

REPUBLIK ÖSTERREICH  DATENSCHUTZRAT

BALLHAUSPLATZ 2, A-1014 WIEN  
GZ • BKA-817.230/0002-DSR/2009  
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-3@bmi.gv.at](mailto:bmi-III-3@bmi.gv.at)

**Betrifft:** 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

### **Stellungnahme des Datenschutzrates**

Der **Datenschutzrat** hat in seiner 190. Sitzung am 9. Oktober 2009 **einstimmig beschlossen**, zu der im Betreff genannten Thematik folgende Stellungnahme abzugeben:

Der **Datenschutzrat** verweist ausdrücklich auf die Problematik, dass aufgrund des **primärrechtlichen Ausschlusses der unmittelbaren Anwendbarkeit von Beschlüssen** in Art. 34 Abs. 2 lit. c EUV der **Europol-Beschluss keine subjektiven Rechte oder Pflichten von Rechtsunterworfenen begründen kann**. Alle 26 Mitgliedstaaten haben somit die subjektiven Rechte **auch auf nationaler Ebene** einzuräumen, was wiederum eine **große Rechtsunsicherheit aufgrund der unterschiedlichen Datenschutzniveaus in den verschiedenen Mitgliedstaaten, bzw. bei der Ausgestaltung der subjektiven Rechte wie z.B. des Auskunftsrechtes der Betroffenen**, zur Folge hat.

Das BMI wird daher aufgefordert, die unter Art. I 2. Teil (§§ 5 ff) näher ausgeführte Problematik auch in den internationalen Gremien zu thematisieren.

### Allgemeines zu Art. I 2. Teil (§§ 5 ff) (Zusammenarbeit mit Europol):

1. Aufgrund des primärrechtlichen Ausschlusses der unmittelbaren Anwendbarkeit von Beschlüssen in Art. 34 Abs. 2 lit. c EUV kann der Europol-Beschluss keine subjektiven Rechte oder Pflichten von Rechtsunterworfenen begründen. Das gleiche gilt auch für Durchführungsmaßnahmen des Rates nach der vorzitierten Bestimmung [Schweitzer/Hummer/Obwexer, Europarecht (2007), 375]. Um innerstaatliche Rechtswirkungen zu entfalten bedarf es in Österreich auch bei Durchführungsmaßnahmen erst der Inkorporation (Schweitzer/Hummer/Obwexer, 365), wofür im vorliegenden Fall nur eine spezielle Transformation in Betracht zu kommen scheint. Da es um die Umsetzung unionsrechtlicher Vorgaben geht, ist eine Umsetzung der Bestimmungen, mit denen subjektive Rechte eingeräumt werden sollen, durch den österreichischen Gesetzgeber nicht nur rechtlich zulässig, sondern auch unionsrechtlich geboten.

Die im Entwurf enthaltenen Bestimmungen scheinen jedenfalls aus datenschutzrechtlicher Sicht, gemessen an Kapitel V des Europol Beschlusses, zu wenig detailliert. Fraglich ist auch, ob nicht auch die grundsätzliche Befugnis von Europol zur Speicherung von Daten (Kapitel II des Beschlusses), die ja einen Eingriff in das Recht auf Geheimhaltung nach § 1 Abs. 1 DSG 2000 darstellt, einer Umsetzung bedarf.

2. Es wäre aus systematischen Gründen (LRL 11; vgl. auch die Vermeidung von *leges fugitivae* in LRL 65) wünschenswert, die Zusammenarbeit mit Europol an dieser Stelle abschließend zu regeln und jedenfalls für diesen Bereich nicht daneben auch Regelungen im PolKG zu belassen.

### Zu Art. 1 § 6 ( Nationale Europol-Stelle ) :

1. Auch wenn sich dies letztlich aus dem gemäß § 1 Abs. 2 des Entwurfes geltenden PolKG ergibt (vgl. soeben Allgemeines zum 2. Teil, Pkt. 2.) , scheint es aus Gründen der Übersichtlichkeit ratsam, an dieser Stelle ausdrücklich festzulegen, dass Nationale Europol-Stelle der Bundesminister für Inneres ist (ähnlich wie in § 20 Abs. 2 des Entwurfes für die grenzüberschreitende Zusammenarbeit; vgl. LRL 11 und 54).

2. In Abs. 3 erster Satz ist vorgesehen, dass der Bundesminister für Inneres nachgeordneten Sicherheitsbehörden mittels schriftlicher Weisung „den unmittelbaren Kontakt mit Europol einräumen“ kann. Abgesehen von der Formulierung dieses Satzes (es könnte z.B. besser von der „Befugnis, direkt mit Europol Informationen auszutauschen“ gesprochen werden), ist die Begründung einer außenwirksamen Zuständigkeit durch Weisung – definitionsgemäß eine behördeninterne Norm (vgl. *Walter/Mayer/Kucsko-Stadlmayer*, Bundesverfassungsrecht<sup>10</sup>, Rz. 612) – verfassungsrechtlich nicht möglich. Denkbar wäre nur ein nicht außenwirksames „zwischenbehördliches Mandat“, bei dem gegenüber den Rechtsunterworfenen die Verantwortung des Bundesministers aufrecht bleibt (vgl. *Raschauer*, Allgemeines Verwaltungsrecht<sup>3</sup>, Rz 174). Relevant ist dies insbesondere im Hinblick auf die Zurechnung der mit dem Informationsaustausch regelmäßig verbundenen Eingriffe in das Recht auf Geheimhaltung nach § 1 Abs. 1 DSG 2000.

3. In Abs. 4 ist zunächst nicht klar, was unter „Drittorganisationen“ zu verstehen ist. Weiters ist das Verhältnis bzw. der Unterschied zwischen dem ersten und dem dritten Satz (Erteilung der Zustimmung unter Auflagen vs. Bindung an die Einhaltung von Auflagen) nicht erkennbar.

#### Zu Art. 1 § 7 (Entsendung von Verbindungsbeamten zu Europol) :

1. Das Verhältnis zwischen der Nationalen Europol-Stelle und den Verbindungsbeamten ist nicht klar: Welche Konsequenzen folgen aus der Entsendung? Besteht insbesondere nach wie vor eine Bindung an Weisungen (Art. 20 Abs. 1 B-VG), wie dies im Hinblick auf Art. 9 Abs. 1 des Europol-Beschlusses naheliegender wäre?

2. Auch die Aufgaben der Verbindungsbeamten überschneiden sich mit jenen der Nationalen Europol-Stelle. Es ist einzuräumen, dass diesbezüglich auch der Europol-Beschluss (Art. 9 Abs. 3) einiges offen lässt. Umso mehr sollte auf innerstaatlicher Ebene eine Präzisierung erfolgen, insbesondere im Hinblick darauf, ob der Informationsaustausch zwischen der Nationalen Kontaktstelle und Europol (§ 6 Abs. 2 Z 1 bis 6) ausschließlich über die Verbindungsbeamten zu erfolgen hat.

3. Die an Art. 9 Abs. 2 des Europol-Beschlusses angelehnte Formulierung „Wahrnehmung der Interessen Österreichs“ in § 7 Abs. 2 Z 1 des Entwurfes erscheint sehr weit und unbestimmt. Ist damit etwa auch die Vertretung im Verwaltungsrat (Art. 37 ff des Europol-Beschlusses) gemeint? Für die Bestellung der dortigen Vertreter und deren Rechtsstellung würde sonst eine gesetzliche Regelung (insbesondere auch hinsichtlich der Zuständigkeit und Form der Entsendung) fehlen.

Zu Art. 1 § 9 (Europol-Informationssystem) :

1. Es fehlt eine Regelung, die Art. 12 Abs. 2 des Europol-Beschlusses umsetzt: Die nationale Kontaktstelle darf die in § 9 Abs. 1 Z 1 bis 7 des Entwurfes aufgezählten Datenarten nicht selbst ändern, wenn sie von einer anderen nationalen Kontaktstelle eingegeben wurden. Wünscht sie eine Veränderung, so hat sie diese Kontaktstelle anzusprechen.

2. Andererseits erscheint die Regelung in Abs. 6 im Sinne der obigen Allgemeinen Ausführungen zum zweiten Teil überschießend: Sie sollte sich auf die Rechte und Pflichten der österreichischen nationalen Kontaktstelle in den Fällen beschränken, dass entweder die österreichische Kontaktstelle Daten nach Abs. 1 Z 1 bis 7 löschen will, und weitere Daten nach Abs. 2 vorhanden sind, oder dass die österreichische nationale Kontaktstelle als nächste nach der löschenden ausländischen Kontaktstelle Daten nach Abs. 2 eingegeben hat.

3. Bei den Datenarten in § 9 Abs. 1 Z 6 fällt auf, dass hier auch die Sozialversicherungsnummern mitumfasst sind.

Dazu ist einerseits anzumerken, dass sich aus dem Europol-Beschluss **keine zwingende Verpflichtung zur Speicherung der Sozialversicherungsnummer ergibt**. Gem. Art. 12 Abs. 2 lit f iVm Abs. 1 Europol-Beschluss dürfen im Europol-Informationssystem gespeicherte personenbezogene Daten nur bestimmte Datenkategorien umfassen, wozu insbesondere Sozialversicherungsnummern gehören. Aus dem Wortlaut des Art. 12 Abs. 2 leg. cit. folgt, dass hier der maximale Rahmen der zur Speicherung zugelassenen Datenarten festgelegt wird. Eine unmittelbare Verpflichtung zur Speicherung sämtlicher der genannten Datenarten ergibt sich aus dem Europol-Beschluss nicht. Auch die Einbeziehung der Erwägungsgründe zum Beschluss ergeben keine andere Beurteilung. Eine solche

Pflicht zur vollständigen Speicherung aller Kategorien könnte insofern nur der nationale Gesetzgeber statuieren.

Andererseits besteht bei der Datenkategorie „Sozialversicherungsnummer“ ein hohes Risiko dahingehend, dass sich diese zu einer Art universellem „Personenkennzeichen“ entwickelt. Mit Blick auf die datenpolitisch unerwünschte Konsequenz eines umfassenden Rückgriffs auf ein solches Datum – nämlich die problemlose Verknüpfbarkeit sämtlicher über eine Person verfügbarer Daten – erscheint es problematisch, an dieser Stelle eine gesetzliche Ermächtigung zur Verwendung der Sozialversicherungsnummer neu einzuführen.

#### Zu Art. 1 § 10 (Arbeitsdateien zu Analysezwecken) :

Anders als in § 6 Abs. 4, wo in den Verweis auf § 8 PolKG klar wird, dass Datenschutzaspekte für die Weitergabe von Daten unter Auflagen entscheidend sind, fehlt in § 10 Abs. 3 des Entwurfes eine nach Art. 18 B-VG erforderliche Determinierung für die Datenweitergabe unter Auflagen.

#### Zu Art. 1 § 12 (Speicher- und Löschrufen) :

Auch diese Regelung sollte sich auf die Mitteilungsverpflichtung der österreichischen nationalen Europol-Stelle beschränken und keine Verpflichtung von Europol beinhalten.

#### Zu Art. 1 § 14 (Nationale Kontrollinstanz) :

Bei dieser Art der Regelung, die teilweise (insb. in Abs. 2) Regelungen des DSG 2000 derogiert (zumindest werden diese in anderer sprachlicher Form wiederholt) könnten Auslegungsschwierigkeiten entstehen, inwieweit darüber hinaus die Bestimmungen des DSG 2000, speziell die §§ 30 f leg. cit., anzuwenden sind (zB § 30 Abs. 5 oder § 31 Abs. 3 und 4). Darüber hinaus wird ein nach § 6 Abs. 3 des Entwurfes möglicher Direktkontakt mit Europol unberücksichtigt. Die Bestimmung könnte z.B. folgendermaßen gefasst werden:

„§ 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 Kontrollstelle Zugang zu ihren Diensträumen und ihren Akten zu gewähren. Über entsprechende Aufforderung sind Akten der nationalen Kontrollinstanz zu übermitteln.“

Zu Art. 1 § 15 (Gemeinsame Kontrollinstanz) :

Der in Abs. 1 vorgesehene Entsendungsmodus entspricht nicht der derzeitigen Praxis: Erstens steht demnach die Zugehörigkeit zur Gemeinsamen Kontrollinstanz auch Ersatzmitgliedern der Datenschutzkommission offen, andererseits ist die nach Art. 34 Abs. 1 des Europol-Beschlusses mögliche Entsendung von Stellvertretern nicht vorgesehen. Als solche fungieren derzeit Mitarbeiter der Geschäftsstelle der Datenschutzkommission, die der Kommission selbst jedoch nicht angehören.

Zu Art. 1 § 16 Abs. 2 (Auskunft) :

Hier fällt auf, dass das vorgesehene Auskunftsrecht sowohl hinter dem allgemeinen Standard des DSG 2000 als auch der Vorgaben des Rahmenbeschlusses (RB) für den Datenschutz in der 3. Säule (2008/977/JI) zurückbleibt. Weder in § 26 Abs 2 DSG 2000 noch in Art. 17 Abs. 2 RB 2008/977/JI findet sich nämlich der Verweigerungsgrund der potentiellen Verletzung der „öffentliche Ordnung“. Im Übrigen besteht hier Redundanz mit Ziff. 3 des § 16 Abs. 2 des hier diskutierten Entwurfs. Zudem wird – anders als in § 26 Abs 2 DSG 2000 - nicht auf wichtige „außenpolitische, wirtschaftliche oder finanzielle Interessen“ der Republik Österreich abgestellt, sondern sehr viel weiter auf „andere wesentliche“ Interessen. Unter letzteren Begriff lässt sich freilich nahezu jedes Interesse subsumieren. Schon aus Gründen des verfassungsrechtlichen Determinierungsgebotes erscheint hier eine restriktivere Fassung geboten. Warum eine Auskunftserteilung etwa die öffentliche Ruhe beeinträchtigen können soll bzw. ein solches vages Kriterium eine Auskunftsverweigerung rechtfertigen können soll, erscheint mehr als fraglich. Es sollte daher – wie auch im RB 2008/977/JI und im DSG 2000 - für die Zulässigkeit von Auskunftsverweigerungen lediglich auf die „öffentliche Sicherheit“ und nicht auf „öffentliche Ruhe und Ordnung“ abgestellt werden.

#### Zu Art. 1 § 21 (DNA-Analysedatei) :

Das dem DNA-Abgleich nach dem Prümer Beschluss zu Grunde liegende Konzept eines „Hit-/No-Hit-Systems“ kommt in der Bestimmung nicht hinreichend zum Ausdruck. Wesentlich ist, dass die Fundstellendatensätze keinen unmittelbaren Rückschluss auf die Person, der sie zugeordnet sind, enthalten. Dieses in Art. 2 Abs. 2 zweiter Satz des Prümer Beschlusses ausdrücklich ausgesprochene Verbot sollte auch in den Entwurf übernommen werden. § 21 Abs. 3 Z 2 des Entwurfes lässt offen, wem eine Zuordnung ermöglicht werden soll.

#### Zu Art. 1 § 22 (Verwendung der Daten der DNA-Analysedateien) :

In Abs. 3 wird das einzige Mal das aus dem Prümer Beschluss stammende Wort „Fundstellendatensätze“ verwendet, während der Entwurf ansonsten von den in § 20 definierten „DNA-Profilen“ spricht. Die Terminologie sollte vereinheitlicht werden (vgl. LRL 31). Im Zusammenhang mit der zuvor bei § 21 angemerkten Unklarheit könnten durch verschiedene Ausdrücke weitere Auslegungsschwierigkeiten entstehen, ob DNA-Profile mehr oder weniger Identifikatoren enthalten als Fundstellendatensätze oder umgekehrt.

#### Zu Art. 1 § 23 (Ermittlung erkennungsdienstlicher Daten für Zwecke der Amtshilfe) :

Das Eigenschaftswort „innerstaatlich“ wird in Abs. 1 in einer anderen Bedeutung verwendet als in Abs. 2: In Abs. 1 sind mit „innerstaatlichen Fällen“ Sachverhalte gemeint, die die Vornahme erkennungsdienstlicher Maßnahmen in Österreich rechtfertigen. In Abs. 2 hingegen ist mit dem „jeweiligen innerstaatlichen Recht“ die Rechtsordnung eines fremden (Mitglied-)Staates gemeint. Hier sollten unterschiedliche Begriffe verwendet werden (vgl. LRL 31).

#### Zu Art. 1 § 24 (Verwendung daktyloskopischer Daten) :

Die informierten Vertreter des BMI sagten dem Datenschutzrat zu, bei der Regelung über die Verwendung von daktyloskopischer Daten dieselben datenschutzrechtlichen Standards vorzusehen wie bei den DNA-Daten.

Unbedingt müsste auch hier das „Hit-/No-Hit-System“ (dh keine unmittelbare Identifikation des Fundstellendatensatzes möglich) ausdrücklich festgeschrieben werden.

Zu Art. 1, Überschrift zum 4. Teil (VISA-Informationssystem) :

Die Überschrift ist insofern irreführend, als sie eine umfassende Regelung über die nationalen Zuständigkeiten für das VIS verheißt, obwohl nur ein (kleiner) Aspekt, nämlich die Nutzung dieses Systems für schwerwiegende Straftaten geregelt wird, was erst aus § 29 Abs. 1 erkennbar wird.

Zu Art. 1 § 29 (Zugriffsberechtigung auf VIS-Daten) :

1. Der einleitende Halbsatz in Abs. 1 sollte umformuliert werden: Das VIS besteht bereits auf Grundlage der in den Erläuterungen erwähnten gemeinschaftsrechtlichen Rechtsakte (Entscheidung 2004/512/EG und Verordnung (EG) Nr. 767/2008). Daher könnte es einfach lauten: „Die Sicherheitsbehörden sind ermächtigt, folgende Daten aus dem Visa-Informationssystem (VIS) abzufragen,...“.

2. Zu Abs. 3 gilt das oben zu § 6 Abs. 3 Ausgeführte.

Zu Art. 1, Überschrift zum 5. Teil (Schengener Informationssystem) :

Hier gilt das zur Überschrift zum 4. Teil Ausgeführte sinngemäß: Auch beim Schengener Informationssystem erfolgt nur eine Regelung im Hinblick auf jene Aspekte, die der Beschlusses 2007/533/JI abdeckt, also die „Dritte Säule“. Freilich stellt sich die Frage, ob es nicht zweckmäßig wäre, auch die innerstaatlichen Zuständigkeiten für den im Rahmen der „ersten Säule“ geregelten Teil des SIS II festzulegen.

Allgemeines zu Art. 1, 5. Teil (Schengener Informationssystem) :

Es fehlt sowohl in § 32 als auch in den Paragraphen, die die innerstaatliche Handhabung der verschiedenen Ausschreibungskategorien regeln (§§ 37 ff) eine Ermächtigung zur Abfrage (Benutzung) von Ausschreibungen aus dem N.SIS (II) durch die Sicherheitsbehörden (vgl. z.B. § 57 Abs. 3 SPG).



Zu Art. 1 § 32 (Schengener Informationssystem) :

1. Die Errichtung und Inbetriebnahme des N.SIS II erfolgt auf Grundlage der Verordnung (EG) Nr. 1987/2006 bzw. besteht für den Bereich der dritten Säule dazu eine Verpflichtung auf Grund des Beschlusses 2007/533/JI. Daher sollte es in Abs. 1 erster Satz statt „sind ermächtigt“ einfach „führen“ heißen. Der zweite Satz könnte lauten: „In diesem System werden auch alle Ausschreibungen der zuständigen Stellen anderer Mitgliedstaaten verarbeitet.“

2. In Abs. 1 wird für das nationale Schengener Informationssystem einmal die Abkürzung „N.SIS II“ und einmal die Abkürzung „N.SIS“ festgelegt.

3. Mit der Stellung als Dienstleister (§ 4 Z 5 DSG 2000) ist nach § 11 Abs. 1 Z 1 leg. cit. gesetzlich ein Weisungsrecht des Auftraggebers (§ 4 Z 4 leg. cit.) verbunden. Die Einrichtung des Bundesministers als Dienstleister nachgeordneter Sicherheitsbehörden widerspricht damit seiner Stellung als oberstes Organ bzw. oberste Sicherheitsbehörde nach Art. 19 Abs. 1, Art. 20 Abs. 1 und Art. 78a Abs. 1 B-VG.

4. Die Voraussetzung „soweit die technischen und völkerrechtlichen Voraussetzungen dafür bestehen“ in Abs. 4 ist sehr unbestimmt. Es stellt sich auch die Frage, ob es statt „völkerrechtlichen“ nicht „unionsrechtlichen“ lauten müsste. Besonders bedenklich wäre ein solcher Verweis schlicht auf „Völkerrecht“ im Hinblick auf nicht unmittelbar anwendbare Völkerrechtsakte (bzw. Unionsrechtsakte; vgl. sinngemäß Rz. 44 des EU-Addendums).

Zu Art. 1 § 33 (Zusatzinformationen) :

Es wäre auch hier zweckmäßig, ausdrücklich festzulegen, welche Stelle die Aufgaben des Sirene-Büros wahrnimmt (vgl. oben Pkt. 1. zu § 6).

Zu Art. 1 § 38 (Ausschreibung von Personen und Sachen zum Zweck der verdeckten Kontrolle) :

In Abs. 3 sollte klargestellt werden, dass es sich bei diesen Informationen um Zusatzinformationen im Sinn des § 32 und nicht etwa um einen Teil der Ausschreibung handelt.

14. Oktober 2009  
Für den Datenschutzrat:  
Der Vorsitzende:  
WÖGERBAUER

**Elektronisch gefertigt**