Erläuterungen

Allgemeiner Teil

1. Hauptgesichtspunkte des Entwurfs

Die Entwicklungen in Europa, insbesondere die terroristischen Anschläge in Großbritannien, Deutschland, Frankreich oder Belgien zeigen 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 einem internationalen Informationsverbund mit Sicherheitsorganisationen und ausländischen Sicherheitsbehörden teilzunehmen.

2. Kompetenzgrundlage:

Die Kompetenz des Bundes zur Erlassung eines diesem Entwurf entsprechenden Bundesgesetzes gründet sich auf Art. 10 Abs. 1 Z 7 („Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit“) des Bundes-Verfassungsgesetzes – B-VG, BGBl. Nr. 1/1930.

Besonderer Teil

Zu Z 1 (Inhaltsverzeichnis):

Diese Bestimmung dient der Aktualisierung des Inhaltsverzeichnisses.

Zu Z 2 (§ 2 Abs. 2):

Diese Bestimmung dient der begrifflichen Anpassung an die Verordnung (EU) 2016/794 über die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) und zur Ersetzung und Aufhebung der Beschlüsse 2009/371/JI, 2009/934/JI, 2009/935/JI, 2009/936/JI und 2009/968/JI des Rates, ABl. Nr. L 153 vom 24.05.2016 S. 53, mit deren Inkrafttreten am 1. Mai 2017 Europol eine neue Rechtsgrundlage erhält.

Zu Z 3 (§ 5 Abs. 3 Z 1):

Mit dieser Änderung soll die Möglichkeit geschaffen werden, bei einlangenden Personenfahndungsersuchen bzw. Personeninformationen aus dem Ausland anstelle der bisher manuellen Priorierung in den genannten zentralen Evidenzen in diesen eine automatische Abfrage durchzuführen. Dies erweist sich aufgrund der großen Zahl an einlangenden Personenfahndungsersuchen aus dem Ausland (mehr als hundert pro Tag, mit Zuwachsraten von etwa 10% pro Jahr) als notwendig, da der manuelle Arbeitsvorgang mit großem Aufwand verbunden und die – sehr häufig negativen – Priorierungen wichtige Personalkapazitäten binden, die für aktive Fahndungsmaßnahmen und die Bearbeitung von Treffern dringend benötigt werden würden.

Zu Z 4 (§ 8a):

Der Abs. 1 beschreibt die Zweckbestimmung für die zulässige Teilnahme an einem internationalen Informationsverbundsystem. Dies soll nach Maßgabe der Bestimmungen dieses Hauptstückes, insbesondere §§ 8 ff PolKG, ausschließlich für die in Abs. 2 Z 1 und 2 genannten Zwecke der Sicherheits- und Kriminalpolizei zulässig sein. Dieser umfasst sowohl konkrete Aufgaben nach dem Sicherheitspolizeigesetz, insbesondere den vorbeugenden Schutz von Rechtsgütern oder die Abwehr gefährlicher Angriffe, sowie im Polizeilichen Staatsschutzgesetz verankerte Aufgaben, als auch den im Rahmen von Interpol notwendigen Informationsaustausch, insbesondere zu Fahndungszwecken. Die Teilnahme an solchen Informationsverbundsystemen ermöglicht einen raschen Informationsaustausch zwischen den teilnehmenden Auftraggebern, sodass auch in einer akuten Bedrohungslage – in der ein schnelles Handeln der Auftraggeber gefordert ist – unmittelbar, d.h. ohne zeitliche Verzögerung, eine zielgerichtete, grenzüberschreitende Zusammenarbeit gewährleistet wird.

Die Nichtanwendbarkeit der Bestimmung nach § 50 DSG 2000 erklärt sich daraus, dass ein Informationsverbundsystem im Sinne des § 4 Z 13 DSG 2000 ein Spezifikum des österreichischen Datenschutzrechtes darstellt und andere europäische Datenschutzgesetze diesen Begriff nicht kennen. Da im Zusammenhang mit ausländischen Sicherheitsbehörden und Sicherheitsorganisationen als Dienstleister die Einhaltung der Datensicherheitsmaßnahmen durch jeweils nationale Gesetze und internationale Vereinbarung gewährleistet ist, und zusätzlich die datenschutzrechtlichen Bestimmungen der §§ 8 ff PolKG gelten, müssen keine gesonderten schriftlichen Vereinbarungen zur Einhaltung der österreichischen Regelungen geschlossen werden; § 12 Abs. 5 zweiter Satz DSG 2000 kommt daher nicht zur Anwendung.

Die Verankerung der Regelung des § 8a im 3. Abschnitt des PolKG hat zur Folge, dass die dort normierten Zulässigkeitskriterien für die Übermittlung personenbezogener Daten auch für die Verarbeitung der Daten im Informationsverbundsystem gelten. In diesem Sinn regelt § 8 Abs. 2 PolKG jene Gründe, aus denen eine Verarbeitung von Daten im Informationsverbund unterbleiben muss. § 8 Abs. 3 PolKG legt fest, welche Auflagen für die Sicherheitsorganisationen und ausländischen Sicherheitsbehörden bezüglich der Verwendung von österreichischen Daten gelten, etwa das Erfordernis der Zustimmung der übermittelnden Behörde zu einem anderen als den der Verarbeitung in der Datenanwendung zugrundeliegenden Zweck. Welchen Verwendungsbeschränkungen die von der Sicherheitsbehörde abgefragten Daten aus dem Informationsverbundsystem unterliegen, wird in § 9 PolKG ebenso geregelt wie die Verpflichtung der Löschung. Erkennt die Sicherheitsbehörde, dass Daten unrichtig oder unrechtmäßig im Informationsverbundsystem verarbeitet werden, trifft diese umfassende Verständigungspflichten nach § 10 PolKG. Die Pflicht zur Protokollierung der Datenverarbeitungen im Informationsverbundsystem durch die Sicherheitsbehörde ergibt sich schließlich aus § 11 PolKG.

Abs. 2 regelt die Voraussetzungen der Verarbeitung von sicherheits- oder kriminalpolizeilich ermittelten personenbezogenen Daten einschließlich sensibler Daten durch den Bundesminister für Inneres als Auftraggeber im Informationsverbundsystem. Durch die Voraussetzung, dass nur solche Daten im internationalen Informationsverbundsystem verarbeitet werden dürfen, die zulässigerweise in inländischen sicherheitspolizeilichen Datenanwendungen verarbeitet werden dürfen, ist klargestellt, welche Arten von Daten im internationalen Informationssystem verarbeitet werden können. Denn die in Betracht kommenden inländischen sicherheitspolizeilichen Datenanwendungen, insbesondere § 57 SPG und § 12 PStSG, enthalten taxativ genannte Datenarten, die zulässigerweise darin verarbeitet werden dürfen. Der dritte Satz dient der Klarstellung und normiert durch seinen Verweis auf § 26 DSG 2000, dass das jedermann zustehende Auskunftsrecht im Hinblick auf den Datenbestand, der vom Bundesminister für Inneres als Auftraggeber verarbeitet wurde, auch für den internationalen Informationsverbund gilt.

Die Z 1 von Abs. 2 stellt für die Verarbeitung von personenbezogenen Daten auf die Erforderlichkeit für die internationale Fahndung sowie die Aufklärung einer strafbaren Handlung gegen die sexuelle Integrität und Selbstbestimmung oder von mit mindestens einjähriger Freiheitsstrafe bedrohten vorsätzlichen Handlungen im Rahmen von Interpol ab. Die Teilnahme an Informationsverbundsystemen von Interpol war bislang direkt auf die Bestimmungen der §§ 1 ff PolKG gestützt und als solche auch im DVR registriert, soweit nicht eine Ausnahme von der Meldepflicht bestand. Nunmehr soll diese Teilnahme ausdrücklich im PolKG geregelt werden. Davon umfasst ist etwa ein Informationsverbundsystem zu Personenfahndungen aufgrund einer bestehenden Anordnung zur Festnahme, zur Fahndung nach gestohlenen Administrativ- oder Reisedokumenten sowie Kraftfahrzeugen. Unter den zweiten Fall (Aufklärung von mit mindestens einjähriger Freiheitsstrafe bedrohten vorsätzlichen Handlungen) fällt etwa das Informationsverbundsystem von Interpol zur Aufklärung von Kinderpornographie.

Die Z 2 von Abs. 2 trägt dem Umstand Rechnung, dass sich die zivilen Inlands- und Sicherheitsdienste der EU-Staaten sowie Norwegen und Schweiz Ende 2001 auf Initiative einer Sonderinnenministertagung

als Reaktion auf die Anschläge vom 11. September 2001 zum Zweck der grenzüberschreitenden Terrorismusbekämpfung zu einer Counter-Terrorism-Group zusammengeschlossen haben. Da mit den bestehenden bilateralen Formen der Zusammenarbeit nicht mehr das Auslangen gefunden werden konnte, wird seit dem Jahr 2015 eine Intensivierung des Informationsaustausches in diesem Bereich betrieben, welche auch einen verstärkten Datenaustausch im Rahmen eines Datenverbundes vorsieht. Die regelmäßig stattfindenden Justiz- und Innenministertreffen wurden genutzt, um bereits frühzeitig über die angestrebte Verbesserung der Kooperation durch Schaffung eines gemeinsamen Datenverbundes zu informieren. Basierend auf den jeweiligen nationalen Rechtsgrundlagen soll der automatisierte Datenaustausch über eine gemeinsam genutzte Datenbank erfolgen. Von dem genannten Teilnehmerkreis partizipiert bereits derzeit der Großteil an diesem eingerichteten Datenverbund. Die Bundesrepublik Deutschland hat zu diesem Zweck im Juli 2016 ein Gesetz zum besseren Informationsaustausch bei der Bekämpfung des internationalen Terrorismus erlassen (vgl. BGBl. I Nr. 37 vom 29. Juli 2016). Die Nutzung des Informationsverbundes ist zulässig als Datei, in der angezeigt wird, ob und welche Daten zu einer Person, bei der ein begründete Verdacht vorliegt, dass von ihr eine mit schwerer Gefahr für die öffentliche Sicherheit verbundene Kriminalität ausgehen könnte, durch eine Sicherheitsorganisation oder ausländische Sicherheitsbehörde eingegeben wurden. Eine Nutzung kann demnach zu sicherheitspolizeilichen Zwecken, etwa zur Abwehr gefährlicher Angriffe oder zum vorbeugenden Schutz vor verfassungsgefährdenden Angriffen, die sich auch aus kriminalpolizeilichen Ermittlungen ergeben können, erfolgen. Die Informationen aus diesem internationalen Informationsverbund sollen der Auswertung von Informationen und Erkenntnissen dienen, anhand derer Zusammenhänge erkannt und wahrscheinliche Gefährdungen bewertet werden können. Dazu sollen Informationen zu natürlichen und juristischen Personen, terroristischen Organisationen und Gruppierungen, von denen eine mit schwerer Gefahr für die öffentliche Sicherheit verbundene Kriminalität ausgehen könnte, oder zu deren Gegenständen, wie etwa Fahrzeugen oder Waffen, und Ereignissen verarbeitet werden.

Der Informationsverbund erfüllt nur dann seinen Zweck, wenn die Qualität der darin enthaltenen Daten hoch gehalten wird. Eine verlässliche Qualitätssicherung ist daher unerlässlich. In diesem Sinn normiert Abs. 3, dass die vom Bundesminister für Inneres als Auftraggeber ins Informationsverbundsystem eingespeisten Daten vor und während der Verarbeitung auf ihre Erheblichkeit und Richtigkeit geprüft werden. Erweisen sich Daten bei periodisch stattfindenden Überprüfungen als unrichtig, dann sind sie entweder zu löschen oder zu aktualisieren.

Der Rechtsschutzbeauftragte beim Bundesminister für Inneres (§ 91a SPG) ist von der beabsichtigten Teilnahme an einem internationalen Informationsverbundsystem nach Abs. 2 Z 2 für Zwecke der Sicherheitspolizei nach Maßgabe des § 91c Abs. 2 SPG zu verständigen. Zur Kontrolle der im Informationsverbundsystem von den österreichischen Sicherheitsbehörden gemäß Abs. 2 Z 2 verarbeiteten Daten kommt dem Rechtsschutzbeauftragten die Möglichkeit zu, jederzeit Einsicht in den nationalen Datenbestand einschließlich des Protokolldatenbestandes zu nehmen. Aus dem Verweis auf § 91d ergibt sich, dass der Rechtsschutzbeauftragte auch jederzeit Einblick in alle erforderlichen Unterlagen und Aufzeichnungen, etwa die Protokollaufzeichnungen nach § 11 nehmen kann, und er bei Wahrnehmung von Verletzungen von Rechten Dritter durch das Verwenden personenbezogener Daten den Betroffenen zu informieren oder Beschwerde an die Datenschutzbehörde zu erheben hat. Zudem ist die Teilnahme an einem Informationsverbundsystem nach Abs. 2 Z 2 in den Bericht nach § 91d Abs. 4 SPG aufzunehmen. Durch all diese Maßnahmen wird sichergestellt, dass der Rechtsschutzbeauftragte seine Kontrolle effektiv durchführen kann. Im Übrigen richtet sich der subjektive Rechtsschutz nach den Bestimmungen des SPG bzw. nach dem DSG 2000.

Zu Z 5 (§ 20 Abs. 9):

Diese Bestimmung regelt das Inkrafttreten.