenden Formulierung „ausländische Sicherheitsbehörden" (§ 8a Abs. 1) doch, dass die Teilnahme an diesen Informationsverbundsystemen prinzipiell wohl auch Drittstaaten offenstehen soll. Insbesondere diese mangelnde Begrenzung des Kreises der Staaten, die potentiell an derartigen Informationsverbundsystemen teilnehmen können, macht zusätzliche Schutzbestimmungen erforderlich bzw.

unterläuft andernfalls die – auch unionsrechtlich determinierten – Vorgaben zur Auslandsdatenübermittlung (vgl. § 12 f DSG 2000).

Außerdem ist fraglich, ob der gegenständliche Entwurf einen hinreichend umfassenden und effektiven Rechtsschutzmechanismus gewährleistet: So nennt § 8a Abs. 2 nur das Auskunftsrecht (§ 26 DSG 2000), das überdies auf die „vom Bundesminister für Inneres als Auftraggeber verarbeiteten Daten“ beschränkt wird, womit den Erläuterungen zufolge jener Datenbestand gemeint ist, der vom Bundesminister für Inneres „eingegeben wurde“. Im Hinblick auf grundrechtliche Vorgaben ist es allerdings geboten, umfassende Betroffenenrechte zu gewährleisten, die sich auf sämtliche Datenverwendungen in Österreich beziehen. Es stellt sich weiters die Frage, wie der Betroffene seine Rechte effektiv geltend machen kann, wenn ihn betreffende Daten zwar bereits von anderen Teilnehmerstaaten in das Informationsverbundsystem eingespeist wurden und dem Bundesministerium für Inneres zur Abfrage zur Verfügung stehen, für den Betroffenen aber nicht feststellbar ist, wem gegenüber er seine Betroffenenrechte geltend machen kann.

In diesem Zusammenhang ist zu bedenken, dass die in § 8a Abs. 4 vorgesehene Befugnis des Rechtsschutzbeauftragten, Einblick in den nationalen Datenbestand zu nehmen, ausschließlich die gemäß § 8a Abs. 2 Z 2 verarbeiteten Daten betrifft, nicht hingegen die gemäß § 8a Abs. 2 Z 1 verarbeiteten Daten. Auch die Kontrolle durch den Rechtsschutzbeauftragten ist somit auf gewisse Teilbereiche der Informationsverbundsysteme iSd § 8a beschränkt. Schon aus diesem Grund ist dieses Instrument nicht geeignet, die hier offenbar intendierte Einschränkung der Betroffenenrechte zu rechtfertigen.

2. Die vorgeschlagene Bestimmung stellt wiederholt auf die „Verarbeitung“ der Daten durch den Bundesminister für Inneres ab. Es stellt sich die Frage, ob damit nur die Einspeisung von Daten in das Informationsverbundsystem oder auch die Abfrage von Daten gemeint ist.

So bestimmt § 8a Abs. 2 erster Satz, unter welchen Voraussetzungen der Bundesminister für Inneres als Auftraggeber in einem Informationsverbundsystem personenbezogene Daten „verarbeiten“ darf. Den Erläuterungen zufolge sollen damit die „Voraussetzungen der Speicherung von sicherheits- oder kriminalpolizeilich ermittelten personenbezogenen Daten“ geregelt werden. § 8a Abs. 2 letzter Satz sieht vor, dass § 26 DSG 2000 hinsichtlich der vom Bundesminister für Inneres als Auftraggeber „verarbeiteten“ Daten gilt. Die Materialien erklären hierzu, dieses

Auskunftsrecht bestehe hinsichtlich jenes Datenbestandes, der vom Bundesminister für Inneres „eingegeben“ wurde. Sollte mit „verarbeiten“ jedoch nur „speichern“ bzw. „eingeben“ gemeint sein, stellt sich die Frage, woraus sich die erforderlichen Regelungen für die Datenabfrage durch den Bundesminister für Inneres ergeben.

§ 8a Abs. 2 enthält divergierende Voraussetzungen für die Verarbeitung personenbezogener Daten einerseits und die Verarbeitung sensibler Daten andererseits. Sensible Daten sollen offenbar einem qualifizierten Schutz unterstehen, indem ihre Verarbeitung nicht bloß „erforderlich“, sondern „unbedingt erforderlich“ sein muss. Es sollte – allenfalls unter Darlegung von Beispielen in den Erläuterungen – näher bestimmt werden, worin der Unterschied zwischen diesen beiden Anforderungen besteht.

3. § 8a Abs. 3 sieht vor, dass die Daten ua „während der Verwendung zu aktualisieren“ sind. Die Materialien sprechen diesbezüglich von „periodisch stattfindenden Überprüfungen“. Dieser Vorgang sollte präzisiert werden – etwa durch die Angabe bestimmter Prüffristen.

4. Es sollte in den Materialien genauer dargelegt werden, wie die Anordnung des § 8a Abs. 4 zu verstehen ist, dass der Rechtsschutzbeauftragte von der beabsichtigten Teilnahme an einem internationalen Informationsverbundsystem für Zwecke der Sicherheitspolizei nach Maßgabe des § 91c Abs. 2 SPG zu verständigen ist.

5. Es wäre zu prüfen, inwieweit die in § 8a Abs. 4 enthaltenen Einsichtsrechte in Protokolldaten eine effektive Kontrolle ermöglichen: Dabei ist zu hinterfragen, inwiefern in diesem Bereich überhaupt eine lückenlose Protokollierung vorgeschrieben ist (etwa für ausländische Behörden) und wie die Authentifizierung der abfrageberechtigten Personen ausgestaltet ist. Präzisierungsbedürftig scheint ferner, was mit dem „nationalen Datenbestand“ gemeint ist und wie dieser abzugrenzen ist.

Falls die Anordnung des § 8a Abs. 4 letzter Satz nur bestimmte (Teilbereiche der) Informationsverbundsysteme betreffen soll, sollte dies im Normtext deutlicher zum Ausdruck gebracht werden.

III. Legistische und sprachliche Bemerkungen

Zu Z 2 (§ 5 Abs. 3 Z 1):

Es sollte überprüft werden, ob im Zusammenhang mit dem Zentralen Melderegister nicht auf § 16 (und nicht § 16a) Meldegesetz 1991 verwiesen werden sollte.

Zu Z 3 (§ 8a):

Die Ziffern des Abs. 2 sind der Formatvorlage „52_Ziffer_e1“, der Schlussteil der Formatvorlage „55_SchlussteilAbs“ zuzuweisen (vgl. Punkt 2.5.7.4.1 der Layout-Richtlinien).

Zu Z 4 (§ 20 Abs. 9):

Es sollte die Fassung der in Kraft tretenden Bestimmungen angegeben werden.

IV. Zu den Materialien

Zum Allgemeinen Teil der Erläuterungen:

Im Allgemeinen Teil der Erläuterungen ist anzugeben, worauf sich die Zuständigkeit des Bundes zur Erlassung der vorgeschlagenen Neuregelungen gründet (Punkt 94 der Legistischen Richtlinien 1979). Dabei genügt es nicht, die jeweilige, mehrere Kompetenztatbestände umfassende Ziffer des Art. 10 Abs. 1 B-VG anzuführen; sondern ist auch der Wortlaut des in Anspruch genommenen Kompetenztatbestandes zu nennen (Punkt 94 der Legistischen Richtlinien 1979).

Diese Stellungnahme wird im Sinne der Entschließung des Nationalrates vom 6. Juli 1961 auch dem Präsidium des Nationalrates zur Kenntnis gebracht.

2. März 2017
Für den Bundesminister
für Kunst und Kultur, Verfassung und Medien:
HESSE

Elektronisch gefertigt

Unterzeichner	serialNumber=1026761,CN=Bundeskanzleramt,C=AT
Datum/Zeit	2017-03-02T10:30:07+01:00
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: http://www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: http://www.bka.gv.at/verifizierung
Hinweis	Dieses Dokument wurde amtssigniert.