

# Regierungsvorlage

**Bundesgesetz, mit dem ein Bundesgesetz über die polizeiliche Kooperation mit den Mitgliedstaaten der Europäischen Union und dem Europäischen Polizeiamt (Europol) erlassen wird sowie das Polizeikooperationsgesetz und das Sicherheitspolizeigesetz geändert werden**

Der Nationalrat hat beschlossen:

## Inhaltsverzeichnis

Artikel 1	Bundesgesetz über die polizeiliche Kooperation mit den Mitgliedstaaten der Europäischen Union und dem Europäischen Polizeiamt (Europol) (EU-Polizeikooperationsgesetz, EU-PolKG)
Artikel 2	Änderung des Polizeikooperationsgesetzes
Artikel 3	Änderung des Sicherheitspolizeigesetzes

## Artikel 1

**Bundesgesetz über die polizeiliche Kooperation mit den Mitgliedstaaten der Europäischen Union und dem Europäischen Polizeiamt (Europol), (EU – Polizeikooperationsgesetz, EU-PolKG)**

## Inhaltsverzeichnis

### 1. Teil

#### Allgemeines

- § 1 Anwendungsbereich
- § 2 Begriffsbestimmungen
- § 3 Haftung
- § 4 Verhältnis zu anderen Rechtsakten

### 2. Teil

#### Europol

- § 5 Zusammenarbeit mit Europol
- § 6 Nationale Europol-Stelle
- § 7 Entsendung von Verbindungsbeamten zu Europol
- § 8 Ersuchen von Europol um Einleitung strafrechtlicher Ermittlungen
- § 9 Europol Informationssystem
- § 10 Arbeitsdateien zu Analysezwecken
- § 11 Verwendung von Daten aus Europol-Datenverarbeitungssystemen durch Sicherheitsbehörden
- § 12 Speicher- und Lösungsfristen
- § 13 Verwendung von Protokolldaten
- § 14 Nationale Kontrollinstanz

- § 15 Gemeinsame Kontrollinstanz
- § 16 Auskunftsrecht
- § 17 Recht auf Richtigstellung oder Löschung von Daten
- § 18 Beschwerderecht
- § 19 Kontrollbefugnisse

### **3. Teil**

#### **Grenzüberschreitende Zusammenarbeit**

- § 20 Nationale Kontaktstelle
- § 21 DNA-Analysedatei
- § 22 Verwendung der Daten der DNA-Analysedateien
- § 23 Ermittlung erkennungsdienstlicher Daten zu Zwecken der Amtshilfe
- § 24 Verwendung daktyloskopischer Daten
- § 25 Abfragen aus Zulassungsevidenzen
- § 26 Verwendung von Protokolldaten
- § 27 Einschreiten auf Hoheitsgebiet anderer Mitgliedstaaten
- § 28 Einschreiten von Organen von Sicherheitsbehörden eines Mitgliedstaates im Inland
- § 29 Befugnisse auf fremdem Hoheitsgebiet

### **4. Teil**

#### **Nutzung des Visa-Informationssystems durch Sicherheitsbehörden**

- § 30 Zugriffsberechtigung auf VIS-Daten
- § 31 Übermittlung an Drittstaaten und Sicherheitsorganisationen
- § 32 Auskunft und Richtigstellung

### **5. Teil**

#### **Schengener Informationssystem**

- § 33 Schengener Informationssystem
- § 34 Zusatzinformationen
- § 35 Ausschreibung von Personen zum Zwecke der Übergabe oder Auslieferung
- § 36 Behandlung von Ausschreibungen zum Zwecke der Übergabe oder Auslieferung gesuchter Personen
- § 37 Ausschreibung von Abgängigen
- § 38 Ausschreibung von Personen, die im Hinblick auf ihre Teilnahme an einem Gerichtsverfahren gesucht werden
- § 39 Ausschreibung von Personen und Sachen zum Zwecke der verdeckten Kontrolle
- § 40 Ausschreibung von Sachen zur Sicherstellung oder Beweissicherung
- § 41 Speicherfristen
- § 42 Richtigstellung und Ergänzung von Ausschreibungen
- § 43 Auskunftsrecht

### **6. Teil**

#### **Schlussbestimmungen**

- § 44 Verweisungen
- § 45 Sprachliche Gleichbehandlung
- § 46 Inkrafttreten

## **1. Teil**

### **Allgemeines**

#### **Anwendungsbereich**

§ 1. (1) Dieses Bundesgesetz regelt die polizeiliche Kooperation zwischen den Sicherheitsbehörden und Sicherheitsbehörden der anderen Mitgliedstaaten der Europäischen Union sowie dem Europäischen Polizeiamt (Europol).

(2) Soweit dieses Bundesgesetz nicht ausdrücklich anderes bestimmt, gelten das Bundesgesetz über die internationale polizeiliche Kooperation (Polizeikooperationsgesetz - PolKG), BGBl. I Nr. 104/1997, das Sicherheitspolizeigesetz (SPG), BGBl. Nr. 566/1991, das Informationssicherheitsgesetz (InfoSiG), BGBl. I Nr. 23/2002, das Amtshaftungsgesetz, BGBl. Nr. 20/1949, und das Datenschutzgesetz 2000 (DSG 2000), BGBl. I Nr. 165/1999. Die justizielle Zusammenarbeit nach dem Bundesgesetz über die

justizielle Zusammenarbeit in Strafsachen mit den Mitgliedstaaten der Europäischen Union (EU-JZG), BGBl. I Nr. 36/2004, nach dem Auslieferungs- und Rechtshilfegesetz (ARHG), BGBl. Nr. 529/1979 oder nach zwischenstaatlichen Vereinbarungen bleibt unberührt.

### **Begriffsbestimmungen**

§ 2. Im Sinne dieses Bundesgesetzes bedeutet

1. Mitgliedstaat: jeder Staat, der Vertragspartei des Vertrages über die Europäische Union in der Fassung BGBl. III Nr. 85/1999, geändert durch BGBl. III Nr. 4/2003, und BGBl. III Nr. 54/2004 (EUV), ist; soweit seitens der Europäischen Union nach dem Titel VI des Vertrages über die Europäische Union Übereinkünfte mit Drittstaaten oder mit internationalen Organisationen abgeschlossen werden, sind diese im Rahmen der jeweiligen Übereinkünfte den Mitgliedstaaten gleichzuhalten (Art. 24 und 38 EUV);
2. Drittstaat: ein Staat, der nicht unter Z 1 fällt.

### **Haftung**

§ 3. (1) Soweit durch unrichtige oder unrechtmäßige Verwendung von Daten durch Europol in Österreich ein Schaden entstanden ist, haftet der Bund nach den Bestimmungen des Amtshaftungsgesetzes mit der Maßgabe, dass in jedem Fall das Landesgericht für Zivilrechtssachen Wien in erster Instanz zuständig ist. Wurde der Schaden durch Europol oder Organe eines anderen Mitgliedstaates verursacht, hat der Bund seinerseits Regress bei Europol oder dem anderen Mitgliedstaat zu nehmen.

(2) Der Bund hat einem Mitgliedstaat auf dessen Verlangen jenen Betrag zu erstatten, den der Mitgliedstaat an die Geschädigten zu leisten hatte, wenn österreichische Organe des öffentlichen Sicherheitsdienstes bei einem Einsatz in diesem Mitgliedstaat einen Schaden verursacht haben. Verursachen Organe von Sicherheitsbehörden anderer Mitgliedsstaaten in Österreich einen Schaden und hat der Bund Schadenersatz nach dem Amtshaftungsgesetz zu leisten, ist dieser Betrag von jenem Mitgliedstaat einzufordern, dessen Organe den Schaden verursacht haben; dies gilt nicht für vom Bund ersetzte Schäden, die das Organ bei seinem Einsatz bei Massenveranstaltungen, Katastrophen und schweren Unglücksfällen verursacht hat.

(3) Soweit durch unrichtige oder unrechtmäßige Verwendung von Daten im Schengener Informationssystem durch seine Organe ein Schaden entstanden ist, haftet der Bund nach den Bestimmungen des Amtshaftungsgesetzes. Gleiches gilt für Schäden, die durch einen dem Bund zuzurechnenden Zugriff auf das Schengener Informationssystem verursacht worden sind. Soweit dem Bund aus dem Zugriff eines am Schengener Informationssystem teilnehmenden Staates auf das Schengener Informationssystem ein Schaden entstanden ist, hat der Bund bei diesem Mitgliedstaat Regress zu nehmen.

### **Verhältnis zu anderen Rechtsakten**

§ 4. (1) Die Bestimmungen des 3. Teiles finden gegenüber den einzelnen Vertragsparteien des Prümer Vertrages, BGBl. III Nr. 159/2006, erst Anwendung, wenn diese ihren jeweiligen unionsrechtlichen Verpflichtungen aus dem Beschluss 2008/615/JI zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität, Amtsblatt Nr. L 210 vom 6.8.2008, S. 1 -11 (Prüm-Beschluss), nachgekommen sind. Ab diesen jeweiligen Zeitpunkten sind die Bestimmungen des Prümer Vertrages hinsichtlich des Vergleiches von DNA-Profilen, der Gewinnung molekulargenetischen Materiales und der Übermittlung von DNA-Profilen, des Abrufes von daktyloskopischen Daten sowie des Abrufes von Daten aus Fahrzeugregistern nicht weiter anzuwenden. Der Bundesminister für Inneres hat diese Zeitpunkte im Bundesgesetzblatt kundzumachen.

(2) Der 2. Teil dieses Bundesgesetzes (Europol) ersetzt mit Inkrafttreten dieses Bundesgesetzes das Übereinkommen auf Grund von Artikel K.3 des Vertrages über die Europäische Union über die Errichtung eines Europäischen Polizeiamts (Europol-Übereinkommen), BGBl. III Nr. 123/1998, samt den Änderungsprotokollen BGBl. III Nr. 193/1998, BGBl. III Nr. 81/1999, BGBl. III Nr. 120/2007, BGBl. III Nr. 121/2007 und BGBl. III Nr. 122/2007. Weiters ist das Protokoll auf Grund von Artikel K.3 des Vertrages über die Europäische Union und von Artikel 41 Absatz 3 des Europol-Übereinkommens über die Vorrechte und Immunitäten für Europol, die Mitglieder der Organe, die stellvertretenden Direktoren und die Bediensteten von Europol, BGBl. III Nr. 131/1999, zuletzt geändert durch BGBl. III Nr. 120/2007, nicht mehr anzuwenden. Stattdessen findet das Protokoll über die Vorrechte und Befreiungen der Europäischen Gemeinschaften, BGBl. III Nr. 24/2000, Anwendung.

(3) Der 5. Teil dieses Bundesgesetzes (Schengener Informationssystem) tritt ab dem Zeitpunkt in Kraft, der vom Rat mit Zustimmung aller Mitglieder, die die Regierungen der am SIS 1+ teilnehmenden

Staaten vertreten, festgelegt wird. Mit diesem Zeitpunkt sind anstelle der Art. 64 und 92 bis 119 mit Ausnahme der Art. 92a und 102a des Schengener Übereinkommens die Bestimmungen dieses Bundesgesetzes anzuwenden. Der Bundesminister für Inneres hat diesen Zeitpunkt im Bundesgesetzblatt kundzumachen.

## **2. Teil**

### **Europol**

#### **Zusammenarbeit mit Europol**

**§ 5.** (1) Die polizeiliche Kooperation mit Europol umfasst die Vorbeugung und Bekämpfung von Straftaten im Bereich organisierter Kriminalität, Terrorismus sowie anderer Formen schwerer Kriminalität gemäß **Anhang 1**, wenn zwei oder mehr Mitgliedstaaten betroffen sind.

(2) Die polizeiliche Kooperation mit Europol erstreckt sich auch auf Straftaten, die mit den in Abs. 1 genannten in Zusammenhang stehen und begangen werden,

1. um die Mittel zur Begehung von in den Zuständigkeitsbereich von Europol fallenden Handlungen zu beschaffen,
2. um Handlungen zu erleichtern oder durchzuführen, die in den Zuständigkeitsbereich von Europol fallen oder
3. um sicherzustellen, dass in den Zuständigkeitsbereich von Europol fallende Handlungen straflos bleiben.

#### **Nationale Europol-Stelle**

**§ 6.** (1) Der Nationalen Europol-Stelle obliegt der alleinige Zugriff auf die Europol Informationssysteme und der Kontakt zu Europol.

(2) Der Nationalen Europol-Stelle kommen insbesondere folgende Aufgaben zu:

1. Europol aus eigener Initiative Informationen und Erkenntnisse, die Europol für die Durchführung seiner Aufgaben benötigt, zu übermitteln;
2. Informations-, Erkenntnis- und Beratungsanfragen von Europol zu beantworten;
3. Informationen und Erkenntnisse auf dem aktuellen Stand zu halten;
4. Informationen und Erkenntnisse für die Sicherheitsbehörden auszuwerten und an diese weiterzuleiten;
5. Informations-, Erkenntnis-, Beratungs- und Analyseanfragen an Europol zu richten;
6. Informationen für die Speicherung in seinen Datenbanken an Europol zu übermitteln;
7. die Rechtmäßigkeit des Informationsaustauschs mit Europol zu gewährleisten.

(3) Soweit andere Sicherheitsbehörden als die Nationale Europol-Stelle Abfragen aus dem Europol-Informationssystem durchführen, darf aus dem Abfrageergebnis nur ersichtlich sein, ob ein angefragter Datensatz im Europol-Informationssystem verfügbar ist oder nicht. Weitere Informationen sind ausschließlich über die Nationale Europol-Stelle einzuholen.

(4) Die Nationale Europol-Stelle kann die Zustimmung zur Weitergabe von Daten durch Europol an Einrichtungen der Europäischen Union, Drittstaaten und Sicherheitsorganisationen (§ 2 Abs. 2 Z 2 und 3 PolKG) unter Auflagen (§ 8 Abs. 1 PolKG) erteilen. Die Zustimmung kann allgemein oder eingeschränkt erteilt und jederzeit widerrufen werden. Bei Vorliegen der in § 8 Abs. 2 PolKG angeführten Gründe ist die Zustimmung zu verweigern.

#### **Entsendung von Verbindungsbeamten zu Europol**

**§ 7.** (1) Die Nationale Europol-Stelle hat die erforderliche Anzahl von Verbindungsbeamten zu Europol zu entsenden. Die Verbindungsbeamten gehören der Nationalen Europol-Stelle an.

(2) Den zu Europol entsandten Verbindungsbeamten obliegt insbesondere:

1. die Wahrnehmung der Interessen Österreichs gegenüber Europol im Rahmen ihrer Aufgabenstellung;
2. die Übermittlung von Informationen der Nationalen Europol-Stelle an Europol;
3. die Weiterleitung von Informationen von Europol an die Nationale Europol-Stelle;
4. die Zusammenarbeit mit Bediensteten von Europol bei der Erfüllung der Europol zukommenden Aufgaben;
5. die Unterstützung beim Austausch von Informationen der Nationalen Europol-Stelle mit den Verbindungsbeamten anderer Mitgliedstaaten.

### **Ersuchen von Europol um Einleitung strafrechtlicher Ermittlungen**

§ 8. (1) Die Nationale Europol-Stelle hat Ersuchen von Europol um Einleitung, Durchführung oder Koordinierung von Ermittlungen entgegenzunehmen, zu prüfen, erforderlichenfalls an die zuständigen Stellen weiterzuleiten und Europol darüber zu informieren, ob die Ermittlungen, die Gegenstand des Ersuchens sind, eingeleitet werden. Soweit Ersuchen von Europol bei nachgeordneten Sicherheitsbehörden einlangen, haben diese die Anfrage unverzüglich der Nationalen Europol-Stelle vorzulegen.

(2) Soweit die Nationale Europol-Stelle dem Ersuchen nicht entsprechen kann, hat sie Europol darüber unter Darlegung der Gründe zu informieren. Eine Begründung kann entfallen, wenn wesentliche nationale Sicherheitsinteressen oder der Erfolg laufender Ermittlungen oder die Sicherheit von Personen dadurch gefährdet würden.

### **Europol-Informationssystem**

§ 9. (1) Die Nationale Europol-Stelle sowie die Verbindungsbeamten sind ermächtigt, zu Personen, die wegen einer Straftat oder der Beteiligung an einer Straftat, für die Europol zuständig ist, verurteilt worden sind oder einer solchen Straftat verdächtigt werden oder wenn auf Grund bestimmter Tatsachen anzunehmen ist, dass sie derartige Straftaten begehen werden, folgende Daten im Europol-Informationssystem zu verarbeiten, soweit dies im Einzelfall und zur Erfüllung der ihnen obliegenden Aufgaben erforderlich ist:

1. Name, Geburtsname, Vornamen, gegebenenfalls Aliasnamen;
2. Geburtsdatum und Geburtsort;
3. Staatsangehörigkeit;
4. Geschlecht;
5. Wohnort, Beruf und Aufenthaltsort der betreffenden Person;
6. Fahrerlaubnisse, Ausweispapiere und Passdaten;
7. soweit erforderlich andere zur Identitätsfeststellung geeignete Merkmale, insbesondere objektive und unveränderliche körperliche Merkmale wie daktyloskopische Daten und dem nicht codierenden Teil der DNA entnommene DNA-Profile.

(2) Unter den in Abs. 1 genannten Voraussetzungen dürfen von der Nationalen Europol-Stelle sowie von den Verbindungsbeamten weiters folgende Daten im Europol Informationssystem verarbeitet werden:

1. Verurteilungen, soweit sie Straftaten betreffen, für die Europol zuständig ist;
2. Verdacht auf gerichtlich strafbare Handlungen sowie vermutete oder festgestellte Tatzeiten, Tatorte und Vorgehensweisen;
3. Tatmittel, die verwendet wurden oder verwendet werden könnten;
4. Verdacht der Zugehörigkeit zu einer kriminellen Organisation;
5. Informationen zu juristischen Personen;
6. die aktenführenden Dienststellen und deren Aktenzeichen;
7. Eingabestelle.

Diese Daten dürfen auch verarbeitet werden, wenn noch kein Personenbezug besteht.

(3) Die Nationale Europol-Stelle sowie die Verbindungsbeamten haben Änderungen, Richtigstellungen und Löschungen von Daten ausschließlich hinsichtlich jener Daten durchzuführen, die von ihnen eingegeben worden sind.

(4) Liegen Anhaltspunkte vor, wonach eingegebene Daten unrichtig, unvollständig oder unrechtmäßig verarbeitet worden sind oder sein könnten, haben die Nationale Europol-Stelle sowie die Verbindungsbeamten unverzüglich jene Stelle darüber zu informieren, die die Daten eingegeben hat.

(5) Sind im Europol-Informationssystem bereits Daten gemäß Abs. 2 zu einer Person gespeichert, so ist die Eingabe weiterer Daten nach Abs. 2 zulässig; stehen die einzugebenden Daten allerdings in Widerspruch zu den bereits eingegebenen Daten, hat sich die Nationale Europol-Stelle mit jener Stelle, die solche Daten bereits eingegeben hat, abzustimmen.

(6) Beabsichtigt die Nationale Europol-Stelle eines Mitgliedstaates die von ihr eingegebenen personenbezogenen Daten gemäß Abs. 1 insgesamt zu löschen und hat die österreichische Nationale Europol-Stelle zu dieser Person Daten gemäß Abs. 2 eingegeben, so geht die datenschutzrechtliche Verantwortung und das Recht zur Änderung, Ergänzung, Richtigstellung und Löschung hinsichtlich Daten gemäß Abs. 1 auf die österreichische Nationale Europol-Stelle über, wenn sie als nächste Daten nach Abs. 2 zu dieser Person eingegeben hat.

### **Arbeitsdateien zu Analyse Zwecken**

§ 10. (1) Die Nationale Europol-Stelle sowie die Verbindungsbeamten sind ermächtigt, Europol zur Erstellung von Arbeitsdateien für Analyse Zwecke über in seine Zuständigkeit fallende Straftaten Informationen zu übermitteln, soweit die Sicherheitsbehörden diese Informationen auch nach § 53a Abs. 2 SPG zur Erstellung von Analysen verarbeiten dürfen.

(2) Die Übermittlung und Verarbeitung sensibler Daten (§ 4 Z 2 DSG 2000) ist nur zulässig, wenn diese Daten für die Analysetätigkeit unerlässlich sind und diese Daten andere, in derselben Datei bereits enthaltene personenbezogene Daten ergänzen.

(3) Die Nationale Europol-Stelle ist ermächtigt, Auflagen nach § 8 Abs. 3 PolKG festzulegen, die bei der weiteren Verarbeitung der übermittelten Daten zu beachten sind. So kann insbesondere festgelegt werden, ob die übermittelten Daten allen oder nur bestimmten Mitgliedstaaten zur Verfügung stehen sollen oder die Daten nur für explizit festgelegte Zwecke verwendet werden dürfen.

### **Verwendung von Daten aus Europol-Datenverarbeitungssystemen durch Sicherheitsbehörden**

§ 11. (1) Die Sicherheitsbehörden sind ermächtigt, Daten aus von Europol betriebenen Datenverarbeitungssystemen für Zwecke der Vorbeugung und Bekämpfung von Straftaten im Bereich organisierter Kriminalität, Terrorismus sowie anderen Formen schwerer Kriminalität sowie damit im Zusammenhang stehender Straftaten zu verwenden.

(2) Ist die Verwendung der Daten an bestimmte Auflagen gebunden, darf von diesen Auflagen ohne Zustimmung der übermittelnden Stellen nicht abgegangen werden.

(3) Die Verwendung von Daten für andere Zwecke, als zu denen sie übermittelt wurden, ist nur mit Zustimmung der übermittelnden Stelle zulässig. Ausgenommen davon ist die Verwendung zur Überprüfung der Rechtmäßigkeit der Verwendung dieser Daten.

### **Speicher- und Lösungsfristen**

§ 12. (1) Die Nationale Europol-Stelle hat längstens alle drei Jahre die von ihr in das Europol Informationssystem eingegebenen Daten daraufhin zu prüfen, ob eine über diese drei Jahre hinaus gehende Speicherung für die Erfüllung der Europol obliegenden Aufgaben notwendig ist. Ergibt die Prüfung, dass die Daten zur Erfüllung der Europol obliegenden Aufgaben nicht mehr erforderlich sind, sind sie von der Nationalen Europol-Stelle unverzüglich zu löschen.

(2) Löscht eine Sicherheitsbehörde Daten, die an Europol übermittelt worden sind, ist Europol davon durch die Nationale Europol-Stelle zu informieren.

(3) Die Löschung der Daten nach Abs. 1 hat zu unterbleiben, wenn dadurch schutzwürdige Interessen einer erfassten Person beeinträchtigt würden und diese die Einwilligung zur Weiterverwendung ihrer Daten erteilt.

### **Verwendung von Protokoll Daten**

§ 13. Von Europol zur Überprüfung der Rechtmäßigkeit der Datenabfrage aus seinen automatisierten Dateien erstellte Protokollaufzeichnungen dürfen von der nationalen Kontrollinstanz, der gemeinsamen Kontrollinstanz sowie von Europol ausschließlich für diese Zwecke verwendet werden. Sie sind nach achtzehn Monaten zu löschen, es sei denn, die Daten werden für eine laufende Kontrolle weiterhin benötigt.

### **Nationale Kontrollinstanz**

§ 14. Nationale Kontrollinstanz ist die Datenschutzkommission. Ihr obliegt die Kontrolle der Zulässigkeit der Eingabe in Informationsverarbeitungssysteme nach Kapitel II des Europol-Beschlusses und des Abrufs personenbezogener Daten aus solchen Systemen sowie die Kontrolle jedweder Übermittlung personenbezogener Daten an Europol durch österreichische Behörden und deren Organe. Unbeschadet der Befugnisse nach den §§ 30 und 31 DSG 2000 haben die Nationale Europol-Stelle und die Verbindungsbeamten der Nationalen Kontrollinstanz Zugang zu ihren Diensträumen und ihren Akten zu gewähren. Über entsprechende Aufforderung sind Akten der Nationalen Kontrollinstanz zu übermitteln.

### **Gemeinsame Kontrollinstanz**

§ 15. (1) In die gemeinsame Kontrollinstanz nach Art. 34 des Beschlusses zur Einrichtung des Europäischen Polizeiamtes (Europol), Amtsblatt Nr. L121/2009, S. 37 bis 66, sind von der Nationalen Kontrollinstanz höchstens zwei Mitglieder und jeweils ein Stellvertreter der Nationalen Kontrollinstanz zu entsenden. Diese werden für fünf Jahre ernannt und sind bei der Wahrnehmung ihrer Aufgaben an keine Weisungen gebunden.

(2) Die Nationale Europol-Stelle und die Nationale Kontrollinstanz haben die gemeinsame Kontrollinstanz auf deren Verlangen bei der Erfüllung ihrer Aufgaben zu unterstützen.

#### **Auskunftsrecht**

§ 16. (1) Jedermann kann sich an die Nationale Europol-Stelle wenden, um Auskunft zu erhalten, ob Europol ihn betreffende personenbezogene Daten verarbeitet. Die Nationale Europol-Stelle hat dieses Auskunftsbegehren unverzüglich, spätestens jedoch binnen eines Monats ab Einlangen des Auskunftsbegehrens an Europol weiter zu leiten.

(2) Die Nationale Europol-Stelle hat sich gegen die Beantwortung des Auskunftsbegehrens durch Europol auszusprechen, wenn

1. hierdurch außenpolitische, wirtschaftliche oder finanzielle Interessen der Republik Österreich verletzt werden könnten,
2. die ordnungsgemäße Erfüllung der Aufgaben von Europol beeinträchtigt werden könnte,
3. dies zu Aufrechterhaltung der öffentlichen Sicherheit oder zur Aufklärung und Verfolgung von Straftaten notwendig ist,
4. dadurch Ermittlungen beeinträchtigt werden könnten oder
5. überwiegende schutzwürdige Interessen des Betroffenen oder Dritter verletzt werden.

#### **Recht auf Richtigstellung oder Löschung von Daten**

§ 17. (1) Unrichtige oder unrechtmäßig verarbeitete Daten, die von der Nationalen Europol-Stelle oder den Verbindungsbeamten im Europol-Informationssystem verarbeitet werden oder Europol übermittelt worden sind, sind von diesen zu berichtigen oder zu löschen. Europol ist darüber zu informieren.

(2) Wurden unrichtige oder unrechtmäßig verarbeitete Daten anderen Mitgliedstaaten oder Drittstaaten übermittelt, sind diese davon unverzüglich in Kenntnis zu setzen und es ist ihnen aufzutragen, die Daten zu berichtigen oder zu löschen.

#### **Beschwerderecht**

§ 18. Wird eine Beschwerde wegen der Erteilung oder Nichterteilung der Auskunft oder der Verletzung des Rechts zur Richtigstellung und Löschung von Daten bei der Nationalen Europol-Stelle eingebracht, ist die Beschwerde an die gemeinsame Kontrollinstanz weiterzuleiten.

#### **Kontrollbefugnisse**

§ 19. (1) Jedermann kann die gemeinsame Kontrollinstanz in angemessenen Abständen um Überprüfung der Rechtmäßigkeit der Verwendung ihrer personenbezogenen Daten durch Europol ersuchen.

(2) Jedermann hat das Recht, die nationale Kontrollinstanz zu ersuchen, die Rechtmäßigkeit der Eingabe und der Übermittlung von ihm betreffenden Daten an Europol sowie des Abrufs dieser Daten durch die Nationale Europol-Stelle und die Verbindungsbeamten zu überprüfen.

### **3. Teil**

#### **Grenzüberschreitende Zusammenarbeit**

##### **Nationale Kontaktstelle**

§ 20. (1) Im Sinne dieses Teiles bezeichnet „Nationale Kontaktstelle“ jene von den einzelnen Mitgliedstaaten benannten Stellen, die zum automatisierten Vergleich von DNA-Profilen, zum automatisierten Abruf von daktyloskopischen Daten und zum automatisierten Abruf von Daten aus nationalen Fahrzeugregistern berechtigt sind.

(2) Nationale Kontaktstelle für Österreich ist der Bundesminister für Inneres.

##### **DNA-Analysedatei**

§ 21. (1) Jener Teil der von den Sicherheitsbehörden gemäß § 75 SPG verarbeiteten Daten, die die DNA-Profile bestimmter Menschen (Personenprofile) und die DNA-Profile Unbekannter (offene Spuren) enthalten, stellt die DNA-Analysedatei dar.

(2) DNA-Profile gemäß Abs. 1 dürfen nur in Form eines Buchstaben- oder Zahlencodes, der eine Reihe von Identifikationsmerkmalen des nicht codierten Teiles einer analysierten menschlichen Molekularstruktur an den verschiedenen DNA-Loci abbildet, gespeichert werden, wobei im nicht codierten Teil der DNA keine genetischen Informationen über funktionale Eigenschaften eines

Organismus enthalten sein dürfen. DNA-Profile dürfen keine Daten enthalten, auf Grund derer eine Person unmittelbar identifiziert werden kann.

- (3) Die DNA-Profile sind mit Kennungen zu versehen, die als Fundstellendatensätze
1. den Datensatz als den eines bekannten Menschen oder einer offenen Spur erkennen lassen,
  2. eine Zuordnung zu den Identitätsdaten eines bestimmten Menschen ermöglichen und
  3. ihn als ein von inländischen Behörden ermitteltes Datum ausweist.

#### **Verwendung der Daten der DNA-Analysedateien**

§ 22. (1) Der Bundesminister für Inneres hat den Nationalen Kontaktstellen der anderen Mitgliedstaaten zur Aufklärung und Verfolgung gerichtlich strafbarer Handlungen, die die Voraussetzungen für die Erlassung eines Europäischen Haftbefehles erfüllen, den Zugriff auf die DNA-Analysedatei im Datenfernverkehr in der Weise zu eröffnen, dass sie automatisiert alle in der DNA-Analysedatei (§ 21 Abs. 1) verarbeiteten DNA-Profile mit jeweils ihren national gespeicherten offenen Spuren vergleichen können. Ebenso ist ihnen die Möglichkeit einzuräumen, Personenprofile im Rahmen einer konkreten Ermittlung im Datenfernverkehr mit diesen DNA-Profilen zu vergleichen.

(2) Der Bundesminister für Inneres ist ermächtigt, zur Aufklärung und Verfolgung von gerichtlich strafbaren Handlungen die in der DNA-Analysedatei verarbeiteten DNA-Profile im Wege des Datenfernverkehrs automatisiert mit allen in den Analysedateien der anderen Mitgliedstaaten verarbeiteten DNA-Profilen zu vergleichen. Personenprofile dürfen nur dann mit von Sicherheitsbehörden anderer Mitgliedstaaten verarbeiteten DNA-Profilen im Datenfernverkehr verglichen werden, wenn dies im konkreten Einzelfall erforderlich ist.

(3) Stellen Sicherheitsbehörden anderer Mitgliedstaaten im Zuge eines automatisierten Vergleiches eine Übereinstimmung mit DNA-Profilen fest, so hat die Nationale Kontaktstelle der Nationalen Kontaktstelle des abrufenden Mitgliedstaats die DNA-Profile, mit denen Übereinstimmung festgestellt worden ist, und darüber hinaus nur eine zugehörige Kennung, die eine Zuordnung zu den Identitätsdaten eines bestimmten Menschen ermöglicht, auf automatisierte Weise zu übermitteln. Kann keine Übereinstimmung festgestellt werden, so ist die Nationale Kontaktstelle darüber ebenso auf automatisierte Weise zu informieren.

(4) Im Falle der Übereinstimmung gemäß Abs. 2 dürfen die entsprechenden Daten samt notwendiger Zusatzinformation von den Sicherheitsbehörden weiterverarbeitet werden.

(5) Wird eine Übereinstimmung von DNA-Profilen festgestellt, richtet sich die Übermittlung von über DNA-Profilen und der zugehörigen Kennung hinausgehenden Daten nach den bestehenden Amts- und Rechtshilferegelungen.

#### **Ermittlung erkennungsdienstlicher Daten zu Zwecken der Amtshilfe**

§ 23. (1) Die Sicherheitsbehörden sind ermächtigt, erkennungsdienstliche Maßnahmen an Menschen vorzunehmen, wenn dies erforderlich ist, um einer Sicherheitsbehörde eines anderen Mitgliedstaates Amtshilfe zu leisten, und diese Maßnahme auch in vergleichbaren innerstaatlichen Fällen zulässig wäre.

(2) Eine erkennungsdienstliche Maßnahme gemäß Abs. 1 darf nur vorgenommen werden, wenn ein entsprechend begründetes Ersuchen vorliegt, aus dem von der jeweils zuständigen Stelle die Erklärung hervorgeht, dass die Voraussetzungen für diese Maßnahme nach dem jeweiligen Recht zulässig wäre und die Maßnahme für ein laufendes Ermittlungs- oder Strafverfahren im jeweiligen Mitgliedstaat erforderlich ist.

- (3) Von Maßnahmen nach Abs. 1 Betroffene sind zur Mitwirkung verpflichtet. § 77 SPG gilt.

#### **Verwendung daktyloskopischer Daten**

§ 24. (1) Der Bundesminister für Inneres hat den Nationalen Kontaktstellen der anderen Mitgliedstaaten zur Abwehr gefährlicher Angriffe und zur Aufklärung und Verfolgung gerichtlich strafbarer Handlungen den Zugriff auf die gemäß § 75 SPG verarbeiteten daktyloskopische Daten im Datenfernverkehr in der Weise zu eröffnen, dass sie automatisiert Personenprofile im Rahmen einer konkreten Ermittlung im Datenfernverkehr mit diesen daktyloskopischen Daten vergleichen können.

(2) Der Bundesminister für Inneres ist ermächtigt, zur Abwehr gefährlicher Angriffe und zur Aufklärung und Verfolgung gerichtlich strafbarer Handlungen die von Sicherheitsbehörden ermittelten daktyloskopischen Daten mit jenen abzugleichen, die von den Sicherheitsbehörden anderer Mitgliedstaaten zu diesem Zweck verarbeitet werden. Kommt es bei einem solchen Abgleich zu einer Übereinstimmung, dürfen diese Daten und dazu gehörige Informationen von den Sicherheitsbehörden weiterverarbeitet werden.



(3) Stellen Sicherheitsbehörden anderer Mitgliedstaaten eine Übereinstimmung mit daktyloskopischen Daten fest, so sind der Nationalen Kontaktstelle des abrufenden Mitgliedstaats die daktyloskopischen Daten, mit denen Übereinstimmung festgestellt worden ist, und darüber hinaus nur eine zugehörigen Kennung, die eine Zuordnung zu den Identitätsdaten eines bestimmten Menschen ermöglichen, auf automatisierte Weise zu übermitteln. Kann keine Übereinstimmung festgestellt werden, so ist die Nationale Kontaktstelle darüber ebenso auf automatisierte Weise zu informieren.

(4) Wird eine Übereinstimmung von daktyloskopischen Daten festgestellt, richtet sich die Übermittlung von über daktyloskopischen Daten und der zugehörigen Kennung hinausgehenden Daten nach den bestehenden Amts- und Rechtshilferegelungen.

#### **Abfragen aus Zulassungsevidenzen**

§ 25. (1) Der Bundesminister für Inneres hat den Nationalen Kontaktstellen der anderen Mitgliedstaaten zur Abwehr allgemeiner Gefahren und zur Aufklärung und Verfolgung von Straftaten, die nach dem Recht des Staates der ersuchenden Kontaktstelle in die Zuständigkeit der Gerichte oder Staatsanwaltschaft fallen, sowie zur Abwehr von Gefahren für die öffentliche Sicherheit Abfragen aus der Zulassungsevidenz gemäß § 47 Abs. 4 KFG im Datenfernverkehr zu ermöglichen.

(2) Abfragen gemäß Abs. 1 sind nur zulässig, wenn entweder eine vollständige Fahrgestellnummer oder ein vollständiges Kennzeichen als Abfragekriterium verwendet wird. Die auf Grund einer solchen Abfrage erteilte Auskunft hat sich auf den Zulassungsbesitzer und die Angaben zum Kraftfahrzeug zu beschränken.

(3) Die Sicherheitsbehörden sind zur Abwehr allgemeiner Gefahren und zur Aufklärung und Verfolgung von gerichtlich strafbaren Handlungen ermächtigt, im Wege des Bundesministers für Inneres Abfragen aus Fahrzeugregistern der anderen Mitgliedstaaten durchzuführen, wenn als Abfragekriterium ein vollständiges Kennzeichen oder eine vollständige Fahrgestellnummer verwendet wird.

#### **Verwendung von Protokolldaten**

§ 26. Protokolldaten nach § 22, 24 und 25 sind zwei Jahre aufzubewahren und nach Ablauf dieser Frist unverzüglich zu löschen. Sie dürfen ausschließlich zum Zwecke der Kontrolle der Verwendung von personenbezogenen Daten verwendet werden. Der Bundesminister für Inneres hat der Datenschutzkommission auf deren Ersuchen Protokolldaten unverzüglich, spätestens jedoch innerhalb von vier Wochen nach Einlangen des Ersuchens zur Verfügung zu stellen.

#### **Einschreiten auf Hoheitsgebiet anderer Mitgliedstaaten**

§ 27. (1) Auf Ersuchen eines Mitgliedstaates ist der Bundesminister für Inneres bei Gefahr im Verzug oder zur Bewältigung einer Massenveranstaltung, Katastrophe oder eines schweren Unglücksfalles ermächtigt, zum Schutz von Leben, Gesundheit oder Eigentum geeignete Organe des öffentlichen Sicherheitsdienstes in diesen Mitgliedstaat zur Durchführung bestimmter Einsätze zu entsenden.

(2) Darüber hinaus können mit Zustimmung des Bundesministers für Inneres zur Intensivierung der polizeilichen Kooperation Organe des öffentlichen Sicherheitsdienstes in einen anderen Mitgliedstaat entsandt und mit der gemeinsamen Wahrnehmung von Aufgaben zur Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit oder der Kriminalpolizei im aufnehmenden Mitgliedstaat betraut werden.

#### **Einschreiten von Organen von Sicherheitsbehörden eines Mitgliedstaates im Inland**

§ 28. (1) Der Bundesminister für Inneres ist bei Gefahr im Verzug ermächtigt, zum Schutz von Leben, Gesundheit oder Eigentum oder zur Bewältigung einer Massenveranstaltung, Katastrophe oder eines schweren Unglücksfalles um Entsendung von geeigneten Organen von Sicherheitsbehörden anderer Mitgliedstaaten zu ersuchen.

(2) Darüber hinaus kann der Bundesminister für Inneres zur Intensivierung der polizeilichen Kooperation Organe von Sicherheitsbehörden anderer Mitgliedsstaaten mit Zustimmung des Entsendestaates mit der Wahrnehmung von Aufgaben zur Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit oder der Kriminalpolizei im Bundesgebiet betrauen.

(3) Die mitwirkenden Organe von Sicherheitsbehörden anderer Mitgliedsstaaten unterliegen bei ihren Einsätzen nach Abs. 1 und 2 der Leitung und den Weisungen der örtlich zuständigen Sicherheitsbehörden.

#### **Befugnisse auf fremdem Hoheitsgebiet**

§ 29. (1) Den Organen von Sicherheitsbehörden anderer Mitgliedstaaten kommen in den Fällen des § 28 im Zuge ihres Einsatzes dieselben Befugnisse und Verantwortlichkeiten zu wie österreichischen

Organen des öffentlichen Sicherheitsdienstes. Sie werden in Bezug auf Straftaten, die sie begehen oder die ihnen gegenüber begangen werden, wie österreichische Beamte behandelt.

(2) Die Organe von Sicherheitsbehörden anderer Mitgliedstaaten sind berechtigt,

1. ihre Uniform zu tragen;
2. ihre Dienstwaffen, Munition sowie sonstige Ausrüstungsgegenstände mitzuführen, es sei denn, die Sicherheitsbehörde verfügt im Einzelfall anderes;
3. mit einem gültigen mit Lichtbild und Unterschrift versehenen Dienstausweis nach Österreich einzureisen und sich so lange aufzuhalten, wie es für die Durchführung des Einsatzes notwendig ist;
4. beim grenzüberschreitenden Einsatz Dienstkraftfahrzeuge zu benutzen;
5. die notwendigen technischen Mittel zu verwenden, die zur Aufgabenerfüllung notwendig sind.

(3) Abs. 2 gilt auch für die Teilnahme an gemeinsamen Schulungen und Einsatzübungen.

(4) Die eingesetzten Fahrzeuge sind hinsichtlich der Befreiung von Verkehrsverboten und Verkehrsbeschränkungen den Fahrzeugen der österreichischen Sicherheitsbehörden gleichgestellt.

(5) Die österreichischen Organe des öffentlichen Sicherheitsdienstes sind ermächtigt, ihre Uniformen, Dienstwaffen, Munition, sonstige Zwangsmittel, Transportmittel und sonstige für den Einsatz notwendige Ausrüstungsgegenstände zu dem Einsatz, zu dem sie zur Unterstützung entsandt wurden, mitzunehmen, sofern dies nach dem Recht des ersuchenden Mitgliedstaates zulässig ist und bindendes Völkerrecht dem nicht entgegen steht.

#### **4. Teil**

### **Nutzung des Visa-Informationssystems durch Sicherheitsbehörden**

#### **Zugriffsberechtigung auf VIS-Daten**

**§ 30.** (1) Die Sicherheitsbehörden ermächtigt, folgende Daten aus dem Visa-Informationssystem (VIS) abzufragen, wenn dies im Einzelfall für Zwecke der Verhütung, Aufdeckung und Ermittlung terroristischer Straftaten nach den §§ 278b und 278c StGB sowie sonstiger schwerwiegender Straftaten, wie sie im Anhang 1 Teil A des EU-JZG angeführt sind, erforderlich ist:

1. Nachname, Geburtsname, frühere Nachnamen, Vorname(n), Geschlecht, Datum, Ort und Land der Geburt;
2. gegenwärtige Staatsangehörigkeit und Staatsangehörigkeit zum Zeitpunkt der Geburt;
3. Art und Nummer des Reisedokuments, ausstellende Behörde, Ausstellungsdatum und Ablauf der Gültigkeit;
4. Hauptreiseziel und Dauer des geplanten Aufenthalts;
5. Zweck der Reise;
6. geplanter Tag der Ein- und Ausreise;
7. geplante Grenzübertrittsstelle der ersten Einreise oder geplante Durchreisroute;
8. Wohnort;
9. Fingerabdrücke;
10. Art und Nummer des Visums;
11. zur Person, die eine Einladung ausgesprochen hat sowie zur Person, die verpflichtet ist, die Kosten für den Lebensunterhalt des Antragstellers während des Aufenthalts zu tragen: Nachname, frühere Nachnamen, Vorname(n), Geschlecht, Datum, Ort und Land der Geburt und Staatsangehörigkeit.

(2) Stimmen die Daten mit den zu einer Person gespeicherten Daten überein, sind die Sicherheitsbehörden ermächtigt, auch

1. alle sonstigen, für Zwecke der Ausstellung eines Visums vorliegende Daten;
2. Lichtbilder;
3. Daten zu früher erteilten, abgelehnten, annullierten, aufgehobenen oder verlängerten Visa zu verwenden.

#### **Übermittlung an Drittstaaten und Sicherheitsorganisationen**

**§ 31.** Die Übermittlung personenbezogener Daten, die aus dem VIS abgefragt wurden, an Sicherheitsbehörden von Drittstaaten und internationale Sicherheitsorganisationen ist nur zulässig

1. bei Gefahr im Verzug für Zwecke der Verhütung und Aufdeckung terroristischer oder sonstiger schwerwiegender Straftaten und
2. nur mit Zustimmung jenes Mitgliedstaates, die die Daten in das VIS eingegeben hat.

#### **Auskunft und Richtigstellung**

§ 32. (1) Soweit Auskunft über abgefragte Daten erteilt werden soll, die von einem anderen Mitgliedstaat in das VIS eingegeben worden sind, darf die Auskunft nur erteilt werden, wenn diesem Mitgliedstaat zuvor Gelegenheit zur Stellungnahme gegeben worden ist. Sind abgefragte Daten von einer österreichischen Behörde, die keine Sicherheitsbehörde ist, eingegeben worden, ist vor Auskunftserteilung deren Zustimmung einzuholen.

(2) Liegen Anhaltspunkte vor, wonach im VIS verarbeitete Daten unrichtig oder unrechtmäßig gespeichert sein könnten, so ist jene Stelle davon in Kenntnis zu setzen, die die Daten in das VIS eingegeben hat.

### **5. Teil**

#### **Schengener Informationssystem**

##### **Schengener Informationssystem**

§ 33. (1) Die Sicherheitsbehörden führen zum Zwecke der Ausschreibung von Personen und Sachen gemeinsam eine zentrale Datenanwendung, das nationale Schengener Informationssystem (N.SIS II). Sie haben diese Daten anderen Mitgliedstaaten im Wege des zentralen Schengener Informationssystems (CS.SIS) zur Verfügung zu stellen. Sie sind ermächtigt, Ausschreibungen der zuständigen Stellen anderer Mitgliedstaaten im Wege des zentralen Schengener Informationssystems zu ermitteln und mit den anderen Daten im N.SIS II weiter zu verarbeiten und zu benützen. Dem Bundesminister für Inneres kommt bei der Führung des nationalen Schengener Informationssystems die Aufgabe des Betreibers gemäß § 50 DSG 2000 zu.

(2) Im Schengener Informationssystem dürfen nur folgende Daten zu Personen verarbeitet werden:

1. Nachname(n) und Vorname(n), Geburtsname(n) und frühere(r) Name(n) sowie Aliasnamen;
2. besondere unveränderliche körperliche Merkmale;
3. Geburtsort und -datum;
4. Geschlecht;
5. Lichtbilder;
6. Fingerabdrücke;
7. Staatsangehörigkeit(en);
8. der Hinweis, ob die Person bewaffnet oder gewalttätig ist oder ob sie entflohen ist;
9. Ausschreibungsgrund;
10. ausschreibende Behörde;
11. eine Bezugnahme auf die Entscheidung, die der Ausschreibung zu Grunde liegt;
12. zu ergreifende Maßnahme;
13. Verknüpfungen zu anderen Ausschreibungen im System;
14. die Art der Straftat.

(3) Fingerabdrücke und Lichtbilder dürfen nur zur Überprüfung der Identität nach einer alphanumerischen Abfrage verwendet werden. Darüber hinaus dürfen Fingerabdrücke, soweit die technischen und unionsrechtlichen Voraussetzungen dafür bestehen, auch als Auswahlkriterium für eine Abfrage verwendet werden.

(4) Ausschreibungen müssen jedenfalls die Angaben zu Abs. 2 Z 1, 4 und 12 und zutreffendenfalls Z 11 enthalten. Darüber hinaus sind alle in Abs. 2 genannten Datenarten anzuführen, soweit sie vorhanden sind.

(5) Ausschreibungen im Schengener Informationssystem dürfen nur vorgenommen werden, wenn dies im Hinblick auf die Maßnahme unbedingt geboten erscheint (§ 29 SPG).

(6) Von den Sicherheitsbehörden abgesehen und unbeschadet der für die Abgabenbehörden im Bereich des Bundesministeriums für Finanzen nach sonstigen Rechtsvorschriften eingeräumten Abfrageberechtigungen darf eine Abfrageberechtigung im Wege des Datenfernverkehrs nur dem Bundesminister für Justiz sowie den Gerichten und Staatsanwaltschaften für Zwecke eines Strafverfahrens eingeräumt werden, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist.

(7) Daten, die gemäß Abs. 1 von den Sicherheitsbehörden verarbeitet werden, dürfen von diesen nicht an Behörden von Drittstaaten oder internationalen Organisationen weitergegeben werden.

(8) Über die in Abs. 2 genannten Datenarten hinaus dürfen keine personenbezogenen Daten verarbeitet werden, welche die rassische Herkunft, politische Anschauungen oder religiöse oder andere Überzeugungen erkennen lassen oder die Gesundheit oder das Sexualleben betreffen.

#### **Zusatzinformationen**

**§ 34.** (1) Die Sicherheitsbehörden stellen dem Sirene-Büro alle Unterlagen zur Verfügung, die den Ausschreibungen im Schengener Informationssystem zu Grunde liegen.

(2) Soweit Sicherheitsbehörden anderer Mitgliedstaaten Zusatzinformationen zu Ausschreibungen der Sicherheitsbehörden benötigen, werden diese vom Sirene-Büro auf Grund der Unterlagen gemäß Abs. 1 erteilt.

(3) Erfolgt der Austausch von Zusatzinformationen automationsunterstützt, sind personenbezogene Daten zu löschen, wenn sie für den verfolgten Zweck nicht mehr benötigt werden. Sie sind jedenfalls spätestens ein Jahr nach der Löschung der entsprechenden Ausschreibung zu löschen.

(4) § 33 Abs. 8 gilt auch für Zusatzinformationen.

#### **Ausschreibung von Personen zum Zwecke der Übergabe oder Auslieferung**

**§ 35.** (1) Die Sicherheitsbehörden sind ermächtigt, auf Ersuchen der Gerichte oder Staatsanwaltschaften Daten zu Personen in das Schengener Informationssystem einzugeben, nach denen mit Europäischem Haftbefehl zum Zwecke der Übergabe oder nach denen für Zwecke der Auslieferung gesucht wird.

(2) Abs. 1 gilt auch für Personen, nach denen zum Zwecke der Übergabe mit Haftbefehl gefahndet wird, der auf Grund eines Übereinkommens zwischen der EU und einem Drittstaat, in dem eine Ausschreibung solcher Haftbefehle im Schengener Informationssystem vorgesehen ist, ausgestellt wurde.

(3) Im Falle einer Ausschreibung auf Grund eines Europäischen Haftbefehls ist dieser in einer Kopie des Originals im Schengener Informationssystem zu verarbeiten.

(4) Im Falle einer Ausschreibung zum Zwecke der Übergabe- oder Auslieferungshaft, hat die ausschreibende Sicherheitsbehörde jedenfalls als Zusatzinformationen (§ 34) den Behörden der anderen Mitgliedstaaten zur Verfügung zu stellen:

1. die Identität und die Staatsangehörigkeit der gesuchten Person;
2. Name, Adresse, Telefon- und Telefaxnummer sowie E-Mail-Adresse der ausstellenden Gerichte oder Staatsanwaltschaften;
3. die Angabe, ob ein vollstreckbares Urteil, ein Haftbefehl oder eine andere vollstreckbare justizielle Entscheidung mit gleicher Rechtswirkung vorliegt;
4. die Art und rechtliche Würdigung der Straftat;
5. die Beschreibung der Umstände, unter denen die Straftat begangen wurde, einschließlich der Tatzeit, des Tatortes und der Art der Tatbeteiligung der gesuchten Person;
6. im Fall eines rechtskräftigen Urteils die verhängte Strafe oder der für die betreffende Straftat im Ausstellungsmitgliedstaat gesetzlich vorgeschriebene Strafrahmen;
7. soweit möglich, die anderen Folgen der Straftat.

(5) Ist die Durchführung der Übergabe- oder Auslieferungshaft auf Grund anderer gesetzlicher Bestimmungen oder internationaler Verpflichtungen nicht möglich, so hat die ausschreibende Sicherheitsbehörde das Sirene-Büro jenes Mitgliedstaates, der die Ausschreibung veranlasst hat, zu ersuchen, die Ausschreibung entsprechend zu kennzeichnen. Solcher Art gekennzeichnete Ausschreibungen gelten als Ausschreibungen zur Aufenthaltsermittlung.

(6) Einer Ausschreibung nach Abs. 1 und 2 kommen die Wirkungen einer Anordnung der Festnahme und ihrer Ausschreibung nach den Bestimmungen der Strafprozessordnung 1975 zu. Wird daher eine Person auf Grund einer Ausschreibung gemäß Abs. 1 oder 2 im Inland betreten, so ist sie unter unverzüglicher Verständigung der Staatsanwaltschaft festzunehmen, und in die Justizanstalt des zuständigen Gerichtes einzuliefern (§ 172 StPO).

#### **Behandlung von Ausschreibungen eines Mitgliedstaates zum Zwecke der Übergabe oder Auslieferung gesuchter Personen**

**§ 36.** Ist eine Festnahme wegen einer die Festnahme ablehnenden gerichtlichen Entscheidung oder im Falle einer Ausschreibung zum Zwecke der Auslieferungshaft wegen einer noch nicht

abgeschlossenen Prüfung nicht möglich, so ist die Ausschreibung als Ausschreibung zur Aufenthaltsermittlung zu behandeln.

#### **Ausschreibung von Abgängigen**

§ 37. (1) Die Sicherheitsbehörden sind ermächtigt, in den in § 57 Abs. 1 Z 7 bis 9 SPG genannten Fällen Ausschreibungen auch im Schengener Informationssystem vorzunehmen.

(2) Wird eine im Schengener Informationssystem von Sicherheitsbehörden eines anderen Staates als abgänglich ausgeschriebene Person angetroffen, ist dem ausschreibenden Sirene-Büro der Aufenthalt des Abgängigen mitzuteilen. Ist die abgängige Person volljährig, bedarf die Mitteilung der Einwilligung des Aufgefundenen. Jedenfalls zulässig ist, das ausschreibende Sirene-Büro sowie die Person, die den Betroffenen als abgänglich gemeldet hat, darüber zu informieren, dass die Person aufgefunden wurde, ohne dass dabei Angaben zum Aufenthaltsort mitgeteilt werden.

#### **Ausschreibung von Personen, die im Hinblick auf ihre Teilnahme an einem Gerichtsverfahren gesucht werden**

§ 38. (1) Die Sicherheitsbehörden sind ermächtigt, auf Ersuchen der Gerichte oder Staatsanwaltschaften für Zwecke der Feststellung des Wohnsitzes oder des Aufenthalts Daten zu folgenden Personen in das Schengener Informationssystem einzugeben:

1. die als Zeugen in einem gerichtlichen Strafverfahren gesucht werden;
2. die als Beschuldigte, die im Rahmen eines Strafverfahrens wegen Taten, deretwegen sie verfolgt werden, vor Gericht geladen sind oder die zum Zwecke der Ladung gesucht werden;
3. denen ein Strafurteil oder andere Schriftstücke im Rahmen eines Strafverfahrens wegen Taten, deretwegen sie verfolgt werden, zuzustellen ist;
4. denen als Verurteilte die Ladung zum Antritt einer gerichtlichen Freiheitsstrafe zugestellt werden muss.

(2) Wird der Wohnsitz oder der Aufenthalt einer nach Abs. 1 ausgeschriebenen Person festgestellt, ist der ausschreibende Mitgliedstaat zu informieren und ihm der Wohnsitz oder der Aufenthalt bekanntzugeben.

#### **Ausschreibung von Personen und Sachen zum Zwecke der verdeckten Kontrolle**

§ 39. (1) Die Sicherheitsbehörden sind ermächtigt, zur Aufklärung und Verfolgung gerichtlich strafbarer Handlungen sowie zur Abwehr gefährlicher Angriffe Personen für Zwecke einer verdeckten Kontrolle im Schengener Informationssystem auszuschreiben, wenn

1. auf Grund bestimmter Tatsachen anzunehmen ist, dass eine Person eine im Anhang 1 zum EU-JZG genannte Straftat plant oder begeht, oder
2. die Gesamtbeurteilung einer Person, insbesondere aufgrund der bisher von ihr begangenen Straftaten, erwarten lässt, dass sie künftig eine im Anhang 1 Teil A zum EU-JZG angeführte Straftat begehen wird.

(2) Ausschreibungen von Land-, Wasser- und Luftfahrzeugen und Containern für verdeckte Kontrollen im Schengener Informationssystem sind zulässig, wenn Anhaltspunkte dafür vorliegen, dass eine Verbindung zu den in Abs. 1 Z 1 und 2 angeführten Fällen besteht.

(3) Bei Vorliegen einer Ausschreibung nach Abs. 1 sind die Sicherheitsbehörden ermächtigt, folgende Informationen verdeckt zu ermitteln und der ausschreibenden Stelle gesondert zu übermitteln:

1. Daten zu den Insassen und Begleitpersonen des Land-, Wasser- oder Luftfahrzeuges, bei denen begründeterweise davon ausgegangen werden kann, dass sie mit den ausgeschriebenen Personen in Verbindung stehen;
2. Reiseweg und Reiseziel;
3. die Auffindung der ausgeschriebenen Person oder des ausgeschriebenen Land-, Wasser- oder Luftfahrzeuges oder Containers;
4. nähere Umstände des Auffindens der Person oder des Land-, Wasser- oder Luftfahrzeuges oder Containers;
5. Ort, Zeit oder Anlass der Kontrolle;
6. Angaben zum benutzten Land-, Wasser- oder Luftfahrzeug oder zum benutzten Container;
7. sowie über allenfalls mitgeführte Gegenstände.

(4) Soweit im Schengener Informationssystem Ausschreibungen für gezielte Kontrollen aufscheinen, sind diese als Ausschreibungen zur verdeckten Kontrollen zu behandeln.

### **Ausschreibung von Sachen zur Sicherstellung oder Beweissicherung**

**§ 40.** (1) Die Sicherheitsbehörden sind ermächtigt, Sachen im Schengener Informationssystem zur Fahndung auszuschreiben, wenn sie zur Sicherstellung oder zur Beweissicherung in Strafverfahren gesucht werden.

(2) Folgende Sachen können gemäß Abs. 1 ausgeschrieben werden:

1. Kraftfahrzeuge mit einem Hubraum von mehr als 50 ccm, Wasserfahrzeuge und Luftfahrzeuge;
2. Anhänger mit einem Leergewicht von mehr als 750 kg, Wohnwagen, industrielle Ausrüstungen, Außenbordmotoren und Container;
3. Schusswaffen;
4. gestohlene, unterschlagene oder sonst abhanden gekommene Blankodokumente;
5. gestohlene, unterschlagene, sonst abhanden gekommene oder für ungültig erklärte ausgefüllte Identitätsdokumente wie insbesondere Pässe, Personalausweise, Führerscheine, Aufenthaltstitel und Reisedokumente;
6. gestohlene, unterschlagene, sonst abhanden gekommene oder für ungültig erklärte Kfz-Zulassungsbescheinigungen und Kfz-Kennzeichen;
7. Banknoten (Registriergeld);
8. gestohlene, unterschlagene, sonst abhanden gekommene oder für ungültig erklärte Wertpapiere und Zahlungsmittel wie Schecks, Kreditkarten, Obligationen, Aktien und Anteilspapiere.

(3) Ergibt eine Abfrage, dass eine Sachenfahndungsausschreibung von Sicherheitsbehörden eines anderen Mitgliedstaates vorliegt, so ist der ausschreibende Mitgliedstaat darüber zu informieren und es sind ihm die näheren Umstände bekannt zu geben. Hierfür ist auch die Übermittlung personenbezogener Daten nach § 33 Abs. 2 Z 1 zulässig. Liegt keine Sicherstellungsanordnung vor, so können die Sicherheitsbehörden von sich aus eine Sicherstellung unter den Voraussetzungen des § 110 Abs. 3 StPO durchführen. Die weitere Vorgangsweise richtet sich nach den Bestimmungen über die Sicherstellung oder die Beschlagnahme von Sachen im Strafverfahren.

### **Speicherfristen**

**§ 41.** Die Sicherheitsbehörden haben die von ihnen in das Schengener Informationssystem eingegebenen Ausschreibungen von Personen längstens alle drei Jahre ab ihrer Eingabe auf die Notwendigkeit der weiteren Speicherung hin zu prüfen. Für Zwecke der verdeckten Kontrolle beträgt diese Frist in Bezug auf Personenausschreibungen ein Jahr und auf Sachenausschreibungen fünf Jahre. Ausschreibungen für Zwecke der Sicherstellung oder zur Beweissicherung in Strafverfahren sind längstens alle zehn Jahre daraufhin zu überprüfen, ob eine über diesen Zeitraum hinausgehende Speicherung erforderlich ist.

### **Richtigstellung und Ergänzung von Ausschreibungen**

**§ 42.** (1) Änderungen, Ergänzungen, Richtigstellungen und Aktualisierungen von Daten im Schengener Informationssystem dürfen Sicherheitsbehörden nur hinsichtlich der von ihnen selbst vorgenommenen Ausschreibungen durchführen.

(2) Hat eine Sicherheitsbehörde Anhaltspunkte dafür, dass Daten einer Ausschreibung im Schengener Informationssystem unrichtig oder unrechtmäßig gespeichert wurden, teilt sie dies, soweit es sich um Ausschreibungen anderer Mitgliedstaaten handelt, diesen im Wege des Sirene-Büros unverzüglich, jedoch längstens innerhalb von 10 Tagen, mit.

(3) Kommen Anhaltspunkte hervor, die Zweifel an der eindeutigen Unterscheidbarkeit ausgeschriebener Personen aufkommen lassen, so hat die Sicherheitsbehörde, soweit es sich nicht um eine von ihr selbst veranlasste Ausschreibung handelt, den Sachverhalt abzuklären und im Wege des Sirene-Büros Zusatzinformationen mit der ausschreibenden Stelle auszutauschen. Die Sicherheitsbehörde hat, soweit dies zur eindeutigen Identifizierung einer von ihr ausgeschriebenen Person erforderlich ist, die Ausschreibung um zusätzliche Informationen zu ergänzen.

(4) Besteht die Möglichkeit, dass eine von einer Ausschreibung nicht betroffene Person mit einer tatsächlich ausgeschriebenen verwechselt wird, darf die Sicherheitsbehörde mit ausdrücklicher Zustimmung des Betroffenen die Ausschreibung um dessen Namen, besondere unveränderliche körperliche Merkmale, Geburtsdatum und -ort, Geschlecht, Lichtbild, Fingerabdruck, Staatsangehörigkeit und Daten von Ausweisdokumenten ergänzen. Betroffene sind auf diese Möglichkeit hinzuweisen. Ihre Daten dürfen nur zur Feststellung, dass sie von der Ausschreibung nicht betroffen sind, verwendet werden.

### **Auskunftsrecht**

§ 43. Im Falle einer Auskunft nach § 26 DSG 2000 dürfen Daten, die von einem anderen Mitgliedstaat eingegeben wurden, nur mitgeteilt werden, wenn dem Mitgliedstaat, der die Daten eingegeben hat, Gelegenheit zur Stellungnahme gegeben worden ist.

## **6. Teil**

### **Schlussbestimmungen**

#### **Verweisungen**

§ 44. Soweit in diesem Bundesgesetz auf Bestimmungen anderer Bundesgesetze verwiesen wird, sind diese in ihrer jeweils geltenden Fassung anzuwenden. Verweise auf andere Rechtsnormen beziehen sich auf die Rechtsnorm zum Zeitpunkt der Kundmachung des Verweises nach diesem Bundesgesetz.

#### **Sprachliche Gleichbehandlung**

§ 45. Soweit in diesem Bundesgesetz auf natürliche Personen bezogene Bezeichnungen in männlicher Form angeführt sind, beziehen sie sich auf Frauen und Männer in gleicher Weise. Bei der Anwendung der Bezeichnung auf bestimmte natürliche Personen ist die jeweils geschlechtsspezifische Form zu verwenden.

#### **Inkrafttreten**

§ 46. Dieses Bundesgesetz tritt mit 1.1.2010 in Kraft.

**Anhang****Liste anderer Formen schwerer Kriminalität, für die Europol zuständig ist**

Illegaler Handel mit Drogen,  
Geldwäschehandlungen,  
Kriminalität im Zusammenhang mit nuklearen und radioaktiven Substanzen,  
Schleuserkriminalität,  
Menschenhandel,  
Kraftfahrzeugkriminalität,  
vorsätzliche Tötung, schwere Körperverletzung,  
illegaler Handel mit Organen und menschlichem Gewebe,  
Entführung, Freiheitsberaubung und Geiselnahme,  
Rassismus und Fremdenfeindlichkeit,  
Raub in organisierter Form,  
illegaler Handel mit Kulturgütern, einschließlich Antiquitäten und Kunstgegenständen,  
Betrugsdelikte,  
Erpressung und Schutzgelderpressung,  
Nachahmung und Produktpiraterie,  
Fälschung von amtlichen Dokumenten und Handel damit,  
Geldfälschung, Fälschung von Zahlungsmitteln,  
Computerkriminalität,  
Korruption,  
illegaler Handel mit Waffen, Munition und Sprengstoffen,  
illegaler Handel mit bedrohten Tierarten,  
illegaler Handel mit bedrohten Pflanzen- und Baumarten,  
Umweltkriminalität,  
illegaler Handel mit Hormonen und Wachstumsförderern.



## **Artikel 2**

### **Änderung des Polizeikooperationsgesetzes**

Das Polizeikooperationsgesetz (PolKG), BGBl. I Nr. 104/1997, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 114/2007, wird wie folgt geändert:

1. *In § 8 Abs. 2 wird die Wortfolge „Für Mitgliedstaaten des Schengener Durchführungsübereinkommens oder des Europol-Übereinkommens“ durch die Wortfolge „Für im Anwendungsbereich des EU-Polizeikooperationsgesetzes (EU-PolKG) befindliche Staaten (Art. 24 Abs. 1 und 38 EUV)“ ersetzt.*

2. *Dem § 8 wird folgender Abs. 4 angefügt:*

„(4) Soweit die Zulässigkeit der Übermittlung von Daten von der Zustimmung oder Genehmigung eines Gerichtes oder einer Staatsanwaltschaft abhängig ist, hat die Amtshilfe leistende Sicherheitsbehörde vor der Übermittlung der Daten die Zustimmung oder Genehmigung einzuholen.“

3. *Dem § 20 wird folgender Abs. 5 angefügt:*

„(5) § 8 Abs. 2 und 4 in der Fassung des Bundesgesetzes BGBl. I Nr. XXX/2009 tritt mit 1. Jänner 2010 in Kraft.“

## **Artikel 3**

### **Änderung des Sicherheitspolizeigesetzes**

Das Sicherheitspolizeigesetz (SPG), BGBl. Nr. 566/1991, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 72/2009, wird wie folgt geändert:

1. *In § 58b Abs. 1 lautet der zweite Satz:*

„Zu diesen Zwecken dürfen die zuständigen Stellen auch Daten über angehaltene Menschen einschließlich eines anlässlich der Aufnahme anzufertigenden Lichtbildes in einem vom Bundesminister für Inneres betriebenen Informationsverbundsystem automationsunterstützt verwenden, soweit sie sich auf strafbare Handlungen oder auch für den Vollzug relevante Lebensumstände einschließlich ihres Gesundheitszustandes und ihrer ethnischen oder religiösen Zugehörigkeit beziehen.“

2. *Dem § 58b Abs. 4 wird folgender Satz vorangestellt:*

„Lichtbilder sind bei Entlassung des Betroffenen zu löschen.“

3. *In § 91c Abs. 1 wird vor der Wortfolge „durch verdeckte Ermittlung (§ 54 Abs. 3)“ die Wortfolge „durch Observation (§ 54 Abs. 2)“ eingefügt.*

4. *Dem § 94 wird folgender Abs. 28 angefügt:*

„(28) Die §§ 58b Abs. 1 und 4 sowie 91c Abs. 1 in der Fassung des Bundesgesetzes BGBl. I Nr. XXX/2009 treten mit 1. Jänner 2010 in Kraft.“