DIE ÖSTERREICHISCHEN RECHTSANWÄLTE

Bundesministerium für Inneres
Herrengasse 7
1010 Wien

per E-Mail: bmi-III-1@bmi.gv.at
begutachtungsverfahren@parlament.gv.at

**Zl. 13/1 17/23**

**BMI-LR1340/0004-III/1/2017**
**BG, mit dem das Bundesgesetz über die internationale polizeiliche Kooperation (Polizeikooperationsgesetz – PolKG) geändert wird**

**Referent: VP Dr. Bernhard Fink, Rechtsanwalt in Klagenfurt**

Sehr geehrte Damen und Herren!

Der Österreichische Rechtsanwaltskammertag (ÖRAK) dankt für die Übersendung des Entwurfes und erstattet dazu folgende

**S t e l l u n g n a h m e :**

**Zu den einzelnen Bestimmungen**

**A. Zu Z 2 des Entwurfes**

Ein **manuelles Einholen von Auskünften** anderer Sicherheitsbehörden und von Dienststellen der Gebietskörperschaften, der anderen Körperschaften des öffentlichen Rechts, der von diesen betriebenen Anstalten sowie – unter gewissen Voraussetzungen – auch von Betreibern öffentlicher Telekommunikationsdienste war bereits bisher gem. § 5 Abs. 3 Z 2 und 3 PolKG möglich. Die Daten aus den Fahndungsevidenzen konnten grundsätzlich schon bisher von den Sicherheitsbehörden herangezogen werden, sofern sie diese als Behörde in Vollziehung der Gesetze selbst ermittelt hatten (Z 1 leg. cit.) oder Auskunftsersuchen an andere Sicherheitsbehörden stellten (Z 2 leg. cit.). Der Abgleich der im Zentralen Melderegister verarbeiteten Daten durch den Bundesminister für Inneres (BMI) mit von Sicherheitsbehörden geführten Fahndungsevidenzen war schon bisher gestattet (§ 16a Abs. 11 MeldeG). Das gilt auch für die Abfrage durch Sicherheitsbehörden (vgl. § 16a Abs. 1, 2 und 3 MeldeG). Auch die Abfrage aus dem Fremdenregister durch Sicherheitsbehörden bzw. die Übermittlung an diese war schon bisher gesetzlich vorgesehen (§ 27 Abs 1. und § 29 Abs. 1. BFA-VG).

Dass die Abfragen **zukünftig auch automatisiert** erfolgen sollen, erscheint insbesondere wegen des Aufwandes bei der manuellen Vorgangsweise zielführend. Da die Befugnis zur manuellen Abfrage schon bisher bestand und somit die gleichen Daten wie bisher, jedoch zusätzlich automatisiert, ermittelt werden dürfen, sowie die **Übermittlungsschranken des § 8 Abs. 2 und 3 PolKG** gelten, erweist sich diese Maßnahme als sinnvoll.

**B. Zu Z 3 des Entwurfes**

Zu § 8a Abs. 1:

1. § 8a sieht eine gesetzliche Ermächtigung des Bundesministers für Inneres (BMI) vor, für Zwecke der Sicherheits- und Kriminalpolizei an Informationsverbundsystemen mit Sicherheitsorganisationen und ausländischen Sicherheitsbehörden teilzunehmen, welche als Dienstleister der Informationsverbundsysteme herangezogen werden dürfen. Dadurch solle ein rascher Informationsaustausch für kriminalpolizeiliche und insbesondere sicherheitspolizeiliche Zwecke gewährleistet werden (vgl. zur in den Erläuterungen erwähnten Counter Terrorism Group zuletzt „Terror-Suchmaschine im Aufbau“ in DiePresse, 20.02.2017, Seite 1).

2. **Sicherheitsorganisationen** im Sinne des PolKG sind **Europol** und **Interpol** (§ 2 Abs. 2 Z 1 und 2 PolKG) sowie andere Organisationen, die der BMI mit Verordnung zu Sicherheitsorganisationen erklärt hat (Z 3 leg. cit.). Aktuell betrifft dies nur die Vereinten Nationen, soweit sie im Rahmen des durch die Resolution des Sicherheitsrates Nr. 1267/1999 eingesetzten Komitees tätig werden (§ 1 Sicherheitsorganisationen-Verordnung). Da bei Verordnungserlassung gem. § 13 Z 2 PolKG insbesondere § 8 Abs. 2 und 3 PolKG zu beachten sind, welche auch den Grundrechtschutz des Art 8 EMRK und § 1 DSG 2000 gewährleisten, ergeben sich diesbezüglich keine Bedenken.

**Ausländische Sicherheitsbehörden** sind Dienststellen anderer Staaten, die Aufgaben der Sicherheitspolizei, der Kriminalpolizei, des Passwesens, der Fremdenpolizei und der Grenzkontrolle wahrnehmen (§ 2 Abs. 3 iVm § 1 Abs. 1 PolKG). Obwohl nicht ausdrücklich genannt, kommen **Geheimdienste** als Behörden, denen zur Gewährleistung der inneren Sicherheit des Staates Gefahrenerforschung obliegt (§ 2 Abs. 3 zweiter Halbsatz PolKG) grundsätzlich ebenfalls in Betracht, und zwar weltweit (vgl. hierzu auch „Terror-Suchmaschine im Aufbau“ in DiePresse, 20.02.2017, Seite 1).

3. Aus der Festlegung, dass **Sicherheitsorganisationen und ausländische Sicherheitsbehörden als Dienstleister** herangezogen werden dürfen, ist mangels gesonderter Festlegung dieses Begriffes in diesem Bundesgesetz in systematischer Hinsicht nach der Legaldefinition des § 4 Z 5 DSG 2000 zu schließen, dass diese die gesetzliche Befugnis haben, **„Daten nur zur Herstellung eines ihnen aufgetragenen Werkes“** zu verwenden. Eine **Befugnis zur Abfrage durch Sicherheitsorganisationen und ausländische Sicherheitsbehörden** lässt sich der geplanten Bestimmung insofern nicht schlüssig entnehmen, als diesen in dieser Bestimmung als Dienstleistern die Befugnis zur Verwendung von Daten **„nur zur Herstellung eines ihnen aufgetragenen Werkes“** (vgl. Z 5 leg. cit.) eingeräumt wird.

Bei einer Abfrage der Daten aus dem Informationsverbundsystem treffen diese jedoch allein die Entscheidung hierzu und wären daher gem. § 4 Z 4 DSG 2000 als Auftraggeber anzusehen.

4. Es fragt sich jedoch generell, **nach welchen Kriterien** Sicherheitsorganisationen und ausländische Sicherheitsbehörden auf die vom BMI gem. § 8a Abs. 2 in das Informationssystem eingespeisten Daten zugreifen dürfen. Insbesondere ist eine **determinierte rechtliche Regelung der Zulässigkeit der Abfrage dieser Daten,** welche ja bereits im Informationssystem gespeichert sind, nicht vorgesehen. Stattdessen normiert § 8a Abs. 2 allein die **Voraussetzungen für die Einspeisung** – was laut den Erläuterungen bereits als Übermittlung zu werten ist – die im Zuge einer **allgemeinen ex ante Prognose** – insbesondere für die Aufklärung von Straftaten“ (Z 1 leg. cit.) sowie potenzielle „Gefährder“ (Z 2 leg. cit.) – erfolgt. **Wann diese Daten abgefragt werden dürfen, ergibt sich** insbesondere aufgrund der erwähnten Festlegung von Sicherheitsorganisationen und ausländischen Sicherheitsbehörden als bloße Dienstleister **nicht**.

Die **mangelnde gesetzliche Determinierung einer Abfrage der vom BMI in das Informationsverbundsystem eingespeisten Daten durch ausländische Sicherheitsbehörden und Sicherheitsorganisation** erweist sich im Hinblick auf die damit verbundenen **Eingriffe in Grundrechte** (siehe unten) als **bedenklich**.

5. Der geplante **Ausschluss der in § 12 Abs. 5 zweiter Satz DSG 2000 vorgesehenen Verpflichtung einer schriftliche Zusage des ausländischen Dienstleisters** an den inländischen Auftraggeber bei Überlassungen von Daten ins Ausland, dass der ausländischen Dienstleister die Dienstleisterpflichten gemäß § 11 Abs. 1 DSG 2000 einhalten werde, ist **problematisch**. Die Argumentation, dass diese Norm nicht zur Anwendung komme, weil im Zusammenhang mit ausländischen Sicherheitsbehörden und Sicherheitsorganisationen die Einhaltung der Datensicherheitsmaßnahmen der österreichischen Regelungen durch jeweils nationale Gesetze und internationale Vereinbarungen gewährleistet sei, und somit keine schriftliche Vereinbarung erforderlich sei, ist nicht schlüssig. Eine schriftliche Zusage wäre bei entsprechenden unmittelbar anwendbaren nationalen Gesetzen gem. § 12 Abs. 5 letzter Satz DSG 2000 auch bei grundsätzlicher Anwendung des zweiten Satzes § 12 Abs. 5 DSG 2000 nicht erforderlich. Umgekehrt führt die geplante Regelung aber dazu, dass, sofern die Schutzplichten des § 11 Abs. 1 DSG 2000 **nicht in unmittelbar anwendbaren Rechtsvorschriften im Ausland vorgesehen** sind, das **Erfordernis einer schriftlichen Zusage des Dienstleisters über die Einhaltung des § 11 Abs. 1 DSG 2000 trotzdem nicht** besteht. Dies kann zum Beispiel bei völkerrechtlichen Verträgen sowie den erwähnten internationalen Vereinbarungen der Fall sein – wenn diese nicht unmittelbar anwendbar sind – oder **wenn solche Vereinbarungen nicht einmal bestehen**. In diesem Fall ergeben sich Bedenken hinsichtlich des **Rechtsschutzes bezüglich der Verwendung der Daten durch ausländische Sicherheitsbehörden sowie Sicherheitsorganisationen**. Es wäre darin ein Verstoß gegen das Grundrecht auf Datenschutz (§ 1 DSG 2000) zu erblicken, da die Rechte des § 11 Abs. 1 DSG durch diese Regelung in manchen Fällen nicht gewährleistet werden.

6. Auch der **Ausschluss der Anwendbarkeit des § 50 DSG 2000**, insbesondere des darin vorgesehenen Anspruches des Betroffenen, auf Antrag binnen zwölf

Wochen alle Auskünfte vom Betreiber zu erhalten, die notwendig sind, um den für die Verarbeitung seiner Daten im System verantwortlichen Auftraggeber festzustellen, **höhlt die Rechte der Betroffenen ebenfalls weiter aus**. Um einem Missbrauch vorzubeugen, wäre es jedenfalls erforderlich, diese Rechte nur bei Vorliegen eines der **in § 26 Abs. 2 DSG 2000 genannten Tatbestände** auszuschließen. Handeln die inländischen Behörden als Auftraggeber sowie die Sicherheitsorganisationen und ausländischen Sicherheitsbehörden bei der Abfrage von Daten (als Auftraggeber) rechtmäßig, so bestünde dann bei Vorliegen dieser Voraussetzungen ebenfalls kein Recht auf Auskunft gemäß § 50 DSG 2000.

Zu § 8a Abs. 2:

1. Zu **Z 1** ist festzustellen, dass die **Übermittlung für Fahndungszwecke** legitim und erforderlich ist. Die Befugnis, personenbezogene Daten im Rahmen von Interpol für die Aufklärung von strafbaren Handlungen gegen die **sexuelle Integrität und Selbstbestimmung** sowie von mit **mindestens einjähriger Freiheitsstrafe bedrohten vorsätzlichen gerichtlich strafbaren Handlungen** zu verarbeiten (übermitteln), erscheint insbesondere verhältnismäßig. Mit mindestens einjähriger Freiheitsstrafe sind in Österreich aktuell regelmäßig nur Taten mit besonderer Sozialschädlichkeit und hohem Unrechtsgehalt bedroht. Probleme bezüglich der Verhältnismäßigkeit der Verarbeitung könnten sich jedoch ergeben, wenn dies im Ausland nicht der Fall ist und Daten zur Aufklärung solcher Taten nach dem Gesetzeswortlaut trotzdem übermittelt werden dürfen. Beispielsweise sind die im Vergleich zur österreichischen Rechtslage weit strengeren Strafdrohungen für Drogendelikte in manchen asiatischen Staaten zu nennen, die bis zur Todesstrafe reichen.

2. Das **Grundrecht auf Datenschutz** lässt bei einer Verwendung von personenbezogenen Daten, die nicht im lebenswichtigen Interesse des Betroffenen oder mit seiner Zustimmung erfolgt, **Beschränkungen des Anspruchs auf Geheimhaltung nur zur Wahrung überwiegender berechtigter Interessen eines anderen** zu, und zwar bei Eingriffen einer staatlichen Behörde nur auf Grund von Gesetzen, die aus den in Art 8 Abs. 2 EMRK genannten Gründen notwendig sind. Derartige Gesetze dürfen die Verwendung von Daten, die ihrer Art nach besonders schutzwürdig sind, nur zur Wahrung wichtiger öffentlicher Interessen vorsehen und müssen gleichzeitig **angemessene Garantien für den Schutz der Geheimhaltungsinteressen** der Betroffenen festlegen. Auch im Falle zulässiger Beschränkungen darf der Eingriff in das Grundrecht jeweils **nur in der gelindesten, zum Ziel führenden Art** vorgenommen werden (§ 1 DSG 2000)

Die einschlägig anwendbaren Schranken des § 8 Abs. 2 und 3 PolKG beinhalten zwar Regelungen insbesondere hinsichtlich des **Grundrechtschutzes des Art 8 EMRK und § 1 DSG 2000**, jedoch stellt Abs. 2 leg cit in dessen letztem Satz klar, dass für im Anwendungsbereich des EU-Polizeikooperationsgesetzes (EU-PolKG) befindliche Staaten (Art 24 Abs. 1 und 38 EUV) hierfür nur bestimmte Tatsachen des Einzelfalls in Betracht kommen. Hieraus ergibt sich **kein ausreichender Rechtsschutz**. Denn das Abstellen darauf, dass die Übermittlung zur Aufklärung bestimmter Straftaten **bloß erforderlich** sein muss, lässt einen so **weiten Kreis potenziell betroffener personenbezogener Daten** offen, dass eine Einzelfallprüfung nicht ausreicht. Darauf, ob dies insbesondere **im Hinblick auf Art 8 Abs. 2 EMRK oder § 1 DSG 2000**

**gerechtfertigt und verhältnismäßig** ist, wird auch in der Befugnis **nicht Bedacht genommen**. Wenn § 8a Abs. 2 zweiter Satz die **unbedingte Erforderlichkeit** zur Erfüllung des Zweckes **nur bei der Verarbeitung sensibler Daten** – also insbesondere nicht bei Namen, Adressen, Fingerabdrücken (vgl. § 4 Z 2 DSG 2000) – voraussetzt, ergibt sich hieraus ebenfalls bei weitem kein ausreichender Rechtsschutz. Die **mangelnde Differenzierung des Kriteriums der Erforderlichkeit** erscheint aufgrund des Eingriffes in die **Schutzbereiche von Art 8 EMRK und § 1 DSG 2000** sowie im Hinblick auf das – bei Eingriffen in Grundrechten strikte – **Legalitätsprinzip** (Art 18 Abs. 1 B-VG) **verfassungsrechtlich bedenklich**.

3. Auch der betroffene Personenkreis ist zu weit gefasst. Es wäre nach der geplanten Regelung eine **internationale Datenbank von personenbezogenen Informationen bezüglich nicht aufgeklärter mit mindestens einjähriger Freiheitsstrafe bedrohter vorsätzlicher gerichtlich strafbarer Handlungen** zulässig. Das Anknüpfen allein an die Erforderlichkeit zu ihrer Aufklärung ließe für eine Übermittelung prinzipiell **Daten von allen mit einer solchen Straftat in irgendeiner Weise in Verbindung stehenden Personen** in Betracht kommen. Dies können unter anderem Opfer, Zeugen oder Personen sein, die einen sonstigen (zufälligen) Bezug zur Tat aufweisen. Da grundsätzlich sogar ganze Akten (alle Daten, die für Zwecke der Sicherheits- und Kriminalpolizei ermittelt wurden, siehe hierzu auch die Ausführungen unten) übermittelt werden dürfen, ist dieser Eingriff als **unverhältnismäßig** zu qualifizieren und sollte jedenfalls auf Daten von Beschuldigten und Verdächtigen eingeschränkt werden.

4. Im Gegensatz dazu werden in **Z 2** konkretere Anforderungen für die Zulässigkeit der Übermittlung gestellt. Die Erforderlichkeit zur Identifizierung von Personen, von denen angenommen werden kann, dass von ihnen eine mit schwerer Gefahr für die öffentliche Sicherheit verbundene Kriminalität ausgehen könnte (sog. Gefährder), erscheint im Hinblick auf das angestrebte Ziel der **Terrorismusbekämpfung** grundsätzlich legitim. Das Erfordernis einer potenziellen schweren Gefahr für die öffentliche Sicherheit sollte grundsätzlich für die angemessene Verhältnismäßigkeit sorgen, jedoch wird überhaupt nicht darauf abgestellt, **mit welcher Wahrscheinlichkeit** eine solche Kriminalität von der betroffenen Person ausgeht. Somit wäre auch bei einem **bloß geringsten und auch substanzlosen Verdacht** eine Übermittlung an das Informationsverbundsystem zulässig und sind somit wiederum auch **unverhältnismäßige Eingriffe in die Grundrechte** der Betroffenen gestattet.

5. Auch die in Z 2 gestattete Übermittlung zur Identifizierung von Personen zu deren Zuordnung zu einem Objekt oder Ereignis, das mit einer solchen Gefahr in Verbindung steht, ist als Tatbestand deutlich zu weit gefasst. Das bloße **In-Verbindung-Stehen mit einer solchen Gefahr** solle eine Übermittlung durch den BMI zulässig machen. Auch dies ist im Hinblick auf den Eingriff in **verfassungsgesetzlich gewährleistete Rechte** – insbesondere die Rechte auf Privatleben und Datenschutz – sowie auch im Hinblick auf die **mangelnde Determinierung** dieses Tatbestandes als **verfassungswidrig** zu qualifizieren.

6. Es fragt sich zudem, **welche Daten** vom BMI verarbeitet werden dürfen. Für das Schengener Informationssystem (SIS III) ist dies in § 33 EU-PolKG ausdrücklich und taxativ festgelegt. Dies gilt auch für das Europol-Informationssystem (§ 9 Abs. 1 und 2 EU-PolKG). Da eine solche Beschränkung in § 8a Abs. 2 nicht vorgesehen ist,

umfasst diese Befugnis zur Übermittlung und Verarbeitung vielmehr **alle Daten**, die für Zwecke der Sicherheits- und Kriminalpolizei ermittelt wurden. Es erscheint dies ob des großen Umfanges im Hinblick auf die gebotene **Verhältnismäßigkeit** (§ 1 Abs. 2 DSG 2000, Art 8 Abs. 2 EMRK) insbesondere für die Ziele der Z1 **nicht erforderlich und daher unverhältnismäßig**.

7. Dass explizit das **Auskunftsrecht des § 26 DSG** vorgesehen ist, ist zu begrüßen. Allerdings wird dieses aufgrund der Ausnahmetatbestände des Abs. 2 leg. cit. – insbesondere jenes der Vorbeugung, Verhinderung oder Verfolgung von Straftaten in Z 5 – den Betroffenen selten zustehen. Hier ergeben sich, wie unten noch ausgeführt wird, **Rechtsschutzlücken**, da hinsichtlich der Befugnisse in § 8a Abs. 2 Z 1 PolKG gem. Abs. 4 **keine Kontrollmöglichkeiten des Rechtsschutzbeauftragten oder durch Gerichte** vorgesehen sind.

Zu § 8a Abs. 3:

Dass die Daten vor der Verarbeitung auf ihre Erheblichkeit und Richtigkeit geprüft werden müssen, ist angesichts der Intensität des Eingriffs in die Rechte der Betroffenen und deren eingeschränkten Rechtsschutz- und Auskunftsmöglichkeiten vorauszusetzen. Erweisen sich Daten (bei periodisch stattfindenden Überprüfungen, vgl. die Erläuterungen) als unrichtig, dann sind diese zu löschen oder richtigzustellen. Im Gegensatz zu § 73 SPG (Pflicht zur Löschung erkennungsdienstlicher Daten von Amts wegen) ist ein **Zeitraum, nach dem die Daten zu löschen sind, nicht vorgegeben**. Ebenso wenig wird gefordert, dass die Daten bei **Wegfall der Voraussetzungen** gelöscht werden müssen. Somit können die einmal übermittelten personenbezogenen Daten einerseits **ohne jegliche zeitliche Begrenzung** sowie auch bei Wegfall der Voraussetzungen im Informationssystem gespeichert bleiben und andererseits alle Daten – etwa Adressen, aber auch sensible Daten – nach dem Wortlaut des § 8a Abs. 3 **auch bei Wegfall der Voraussetzungen des Abs. 2 immer noch richtiggestellt** werden. Dass den Sicherheitsorganisationen oder ausländischen Sicherheitsbehörden gem. § 8 Abs. 3 Z 2 lit. c PolKG auferlegt werden muss, die übermittelten Daten zu löschen, wenn die Daten nicht mehr zur Erfüllung der für die Übermittlung maßgeblichen behördlichen Aufgabe benötigt werden, es sei denn, dass eine ausdrückliche Ermächtigung besteht, die übermittelten Daten zu anderen Zwecken zu verwenden, vermag daran nichts zu ändern, da der BMI ja Auftraggeber der Verarbeitung (Speicherung) ist und ihn diese Bestimmung in dieser Hinsicht ebenfalls nicht bindet. Dieser massive Eingriff ist generell und besonders angesichts der verminderten Auskunftsrechte des Betroffenen **sachlich nicht gerechtfertigt und unverhältnismäßig** und daher in Bezug auf den **Gleichheitssatz** und die Grundrechte des **Art 8 EMRK und § 1 DSG 2000 verfassungsrechtlich bedenklich**.

Zu § 8a Abs. 4:

Die **Beschränkung der Kontrolle durch den Rechtschutzbeauftragten auf § 8a Abs. 2 Z 2** eröffnet eine **Rechtschutzlücke hinsichtlich der gemäß § 8a Abs. 2 Z 1 verarbeiteten Daten**, über welche bei Vorliegen der Voraussetzungen des § 26 Abs. 2 DSG 2000 der BMI keine Auskunft erteilen muss. Wenn der Betroffene kein Auskunftsbegehren stellt, unterliegen die Daten nicht der Kontrolle durch die Datenschutzbehörde gem. § 26 Abs. 5 DSG 2000 und ist auch der

Rechtschutzbeauftragte zur Kontrolle nicht zuständig. Dies ist unter anderem mit dem **rechtsstaatlichen Prinzip** im Sinne des **Rechtschutzstaates** nicht vereinbar und widerspricht der bei Eingriffen in die Grundrechte (Recht auf Privatleben und Datenschutz) erforderlichen **Verhältnismäßigkeit**. Auch ist eine **sachliche Rechtfertigung** hiefür im Hinblick auf den Gleichheitssatz nicht gegeben, weshalb diese Regelung verfassungsrechtlich äußerst bedenklich ist.

## Abschließende Bemerkungen

Aufgrund der dargestellten Probleme besonders bezüglich der Verhältnismäßigkeit sowie der mangelnden Differenzierung und Determinierung einzelner Regelungen des Entwurfes bestehen **zahlreiche Bedenken** gegen dessen Übereinstimmung mit verfassungsgesetzlich gewährleisteten Rechten. Auch die bereits in der medialen Berichterstattung (siehe z.B. den eingangs zitierten Artikel) geäußerten Bedenken, unter anderem bezüglich der teilweise fragwürdigen Quellen der verarbeiteten personenbezogenen Daten sowie der – wie erwähnt – bestehenden Unklarheit der Funktionsweise, werden geteilt. **Es wird daher zusammenfassend dringend zu einer Überarbeitung unter Einbeziehung von Grundrechtsexperten geraten.**

Wien, am 3. März 2017

DER ÖSTERREICHISCHE RECHTSANWALTSKAMMERTAG

Dr. Rupert Wolff
Präsident