REPUBLIK ÖSTERREICH DATENSCHUTZRAT

BALLHAUSPLATZ 2, A-1014 WIEN
GZ ● BKA-817.230/0002-DSR/2017
TELEFON ● (+43 1) 53115/2527
FAX ● (+43 1) 53115/2702
E-MAIL ● DSRPOST@BKA.GV.AT
DVR: 0000019

An das
Bundesministerium für Inneres

Per Mail:
bmi-III-7@bmi.gv.at

Betrifft: Bundesgesetz, mit dem das Bundesgesetz über die internationale polizeiliche Kooperation (Polizeikooperationsgesetz – PolKG) geändert wird
Stellungnahme des Datenschutzrates

Der **Datenschutzrat** hat in seiner **233. Sitzung am 6. März 2017 einstimmig** beschlossen, zu der im Betreff genannten Thematik folgende Stellungnahme abzugeben:

1) Allgemeines

Laut den Erläuterungen zeigen nach Ansicht des Bundesministeriums für Inneres die Entwicklungen in Europa, insbesondere die terroristischen Anschläge in Frankreich, Belgien oder Deutschland die Notwendigkeit der Verbesserung des internationalen Informationsaustausches zwischen den zuständigen Behörden auf. Auch in Österreich besteht derzeit eine erhöhte Gefährdungslage durch islamistischen Terrorismus. Aufgrund der international operierenden und vernetzten Terrorgruppierungen ist es zur Gewährleistung der Sicherheit in Österreich unabdingbar, dass dieser Informationsaustausch nicht nur auf nationaler Ebene, sondern auch mit ausländischen Sicherheitsbehörden und Sicherheitsorganisationen erfolgt und weiter ausgebaut wird. Dies gilt sowohl in quantitativer als auch in qualitativer Hinsicht.
Neben der bereits bestehenden Nutzung des Schengener Informationssystems (SIS II) sowie weiterer Möglichkeiten des Informationsaustausches mit

Sicherheitsorganisationen, wie z.B. Europol und Interpol, ist die bessere Vernetzung mit Sicherheitsorganisationen und ausländischen Sicherheitsbehörden zur Intensivierung der Zusammenarbeit zur Vorbeugung und Abwehr von mit schwerer Gefahr für die öffentliche Sicherheit verbundener Kriminalität, etwa solcher, die sich aus der Gefahr durch Foreign Terrorist Fighters ergibt, notwendig. Die Notwendigkeit der besseren Vernetzung gründet sich insbesondere auch darin, dass sich in einer globalen Welt mögliche Gefährder und damit einhergehende Gefahren örtlich rasch verschieben können.

Um den Informationsaustausch und die operative Zusammenarbeit vorantreiben zu können, sind technische Zusammenschlüsse zur Stärkung des Informationsaustausches notwendig, wodurch Informationen und Erkenntnisse einer Vielzahl von Behörden zeitnah zusammengeführt und übergreifend analysiert werden können. Ein Informationsaustausch über ein Informationsverbundsystem geschieht im Vergleich zum üblichen bilateralen Informationsaustausch rascher, sodass die Sicherheitsbehörden in die Lage versetzt werden, Gefahren in den genannten Bereichen ehestens zu erkennen oder auch über solche zeitnah informieren zu können.

Für die Teilnahme österreichischer Sicherheitsbehörden an internationalen Datenverbünden soll nunmehr eine ausdrückliche nationale Rechtsgrundlage geschaffen werden, die es erlaubt, an internationalen Informationsverbund-systemen mit Sicherheitsorganisationen und ausländischen Sicherheitsbehörden teilzunehmen.

2) Datenschutzrechtlich relevante Bestimmungen

Zu Z 3 (§ 8a):

Der Datenschutzrat merkt vorweg an, dass die gesetzliche Ermächtigung zur Teilnahme an internationalen Informationsverbundsystemen in ihrer vorgeschlagenen Form zu pauschal ist, 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 Informations-verbundsystemen verwendet werden dürfen, deutlich enger und genauer festgelegt werden**. Unklar erscheint hier auch die Abgrenzung der

Datenverwendung zur allgemeinen Kriminalitätsbekämpfung und zur Bekämpfung des Terrorismus sowie zu nachrichtendienstlichen Zwecken. Determinierungsbedürftig ist zudem auch, 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.

Es sollte gesetzlich klargestellt werden, dass für Eingaben in Informationsverbundsysteme dieselben datenschutzrechtlichen Vorgaben gelten wie für Einzelübermittlungen. Eine diesbezügliche Prüfung wird von den informierten Vertretern in der Sitzung des Datenschutzrates zugesichert.

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).

Es muss daher im Normtext klargestellt werden, dass die an Informationsverbundsystemen teilnehmenden Staaten – wie von den informierten Vertretern ausgeführt – auf EU-Mitgliedstaaten, Vertragsstaaten des Europäischen Wirtschaftsraums sowie die Schweiz beschränkt sind. Der

Datenschutzrat geht diesfalls davon aus, dass die Einhaltung rechtsstaatlicher Garantien, wie sie von Österreich gemäß langjähriger Praxis in bilateralen Polizeikooperationsabkommen vereinbart werden, in rechtsverbindlicher Form gewährleistet ist.

Außerdem ist fraglich, ob der gegenständliche Entwurf einen hinreichend umfassenden und **effektiven Rechtsschutzmechanismus** gewährleistet:

Zum einen sieht § 8a Abs. 4 des Entwurfes nur eine **Verständigungspflicht** des Rechtsschutzbeauftragten vor; er kann dem Wortlaut des Entwurfes zufolge aber die Teilnahme an einem internationalen Informationsverbundsystem nicht beeinspruchen bzw. verhindern, auch wenn datenschutzrechtliche Vorgaben im Verbundsystem nicht berücksichtigt sind. Nach Ansicht des Datenschutzrates ist es aber entscheidend, zu wissen, nach welchen Kriterien diese Informationsverbundsysteme geführt werden und ob Betroffene ihre Rechte gegenüber allen Sicherheitsorganisationen und ausländischen Sicherheitsbehörden, die an diesen Informationsverbundsystemen teilnehmen, auch durchsetzen können.

Weiters 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 wesentliche Frage, wie der Betroffene seine Rechte effektiv geltend machen kann, wenn ihn betreffende Daten zwar bereits von Organisationen und Behörden anderer Teilnehmerstaaten in ein Informationsverbundsystem eingespeist wurden und u.a. auch dem Bundesministerium für Inneres zur Abfrage zur Verfügung stehen, **für den Betroffenen aber nicht feststellbar ist, wem gegenüber er seine Betroffenenrechte geltend machen kann**.

Dem Entwurf ist auch keine Regelung zu entnehmen, unter welchen Voraussetzungen und wann Daten in den angesprochenen internationalen Informationsverbundsystemen gelöscht werden können/müssen und wer dies vorzunehmen hat.

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 diese Form der Kontrolle durch den Rechtsschutzbeauftragten ist somit auf gewisse Teilbereiche der Informationsverbundsysteme iSd § 8a beschränkt.

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 sei, 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.

§ 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.**

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 und eine Genehmigung nicht vorgesehen ist.

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 gegenüber Daten aus anderen Teilnehmerstaaten 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.

Der **Datenschutzrat** erlaubt sich im Zusammenhang mit dieser Stellungnahme auf aktuelle wissenschaftliche Beiträge zu verweisen, die sich grundsätzlich mit dem österreichischen System des Rechtsschutzbeauftragten und offensichtlichen Rechtsschutzdefiziten d.h. Rechtsschutzlücken im Polizeilichen Staatsschutzgesetz auseinandersetzen (Polizeiliches Staatsschutzgesetz, Gregor Heißl, ÖJZ (2016) 16, Seiten 719 ff; Der polizeiliche Staatsschutz – Schutz oder Bedrohung der Freiheit?, Farsam Salimi, ÖJZ (2017) 03, Seiten 115 ff.). **Der Datenschutzrat ersucht, diese wissenschaftlichen Beiträge zu analysieren und gegebenenfalls bei zukünftigen Gesetzesvorhaben zu berücksichtigen und mögliche Rechtsschutzlücken zu schließen.**

Abschließend ersucht der Datenschutzrat den Gesetzesentwurf dahingehend zu überprüfen, ob nicht auch die Bestimmungen der Richtlinie (EU) 2016/680 vom 27. April 2016 über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr zur Anwendung kommen.

Der Datenschutzrat ist überdies der Auffassung, dass der Bundesminister für Inneres über diese Datenverwendung jährlich einen Bericht dem Parlament, der Datenschutzbehörde und dem Datenschutzrat vorlegen soll. Dieser Bericht soll u.a. die Anzahl und die Art der durch das BMI verarbeiteten Daten, den jeweiligen Verarbeitungsgrund, die weitere Verwendung dieser Daten durch die am Informationsverbundsystem teilnehmenden Sicherheitsorganisationen und ausländische Sicherheitsbehörden und deren Zugriffe auf die dafür vom Bundesministerium für Inneres verarbeiteten Daten sowie einen Bericht des Rechtsschutzbeauftragten über seine Kontrolltätigkeit enthalten.

8. März 2017
Für den Datenschutzrat
Der Vorsitzende:
MAIER

Elektronisch gefertigt