



EUROPEAN DATA PROTECTION SUPERVISOR

Stellungnahme 3/2016

Stellungnahme zum Austausch von Informationen über Drittstaatsangehörige mit Hilfe des Europäischen Strafregisterinformations- systems (ECRIS)



13. April 2016

Der Europäische Datenschutzbeauftragte (EDSB) ist eine unabhängige Einrichtung der EU und hat nach Artikel 41 Absatz 2 der Verordnung (EG) Nr. 45/2001 „im Hinblick auf die Verarbeitung personenbezogener Daten (...) sicherzustellen, dass die Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere ihr Recht auf Privatsphäre, von den Organen und Einrichtungen der Gemeinschaft geachtet werden“; er ist „für die Beratung der Organe und Einrichtungen der Gemeinschaft und der betroffenen Personen in allen die Verarbeitung personenbezogener Daten betreffenden Angelegenheiten“ zuständig. Gemäß Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 ist die Kommission zur Konsultation des EDSB verpflichtet, „wenn [sie] einen Vorschlag für Rechtsvorschriften bezüglich des Schutzes der Rechte und Freiheiten von Personen bei der Verarbeitung personenbezogener Daten annimmt“.

Er wurde zusammen mit dem Stellvertretenden Datenschutzbeauftragten im Dezember 2014 ernannt und spezifisch mit einem konstruktiven und proaktiven Vorgehen beauftragt. In der im März 2015 veröffentlichten Fünf-Jahres-Strategie legt der EDSB dar, wie er diesen Auftrag auf verantwortungsvolle Weise zu erfüllen gedenkt.

In dieser Stellungnahme geht es um den Auftrag des EDSB, die EU-Organe bezüglich der Datenschutzimplikationen ihrer Politiken zu beraten und eine verantwortliche Politikgestaltung zu fördern, im Einklang mit Maßnahme 9 der Strategie des EDSB: „Förderung einer verantwortungsvollen und fundierten politischen Entscheidungsfindung“. Nach Auffassung des EDSB spielt die Erfüllung der Datenschutzauflagen eine zentrale Rolle für den Erfolg des Informationsaustauschs über Strafregistereinträge von Drittstaatsangehörigen mit Hilfe des ECRIS.

Zusammenfassung

Schon seit langem plante der EU-Gesetzgeber die Ausweitung des Austauschs von Strafregisterinformationen in der EU im ECRIS (Europäisches Strafregisterinformationssystem) auf Drittstaatsangehörige. Der Vorschlag zur Ausweitung des ECRIS auf Drittstaatsangehörige wurde noch durch die Europäische Sicherheitsagenda beschleunigt, in der es heißt: „Bei in der EU verurteilten Nicht-EU-Bürgern (...) funktioniert das System nicht einwandfrei“.

Der ECRIS-Rahmen verwendet derzeit die Staatsangehörigkeit eines Mitgliedstaats von verurteilten Personen als Aufhänger für den Informationsaustausch. Deshalb ist der Aufbau eines Parallelsystems für Drittstaatsangehörige gerechtfertigt. Die Kommission entschied sich für einen Austausch von Strafregisterinformationen über Drittstaatsangehörige in einem dezentralen System, in dem ein Indexfilter für jeden teilnehmenden Mitgliedstaat verwendet wird. Der Indexfilter wird bei jeder Verurteilung eines Drittstaatsangehörigen mit spezifischen Informationen aktualisiert und dann an die anderen Mitgliedstaaten übersandt.

Der EDSB hat den Richtlinienvorschlag sorgfältig geprüft und als Hilfestellung für den Gesetzgeber Empfehlungen formuliert, mit denen sichergestellt werden soll, dass die neuen Maßnahmen im Einklang mit dem EU-Datenschutzrecht und insbesondere mit den Artikeln 7 und 8 der EU-Charta der Grundrechte stehen.

Der EDSB begrüßt zwar den Vorschlag für ein dezentrales EU-System für die Verarbeitung von Daten über Strafregisterinformationen über Drittstaatsangehörige, das einen Abgleich auf Treffer durchführt und mit technischen Vorkehrungen Eingriffe in das Recht auf Schutz des Privatlebens und auf den Schutz personenbezogener Daten beschränken soll, doch möchte er trotzdem in dieser Stellungnahme drei Hauptprobleme ansprechen und noch weitere Empfehlungen formulieren.

Erstens sollte für Drittstaatsangehörige eine der für EU-Bürger geltenden entsprechende Regelung für die Verarbeitung von Fingerabdrücken vorgesehen werden, die den Besonderheiten der nationalen Strafjustizsysteme und somit den Erfordernissen der Notwendigkeit und Verhältnismäßigkeit der Verarbeitung personenbezogener Daten Rechnung trägt.

Zweitens heißt es im Vorschlag unzutreffenderweise, die Informationen im Indexfilter seien „anonym“. Der EDSB empfiehlt eine Klarstellung dahingehend, dass es sich bei den für die Zwecke des ECRIS für Drittstaatsangehörige verarbeiteten Informationen um personenbezogene Daten handelt, die pseudonymisiert, nicht jedoch anonymisiert wurden.

Drittens vertritt der EDSB die Ansicht, dass der Aufbau eines Systems für die Verarbeitung von Daten von EU-Bürgern, die die Staatsangehörigkeit eines Drittlandes haben, und das sich von dem für EU-Bürger bereits bestehenden System unterscheidet, nicht dem im EU-Datenschutzrecht postulierten Erfordernis der Notwendigkeit entspricht und Diskriminierung zur Folge haben könnte. Daher empfiehlt der EDSB, mit den Maßnahmen im Vorschlag nur auf Drittstaatsangehörige und nicht auch auf EU-Bürger abzuheben, die auch die Staatsangehörigkeit eines Drittlandes besitzen.

INHALTSVERZEICHNIS

I.	EINLEITUNG UND HINTERGRUND	4
1.1	KONSULTATION DES EDSB	4
1.2	ZIEL DES VORSCHLAGS	4
II.	DATENSCHUTZIMPLIKATIONEN	5
II.1	SACHLICHER ANWENDUNGSBEREICH DER VORGESCHLAGENEN MASSNAHME	6
A.	<i>Verarbeitung von Fingerabdrücken</i>	6
B.	<i>Anonymisierung/Pseudonymisierung</i>	9
C.	<i>Kategorien von zu verarbeitenden personenbezogenen Daten</i>	11
II.2	PERSÖNLICHER GELTUNGSBEREICH DER MASSNAHME	12
II.3	QUALITÄT DER DATEN	13
III.	SCHLUSSFOLGERUNG	13

DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 16,

gestützt auf die Charta der Grundrechte der Europäischen Union, insbesondere auf Artikel 7 und 8,

gestützt auf die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr,

gestützt auf die Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, insbesondere auf Artikel 28 Absatz 2, Artikel 41 Absatz 2 und Artikel 46 Buchstabe d,

gestützt auf den Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden —

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

I. EINLEITUNG UND HINTERGRUND

1.1 Konsultation des EDSB

1. Am 19. Januar 2016 veröffentlichte die Europäische Kommission einen Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Änderung des Rahmenbeschlusses 2009/315/JI des Rates im Hinblick auf den Austausch von Informationen über Drittstaatsangehörige und das Europäische Strafregisterinformationssystem (ECRIS) und zur Ersetzung des Beschlusses 2009/316/JI des Rates („Vorschlag“)¹. Vor der Veröffentlichung des Vorschlags war der EDSB informell konsultiert worden. Der EDSB bedauert allerdings, dass er nach der Veröffentlichung des Vorschlags nicht um eine Stellungnahme ersucht wurde.

1.2 Ziel des Vorschlags

2. ECRIS ist ein elektronisches System für den Austausch von Informationen über frühere Verurteilungen einer bestimmten Person durch Strafgerichte in der EU für die Zwecke eines Strafverfahrens gegen diese Person und, sofern dies nach nationalem Recht zulässig ist, für andere Zwecke. Das System basiert auf dem Rahmenbeschluss 2009/315/JI des Rates („Rahmenbeschluss“) und dem Beschluss 2009/316/JI des Rates².

¹ COM(2016) 7 final, 2016/0002 (COD), Straßburg, 19. Januar 2016.

² Rahmenbeschluss 2009/315/JI des Rates vom 26. Februar 2009 über die Durchführung und den Inhalt des Austauschs von Informationen aus dem Strafregister zwischen den Mitgliedstaaten, ABl. L 93 vom 7.4.2009, S. 23, und Beschluss 2009/316/JI des Rates vom 6. April 2009 zur Einrichtung des Europäischen Strafregisterinformationssystems (ECRIS) gemäß Artikel 11 des Rahmenbeschlusses 2009/315/JI, ABl. L 93 vom 7.4.2009, S. 33.

3. In der Begründung des Vorschlags heißt es, dem ECRIS liege das Prinzip zugrunde, dass vollständige Informationen über frühere Verurteilungen eines EU-Bürgers vom Herkunftsmitgliedstaat bezogen werden können, und dieser könne umfassende aktuelle Auskünfte über Vorstrafen seiner Staatsangehörigen erteilen, unabhängig davon, wo in der EU die Verurteilungen ergangen seien. Diese Struktur erschwert derzeit den Behörden den Austausch von Informationen über Verurteilungen von Drittstaatsangehörigen und Staatenlosen mit Hilfe von ECRIS, da „Drittstaatsangehörige keinen Herkunftsmitgliedstaat haben“, und um einen vollständigen Überblick über die Vorstrafen einer bestimmten Person zu erhalten, müssen Auskunftersuchen an alle Urteilsmitgliedstaaten gesendet werden³.

4. Ziel des Vorschlags ist daher, die Effizienz von ECRIS beim Austausch von Strafregisterinformationen von Drittstaatsangehörigen zu verbessern.

5. In der Begründung wird das System beschrieben, mit dem dieses Ziel erreicht werden soll. Das System wird dezentral organisiert werden, d. h., es wird keine einheitliche EU-Datenbank mit den einschlägigen Informationen geben; vielmehr wird jeder Mitgliedstaat seine eigene Datei unterhalten. Die Mitgliedstaaten müssen bei der Verurteilung eines Drittstaatsangehörigen Identitätsdaten aus ihrem Strafregister aussondern und in eine separate Datei eingeben, den „Indexfilter“. Die Daten werden verschlüsselt. Der Indexfilter wird allen Mitgliedstaaten übermittelt, so dass sie die Suche unabhängig in ihren eigenen Räumlichkeiten durchführen können. Das System erlaubt es den Mitgliedstaaten, diese Daten mit ihren eigenen Daten abzugleichen und zu ermitteln, ob es weitere Einträge in Strafregistern anderer Mitgliedstaaten gibt (ein System mit Abgleich auf Treffer).

II. DATENSCHUTZIMPLIKATIONEN

6. Der EDSB begrüßt, dass in Erwägungsgrund 12 des Vorschlags der Rahmenbeschluss 2008/977/JI⁴ des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, und seine Anwendung auf den elektronischen Austausch von Strafregisterinformationen erwähnt werden, wodurch für ein angemessenes Datenschutzniveau beim Austausch von Informationen zwischen Mitgliedstaaten gesorgt ist, wobei es den Mitgliedstaaten erlaubt ist, höhere Schutzstandards bei der nationalen Datenverarbeitung vorzusehen. Des Weiteren hält der EDSB fest, dass auch die vorgeschlagene Datenschutzrichtlinie für Polizei und Justiz⁵ nach ihrem Inkrafttreten in vollem Umfang auf die im Vorschlag vorgesehene Verarbeitung personenbezogener Daten Anwendung finden soll. **Der EDSB empfiehlt daher, in die Präambel des Vorschlags einen Verweis auf die Datenschutzrichtlinie für Polizei und Justiz aufzunehmen und die Beziehung zwischen den beiden Rechtsakten klarzustellen.**

7. Die im Vorschlag geplanten Maßnahmen sehen die Verarbeitung personenbezogener Daten vor und sind somit ein Eingriff in das Grundrecht auf Privatleben, wie es in Artikel 7

³ Begründung des Vorschlags, S. 3.

⁴ Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, ABl. L 350 vom 30.12.2008, S. 60.

⁵ Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr, in der am 18. Dezember 2015 vom Rat vereinbarten Fassung.

der Charta der Grundrechte der Europäischen Union („EU-Charta“) verankert ist, und in das Recht auf Schutz personenbezogener Daten, garantiert in Artikel 8 der EU-Charta⁶. In diesem Sinne begrüßt der EDSB, dass in der Begründung des Vorschlags auf die Rechtsprechung des Gerichtshofs der Europäischen Union zur Anwendung der Artikel 7 und 8 der EU-Charta auf den Zugriff von Behörden auf personenbezogene Daten für Zwecke der Strafverfolgung und insbesondere in der Rechtssache *Digital Rights Ireland* („DRI“) verwiesen wird.

8. Artikel 52 Absatz 1 der Charta besagt: „Jede Einschränkung der Ausübung der in dieser Charta anerkannten Rechte und Freiheiten muss gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten achten. Unter Wahrung des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen nur vorgenommen werden, wenn sie erforderlich sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen“⁷.

9. Die Terrorismusbekämpfung und die Bekämpfung schwerer Kriminalität zur Gewährleistung der öffentlichen Sicherheit gelten im EU-Recht als eine dem Gemeinwohl dienende Zielsetzung⁸. In der Präambel des Vorschlags heißt es: „Der Austausch von Informationen über strafrechtliche Verurteilungen ist wichtig für jede Strategie zur Bekämpfung von Kriminalität und Terrorismus“ (Erwägungsgrund 7). Die vorgeschlagenen Maßnahmen dienen somit einem dem Gemeinwohl dienenden Ziel und lassen sich vorbehaltlich der Wahrung des Grundsatzes der Verhältnismäßigkeit rechtfertigen. Gegenstand der nachstehenden Analyse sind mehrere Aspekte der Verhältnismäßigkeit der vorgeschlagenen Maßnahmen; darüber hinaus wird auf die Notwendigkeit eingegangen, den sachlichen Anwendungsbereich des Vorschlags bezüglich der Art der Datenverarbeitung besser festzulegen (Anonymisierung/Pseudonymisierung).

II.1 Sachlicher Anwendungsbereich der vorgeschlagenen Maßnahme

A. Verarbeitung von Fingerabdrücken

10. Der Vorschlag sieht einerseits in Artikel 1 Absatz 4 vor, dass die Mitgliedstaaten unbedingt verpflichtet sind, die Fingerabdrücke verurteilter Drittstaatsangehöriger zu speichern (es sei denn, die Fingerabdrücke können aus sachlichen Gründen nicht abgenommen werden⁹). Darüber hinaus müssen Fingerabdrücke verurteilter Drittstaatsangehöriger *im Indexfilter* gespeichert werden. Andererseits müssen Mitgliedstaaten die Fingerabdrücke verurteilter EU-Bürger nur speichern, wenn sie den Zentralbehörden zur Verfügung stehen (Artikel 11 Absatz 1 Buchstabe c Ziffer ii des Rahmenbeschlusses). Man geht also davon aus, dass die Fingerabdrücke von EU-Bürgern je nach den nationalen Rechtsvorschriften der Zentralbehörde zur Verfügung stehen oder auch nicht.

⁶ EuGH, C-293/12 und C-594/12 *Digital Rights Ireland*, 8. April 2014, Rdnrn. 33 und 36.

⁷ Siehe ferner *Digital Rights Ireland*, Rdnr. 38.

⁸ EuGH, Rechtssachen C-402/05 P und C-415/05 P *Kadi und Al Barakaat International Foundation / Rat und Kommission* EU:C:2008:461, Rdnr. 383; Rechtssachen C-539/10 P und C-550/10 P *Al-Aqsa / Rat* EU:C:2012:711, Rdnr. 130; Rechtssache C-145/09 *Tsakouridis* EU:C:2010:708, Rdnrn. 46 und 47.

⁹ Formuliert wird diese Ausnahme in Artikel 4a Absatz 1 folgendermaßen: „... es sei denn, dass dies in einzelnen Ausnahmefällen nicht möglich ist“.

11. Die vorgeschlagene obligatorische Erhebung, Speicherung und Nutzung von Fingerabdrücken für das ECRIS für Drittstaatsangehörige ist ein Eingriff im Sinne sowohl von Artikel 7 als auch von Artikel 8 der Charta. In diesem Sinne befand der Gerichtshof der Europäischen Union (EuGH) in seinem Urteil in der Rechtssache *Schwarz*, dass „die Erfassung und die Speicherung von Fingerabdrücken durch die nationalen Behörden (...) einen Eingriff in die Rechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten darstellen“¹⁰. Zwar dienen die Nutzung und die Speicherung von Fingerabdrücken für das ECRIS für Drittstaatsangehörige durchaus einem legitimen Interesse, wie es in Artikel 52 Absatz 1 der Charta verlangt wird, und hier vor allem dem Kampf gegen Terrorismus und der Bekämpfung schwerer Kriminalität zur Gewährleistung der öffentlichen Sicherheit, doch ist die Frage zu prüfen, ob diese Maßnahme erforderlich und verhältnismäßig ist.

12. Einleitend sei darauf hingewiesen, dass „die Bedingungen, unter denen Mitgliedstaaten Fingerabdrücke im Verlauf strafrechtlicher Ermittlungen und Verfahren speichern, im EU-Recht nicht harmonisiert sind“¹¹. In der Praxis bedeutet dies, dass es in den Mitgliedstaaten derzeit je nach Schwere der Straftatbestände unterschiedliche Vorschriften für die Speicherung von Fingerabdrücken für Strafverfolgungszwecke gibt. Ein Faktor, der bei der Beurteilung der Notwendigkeit der obligatorischen Verwendung von Fingerabdrücken zu berücksichtigen ist, ist die Tatsache, dass jeder Mitgliedstaat seine ureigenste Strafrechtspolitik mit verschiedenen Schwellen für die Schwere der Straftaten betreibt, die die Speicherung von Fingerabdrücken verurteilter Personen in ihren eigenen justiziellen Datenbanken verlangen¹². Folglich kann es dazu kommen, dass ein Mitgliedstaat im Einklang mit dem Vorschlag dazu verpflichtet ist, die Fingerabdrücke einer Person wegen eines minder schweren Vergehens abzunehmen und zu speichern (was einen Eingriff in das Recht einer Person auf Privatleben darstellt), während es nach dem innerstaatlichen Recht nicht erforderlich ist, die Fingerabdrücke im Zusammenhang mit Vorstrafen dieser Person zu speichern.

13. Die Verpflichtung zur Speicherung der Fingerabdrücke verurteilter Drittstaatsangehöriger im Indexfilter wird vom Gesetzgeber mit der Notwendigkeit einer „sicheren Identifizierung“ begründet¹³, weil „nur über Fingerabdrücke (...) die Identität einer Person sicher festgestellt werden [kann]“¹⁴. Die Verwendung von Fingerabdrücken gerade zur Identifizierung von Drittstaatsangehörigen erbringt eindeutig einen Mehrwert, denn es ist durchaus denkbar, dass es Drittstaatsangehörige gibt, die keine Identifizierungsdokumente haben oder deren Namen in einem Alphabet geschrieben sind, das in den Amtssprachen der Union nicht verwendet wird, und somit Raum für Identifizierungsfehler entsteht.

14. In der Begründung heißt es jedoch, dass die Zentralbehörden zahlreicher Mitgliedstaaten derzeit Fingerabdrücke nicht in ihren nationalen Strafregistern speichern und nicht an das

¹⁰ Siehe hierzu EuGH, C-291/12 *Schwartz gegen Stadt Bochum*, 17. Oktober 2013, Rdnr. 30.

¹¹ Folgenabschätzung, S. 15.

¹² Es gilt, was die Kommission in einer ihrer Mitteilungen einräumte: „Das Strafrecht ist ein sensibler politischer Bereich, in dem zwischen den einzelstaatlichen Systemen weiterhin bedeutende Unterschiede - beispielsweise in Bezug auf Straftaten und Strafmaß sowie die Klassifizierung bestimmter Verhaltensweisen als Ordnungswidrigkeit oder als Straftat - herrschen“; Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, „*Auf dem Weg zu einer europäischen Strafrechtspolitik: Gewährleistung der wirksamen Durchführung der EU-Politik durch das Strafrecht*“, KOM(2011) 573 endgültig, 20. September 2011, S. 2.

¹³ Erwägungsgrund 10 der Präambel.

¹⁴ Begründung, S. 6.

nationale automatisierte Fingerabdruck-Identifizierungssystem (AFIS) angeschlossen sind¹⁵. Einige Mitgliedstaaten äußerten ferner „verfassungsrechtliche Bedenken“¹⁶ aufgrund der Verpflichtung zur Speicherung der Fingerabdrücke aller verurteilten Drittstaatsangehörigen, und zwar unabhängig von der Art des begangenen Vergehens oder der begangenen Straftat.

15. Man kann also nicht davon ausgehen, dass es keine andere Möglichkeit der sicheren Identifizierung der Personen gibt als die Verwendung von Fingerabdrücken, weshalb die Notwendigkeit einer obligatorischen Verwendung von Fingerabdrücken bei Drittstaatsangehörigen im ECRIS noch nachzuweisen wäre.

16. In Anbetracht all dessen scheint es weder erforderlich noch verhältnismäßig zu sein, alle Mitgliedstaaten zur Speicherung der Fingerabdrücke von Drittstaatsangehörigen zu verpflichten, und dies unabhängig von den Sanktionsschwellen und der Art von Straftaten in ihren eigenen nationalen Systemen. **Der EDSB empfiehlt dem Gesetzgeber, bezüglich der Verarbeitung von Fingerabdrücken eine der bestehenden Regelung für EU-Bürger entsprechende Regelung für Drittstaatsangehörige zu schaffen, und zwar durch Ausdehnung des in Artikel 11 des derzeitigen Rahmenbeschlusses 2009/315/JI festgelegten persönlichen Geltungsbereichs auf Drittstaatsangehörige. Auf diese Weise wäre die Speicherung von Fingerabdrücken auf nationaler Ebene je nach den Verfassungssystemen der Mitgliedstaaten fakultativ, jedoch würde die Verpflichtung bestehen bleiben, auf nationaler Ebene gespeicherte Fingerabdrücke von Drittstaatsangehörigen in den Indexfilter einzugeben.**

17. In früheren Stellungnahmen zu Datenbanken mit biometrischen Daten hat der EDSB unterstrichen, dass „der sensible Charakter, der den biometrischen Daten inhärent ist, spezielle Schutzgarantien [erfordert]“¹⁷, wie beispielsweise eine gezielte Folgenabschätzung der Nutzung biometrischer Daten, eine verstärkte Beachtung des Erfassungsverfahrens (Methode der Erfassung), die besondere Betonung des Genauigkeitsgrads und die Einrichtung eines Ausweichverfahrens, um die Würde der Personen, die irrtümlicherweise identifiziert worden sein könnten, zu wahren und zu vermeiden, dass sie unter den Mängeln des Systems zu leiden haben¹⁸.

18. Bei der hier zu prüfenden Maßnahme enthält die Folgenabschätzung zum Vorschlag eigene Abschnitte mit einer Analyse der Nutzung von Fingerabdrücken, wobei mehrere Optionen durchgespielt werden, also zentrale/dezentrale Speicherung, obligatorische/fakultative Nutzung. Des Weiteren enthält der Vorschlag für einen Rechtsakt spezifische Garantien, die dem sensiblen Charakter biometrischer Daten Rechnung tragen. Sowohl der Mechanismus zur Pseudonymisierung von Daten im Indexfilter als auch die Einführung eines dezentralen EU-Systems zum Abgleich auf Treffer sind willkommene Garantien bezüglich der Verarbeitung von Fingerabdrücken in der Datei. Darüber hinaus **empfiehlt der EDSB, in den später von der Kommission vorzuschlagenden Durchführungsrechtsakten weitere Schutzgarantien für das Erfassungsverfahren, die Betonung des Genauigkeitsgrads und die Einführung eines Ausweichverfahrens vorzusehen.**

¹⁵ Begründung, S. 6.

¹⁶ Begründung, S. 6.

¹⁷ Stellungnahme vom 19. Oktober 2005 zu drei Vorschlägen betreffend das Schengener Informationssystem der zweiten Generation (SIS II) (KOM(2005) 230 endgültig, KOM(2005) 236 endgültig und KOM(2005) 237 endgültig), ABl. C 91 vom 19.4.2006, S. 43.

¹⁸ Stellungnahme des EDSB zu SIS II, 2005, S. 44.

B. Anonymisierung/Pseudonymisierung

19. Im Vorschlag wird ein „anonymer“ Indexfilter erwähnt, mit dessen Hilfe Mitgliedstaaten überprüfen können, ob andere Mitgliedstaaten im Besitz von Informationen über einen bestimmten Drittstaatsangehörigen sind. Gestützt auf die ihm vorliegenden Informationen ist der EDSB zu der Auffassung gelangt, dass die Informationen wegen der Natur des Systems nicht als „anonym“ bezeichnet werden können, denn es erlaubt die Identifizierung von Personen, die in einem anderen Mitgliedstaat vorbestraft sind. Um die Frage beantworten zu können, ob in dem Vorschlag die korrekten Begriffe verwendet werden, sei hier noch einmal auf die einschlägigen Begriffsbestimmungen hingewiesen:

- „Personenbezogene Daten“ sind in der EU-Rechtsordnung definiert als alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann¹⁹. Der Begriff deckt also auch die indirekte Identifizierung ab, z. B. durch Zuordnung einer Kennnummer;
- „Pseudonymisierte Daten“ werden in der Datenschutzrichtlinie für Polizei und Justiz definiert als personenbezogene Daten, die ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden²⁰. Pseudonymisierte Daten sind nach wie vor personenbezogene Daten und unterliegen als solche dem Datenschutzrecht;
- „Anonymisieren“ ist in Artikel 2 Buchstabe k des Rahmenbeschlusses 2008/977/JI des Rates definiert als „das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbar natürlichen Person zugeordnet werden können“. Die Artikel 29-Datenschutzgruppe befand Folgendes: „„Anonymisierte Daten“ sind somit anonyme Daten, die sich zuvor auf eine bestimmbar Person bezogen, die jedoch nicht mehr identifizierbar ist“²¹. Da sich „anonyme Daten“ nicht auf bestimmte oder bestimmbar natürliche Personen beziehen, fallen sie nicht in den Anwendungsbereich des Datenschutzrechts.

Der Wortlaut des Vorschlags ist vor dem Hintergrund dieser etablierten Definitionen zu bewerten.

20. Neben dem eigentlichen Informationsaustausch erlaubt der Vorschlag zwei unterschiedliche Verarbeitungen von personenbezogenen Daten von Drittstaatsangehörigen. Bei der ersten Verarbeitung handelt es sich um die „Speicherung“ von elf personenbezogenen Angaben²², darunter der Fingerabdrücke der Person, in dem Mitgliedstaat, „in dem eine

¹⁹ Artikel 3 Absatz 1 der Datenschutzrichtlinie für Polizei und Justiz.

²⁰ Artikel 3 Absatz 4a der Datenschutzrichtlinie für Polizei und Justiz.

²¹ Siehe hierzu die Schlussfolgerung der Artikel 29-Datenschutzgruppe in der Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“, wo es heißt: „„Anonymisierte Daten“ sind somit anonyme Daten, die sich zuvor auf eine bestimmbar Person bezogen, die jedoch nicht mehr identifizierbar ist“ (S. 24). Siehe ferner „Zusätzliche Anmerkungen des EDSB zum Datenschutzreformpaket“, S. 1 bis 3, veröffentlicht am 13. März 2013.

²² Artikel 4a Absatz 1: a) Informationen zu der Person, gegen die die Verurteilung ergangen ist (vollständiger Name, Geburtsdatum, Geburtsort (Stadt und Staat), Geschlecht, Staatsangehörigkeit und - gegebenenfalls - frühere/e Name/n); b) Informationen zur Art der Verurteilung (Datum der Verurteilung, Bezeichnung des

Verurteilung gegen einen Drittstaatsangehörigen ergeht (...), es sei denn, dass dies in einzelnen Ausnahmefällen nicht möglich ist“²³.

21. Gegenstand der zweiten Verarbeitung personenbezogener Daten ist die Einrichtung und Nutzung des Indexfilters. Artikel 1 Absatz 4 des Vorschlags, mit dem ein *Artikel 4a Absatz 2* in die ECRIS-Richtlinie eingefügt wird, besagt: „Die Zentralbehörde erstellt (...) einen Indexfilter mit *anonymisierten Informationen*“ (Hervorhebung durch uns), der fünf der von Mitgliedstaaten gespeicherten Angaben²⁴ enthalten muss, darunter Fingerabdrücke. In der Begründung heißt es hingegen, der oben beschriebene Indexfilter „*wird (...) keine personenbezogenen Daten enthalten*“²⁵, da die im Indexfilter gespeicherten Informationen *anonymisiert* werden²⁶. Weiter heißt es in der Präambel des Vorschlags: „Die personenbezogenen Daten *sollten so anonymisiert werden*, dass der Betroffene *nicht identifiziert werden kann*“²⁷ (Hervorhebung durch uns).

22. Damit liegt klar auf der Hand, dass der eigentliche Zweck des Filterindex mit Fingerabdrücken die genaue Identifizierung von Drittstaatsangehörigen mit Vorstrafen in anderen Mitgliedstaaten ist, und zwar durch Identifizierung dieser Mitgliedstaaten und anschließende Anforderung aller verfügbaren Informationen über den betreffenden Drittstaatsangehörigen, um den es in der Abfrage geht. Da nach den etablierten Begriffsbestimmungen alle Informationen über eine bestimmte oder bestimmbare natürliche Person personenbezogene Daten sind, gehören zu ihnen auch die Informationen im Indexfilter. In der Begründung des Vorschlags heißt es: „Zur wirksamen Identifizierung von Drittstaatsangehörigen sollten Fingerabdrücke in die im Strafregister der betreffenden Person und im Indexfilter zu speichernden Identifikationsdaten aufgenommen werden“²⁸.

23. Auch wenn das Verfahren für die Eingabe von Daten in den Indexfilter als „unwiderruflich“²⁹ bezeichnet wird, bleibt doch ganz ohne Zweifel die Tatsache, dass der Zweck der Verarbeitung von Daten im Indexfilter durch einen Abgleich auf Treffer in der Identifizierung bestimmter Drittstaatsangehöriger besteht, die in anderen Mitgliedstaaten vorbestraft sind. Das Ergebnis des Abgleichs auf Treffer führt zusammen mit den für die Suche im Indexfilter verwendeten Identitätsdaten zur Identifizierung natürlicher Personen und zu weiteren Informationen über sie (z. B. ob sie in einem oder mehreren anderen Mitgliedstaaten vorbestraft sind).

24. Die im Indexfilter verarbeiteten Daten können daher nicht als „anonym“ bezeichnet werden. Angebrachter wäre die Bezeichnung „pseudonymisiert“; damit sind

Gerichts, Datum, an dem die Entscheidung rechtskräftig wurde); c) Informationen über die der Verurteilung zugrunde liegende Straftat (Datum der dem Urteil zugrunde liegenden Straftat und Bezeichnung oder rechtliche Qualifikation der Straftat sowie Bezugnahme auf die anwendbaren gesetzlichen Vorschriften); d) Informationen zum Inhalt der Verurteilung, insbesondere Hauptstrafe und etwaige zusätzliche Strafen, Maßnahmen der Besserung und Sicherung sowie Folgeentscheidungen, die die Vollstreckung der Strafe abändern; e) Namen der Eltern der verurteilten Person; f) Aktenzeichen des Urteils; g) Ort der Tatbegehung; h) gegebenenfalls Rechtsverluste, die sich aus der Verurteilung ergeben; i) Identitätsnummer der verurteilten Person oder Art und Nummer des Identitätsdokuments der Person; j) Fingerabdrücke der Person; k) gegebenenfalls Pseudonym und/oder Aliasname(n).

²³ Artikel 1 Absatz 4 (neu Artikel 4a Absatz 1) des Rahmenbeschlusses).

²⁴ Buchstaben a, e, i, j und k der Auflistung in Fußnote 22.

²⁵ Begründung des Vorschlags, S. 5.

²⁶ Erwägungsgrund 11 der Präambel des Vorschlags.

²⁷ Erwägungsgrund 11 der Präambel des Vorschlags.

²⁸ Begründung, S. 9.

²⁹ Begründung, S. 5.

personenbezogene Daten gemeint, die dem weiter oben unter Punkt 9 beschriebenen Verfahren der Pseudonymisierung unterzogen wurden.

25. Einerseits begrüßen wir die geplante Technik³⁰, mit der die Daten im Indexfilter verschlüsselt werden, denn dies ist eine geeignete Garantie zur Beschränkung von Eingriffen in das Privatleben und das Recht auf Schutz personenbezogener Daten der betreffenden Personen³¹, andererseits weisen wir darauf hin, dass das Datenschutzrecht auch für die Daten im Indexfilter gilt. Wir empfehlen daher, im Sinne von Klarheit und Rechtssicherheit den Wortlaut der Vorschlags an den Wortlaut der Datenschutzrichtlinie für Polizei und Justiz³² insofern anzugleichen, als **im Vorschlag nicht länger von anonymen Daten gesprochen werden, sondern korrekterweise vom Verfahren der Pseudonymisierung die Rede sein sollte.**

C. Kategorien von zu verarbeitenden personenbezogenen Daten

26. In Artikel 1 Absatz 4 des Vorschlags zur Einfügung eines neuen Artikels 4a Absatz 1 in die ECRIS-Richtlinie sind konkret die Daten aufgelistet, die von der Zentralbehörde eines Mitgliedstaats im Fall einer Verurteilung eines Drittstaatsangehörigen zu speichern sind. Eine ähnliche Liste findet sich in Artikel 11 des derzeitigen Rahmenbeschlusses für EU-Bürger, die verurteilt wurden. Artikel 11 des Rahmenbeschlusses sieht allerdings einen geringeren Eingriff in das Privatleben von EU-Bürgern vor als der neue Artikel 4a. Er unterscheidet zwischen drei verschiedenen Kategorien von Daten, die für ECRIS-Zwecke verarbeitet werden, nämlich Daten, die übermittelt werden müssen, Daten, die übermittelt werden können (z. B. Namen der Eltern der verurteilten Person), und zusätzliche Informationen. Diese Unterscheidung wird bei Daten von Drittstaatsangehörigen, die für ECRIS-Zwecke verarbeitet werden sollen, nicht gemacht.

27. Ein Vergleich der beiden Listen macht deutlich, dass Angaben wie „Namen der Eltern der verurteilten Person“, „Aktenzeichen des Urteils“ und „Ort der Tatbegehung“, deren Übermittlung bei EU-Bürgern fakultativ ist, bei Drittstaatsangehörigen übermittelt werden müssen. Die Existenz zweier Artikel in der vorgeschlagenen Richtlinie, in denen die auszutauschenden Informationen aufgeführt sind, einmal für EU-Bürger und einmal für Drittstaatsangehörige, dürfte kaum gerechtfertigt sein. Über Drittstaatsangehörige werden zusätzliche Informationen verlangt, deren Übermittlung bei EU-Bürgern lediglich fakultativ ist. Diese Unterscheidung wäre nur dann gerechtfertigt, wenn sie sich auf starke und präzise rechtliche Argumente stützt, an denen es jedoch offenbar mangelt. Der EDSB empfiehlt, den persönlichen Anwendungsbereich von Artikel 11 („Format und sonstige Modalitäten für die Durchführung und Erleichterung des Informationsaustauschs über Verurteilungen“) des Rahmenbeschlusses 2009/315/JI auf Drittstaatsangehörige auszuweiten, anstatt in die Richtlinie einen weiteren Artikel einzufügen, in dem die nur bei Drittstaatsangehörigen zu verarbeitenden Daten aufgeführt sind.

³⁰ Anscheinend hat die Europäische Kommission bereits eine technische Lösung für die Umsetzung des ECRIS für Drittstaatsangehörige geplant und der Wortlaut des Vorschlags wurde so verfasst, dass er zu dieser technischen Lösung passt. Eigentlich sollten zunächst die Anforderungen an eine technische Lösung festgelegt und erst dann sollte eine Lösung erarbeitet werden, die diesen Anforderungen gerecht wird.

³¹ Im Vergleich zu einer vollständig zentralen Indexdatei.

³² Die Datenschutzrichtlinie für Polizei und Justiz steht kurz vor ihrer Annahme. Am 18. Dezember 2015 bestätigte der Ausschuss der ständigen Vertreter (AStV) den mit dem Europäischen Parlament ausgehandelten Kompromisswortlaut für die Datenschutzreform. Die Einigung zwischen Rat, Parlament und Kommission wurde am 15. Dezember erzielt. Die offizielle Annahme wird für die erste Jahreshälfte 2016 erwartet.

II.2 Persönlicher Geltungsbereich der Maßnahme

28. Der Vorschlag unterscheidet in zweierlei Hinsicht beim persönlichen Geltungsbereich der vorgeschlagenen Maßnahme, nämlich einmal zwischen EU-Bürgern und Drittstaatsangehörigen, und einmal zwischen EU-Bürgern, die nur die Staatsangehörigkeit eines EU-Mitgliedstaats haben, und EU-Bürgern, die auch die Staatsangehörigkeit eines Drittlandes besitzen. Die beiden Unterscheidungen dürften ein Ergebnis der Einrichtung des Indexfilters sein, der Daten von Drittstaatsangehörigen enthält, darunter EU-Bürger, die auch die Staatsangehörigkeit eines Drittlandes besitzen. Hierzu besagt Artikel 1 Absatz 4 des Vorschlags (*neuer Artikel 4a Absatz 4* der künftigen ECRIS-Richtlinie), dass die Einrichtung des Indexfilters „*auch im Zusammenhang mit Drittstaatsangehörigen [gilt], die die Staatsangehörigkeit eines Mitgliedstaats besitzen*“. Diese Unterscheidung wird auch im neuen Artikel 4b Absatz 2 über die „Verwendung des Indexfilters“ gemacht.

29. Der EDSB erinnert daran, dass gemäß Artikel 8 Absatz 2 der Charta die Verarbeitung personenbezogener Daten nach Treu und Glauben erfolgen muss. Wie außerdem bereits ausgeführt, stellt die Verarbeitung personenbezogener Daten einen Eingriff in das Recht auf Schutz personenbezogener Daten dar³³ und enthält Artikel 52 Absatz 1 der Charta die Forderung, dass jede Einschränkung der Rechte in Artikel 8 erforderlich und verhältnismäßig sein muss.

30. Die Unterscheidung zwischen Drittstaatsangehörigen und EU-Bürgern bezüglich der verschiedenen Arten der Verarbeitung ihrer personenbezogenen Daten scheint erforderlich zu sein, weil sie durch objektive Faktoren im Zusammenhang mit dem Zweck der vorgeschlagenen Maßnahme gerechtfertigt ist, wie in Absatz 3 dieser Stellungnahme dargestellt ist. So ist insbesondere die Einrichtung der Indexdatei für Drittstaatsangehörige durch die Tatsache gerechtfertigt, dass Drittstaatsangehörige nicht die Staatsangehörigkeit eines Mitgliedstaats besitzen, so dass das normale ECRIS-Verfahren für den Informationsaustausch auf sie nicht angewandt werden kann³⁴.

31. Mit Blick auf die Unterscheidung zwischen EU-Bürgern, die nur EU-Bürger sind, und EU-Bürgern, die auch Bürger eines Drittlandes sind, wird die Notwendigkeit der Maßnahmen nicht nachgewiesen. Ist ein bestimmter Verarbeitungsvorgang - wie die Verarbeitung von Daten im Indexfilter - für EU-Bürger nicht erforderlich ist, dann ist sie auch für EU-Bürger nicht erforderlich, die gleichzeitig Bürger eines Drittlandes sind.

32. In der Rechtssache *Huber* befand der Gerichtshof, dass der frühere Artikel 12 Absatz 1 EGV über das Recht auf Nichtdiskriminierung aufgrund der Staatsangehörigkeit innerhalb der EU (derzeit Artikel 18 Absatz 1 AEUV) dahin auszulegen ist, „dass er es einem Mitgliedstaat verwehrt, zur Bekämpfung der Kriminalität ein System zur Verarbeitung personenbezogener Daten zu errichten, das nur Unionsbürger erfasst, die keine Staatsangehörigen dieses Mitgliedstaats sind“³⁵. Der Gerichtshof verwies darauf, „dass vergleichbare Sachverhalte nicht ungleich und ungleiche Sachverhalte nicht gleichbehandelt werden dürfen. *Eine solche Behandlung wäre allenfalls dann gerechtfertigt, wenn sie auf objektiven, von der Staatsangehörigkeit der Betroffenen unabhängigen Erwägungen beruhte*

³³ Siehe hierzu weiter oben Absatz 7 und die dortigen Ausführungen.

³⁴ Begründung, S. 3.

³⁵ C-524/06 *Heinz Huber gegen Deutschland*, 16. Dezember 2008, Rdnr. 81.

*und in einem angemessenen Verhältnis zu einem legitimerweise verfolgten Zweck stünde*³⁶
(Hervorhebung durch uns).

33. Die im Vorschlag vorgesehene unterschiedliche Behandlung dürfte für das Erreichen des verfolgten Zwecks nicht erforderlich sein, wenn man berücksichtigt, dass im Falle von EU-Bürgern die bestehenden ECRIS-Verfahren angewandt werden können, damit Behörden Informationen austauschen können. In der Begründung des Vorschlags wird keinerlei Grund genannt, aus dem eine solche Unterscheidung erforderlich wäre. Diese Ungleichbehandlung kann zu Diskriminierung führen, die wiederum ein Verstoß gegen Artikel 21 Absatz 1 der EU-Charta wäre. Dieser Artikel verbietet im Anwendungsbereich des EUV jegliche Diskriminierung, die sich im Einklang mit Artikel 52 Absatz 1 der Charta nicht rechtfertigen lässt.

34. Schließlich verfolgt das Datenschutzrecht in allen Bereichen (Handels- oder Strafsachen) das Ziel, „einen hohen Schutz der Grundrechte und Grundfreiheiten natürlicher Personen (...) bei der Verarbeitung personenbezogener Daten (...) zu gewährleisten“³⁷, darunter das Recht auf Nichtdiskriminierung. Daher würde eine Situation, in der die Verarbeitung personenbezogener Daten gegen die Grundrechte der Personen verstoßen würde, deren Daten verarbeitet werden, wie das in Artikel 21 der EU-Charta verankerte Recht auf Nichtdiskriminierung, nicht im Einklang mit dem EU-Datenschutzrecht stehen.

35. Der EDSB empfiehlt daher, im Indexfilter nur Informationen über Drittstaatsangehörige zu speichern, nicht jedoch über EU-Bürger, die auch die Staatsangehörigkeit eines Drittlandes besitzen.

II.3 Qualität der Daten

36. Der EDSB begrüßt die Bestimmung in Artikel 4a Absatz 3 des Vorschlags über eine automatische Aktualisierung der im Indexfilter enthaltenen personenbezogenen Daten nach jeder Änderung oder Streichung von Informationen; dies entspricht weitgehend der in Artikel 4 Absatz 3 des derzeitigen Rahmenbeschlusses 2009/315/JI des Rates verankerten Verpflichtung bezüglich Eintragungen im Strafregister von EU-Bürgern. Bei einem Informationsaustausch in Strafsachen kommt der sachlichen Richtigkeit von Daten besondere Bedeutung zu, denn hier kann eine Person Gegenstand von Entscheidungen sein, die als Folge der Verarbeitung von Daten rechtliche Wirkung oder nachteilige Auswirkungen haben.

III. SCHLUSSFOLGERUNG

37. Schon in seiner Stellungnahme aus dem Jahr 2006 zum ECRIS-Vorschlag stellte der EDSB fest: „Für Drittstaatsangehörige könnte ein alternatives System erforderlich sein“, da „aus ersichtlichen Gründen (...) das vorgeschlagene System in diesen Fällen nicht funktionieren [kann]“³⁸. Daher begrüßen wir den vorliegenden Vorschlag und räumen ein, dass einem effizienten Austausch von Informationen über Strafregistereinträge verurteilter

³⁶ C-524/06 *Huber*, Rdnr. 75.

³⁷ Siehe Artikel 1 Absatz 1 des Rahmenbeschlusses 2008/977/JI des Rates und Artikel 1 Absatz 1 der Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281 vom 23.11.1995, S. 31.

³⁸ Stellungnahme des EDSB zu dem Vorschlag für einen Rahmenbeschluss des Rates über die Durchführung und den Inhalt des Austauschs von Informationen aus den Strafregistern zwischen den Mitgliedstaaten (KOM(2005) 690 endg.), ABl. C 313 vom 20.12.2006, S. 26, Punkte 15 und 18.

Personen große Bedeutung zukommt, insbesondere vor dem Hintergrund der Annahme der Sicherheitsagenda der EU³⁹.

38. Nach sorgfältiger Prüfung des Vorschlags spricht der EDSB folgende Empfehlungen aus, damit der Vorschlag im Einklang mit dem EU-Datenschutzrecht steht:

- 1) Bezüglich der obligatorischen Nutzung von Fingerabdrücken bei Drittstaatsangehörigen **sollte für Drittstaatsangehörige eine entsprechende Regelung gefunden werden, wie es sie bereits für EU-Bürger gibt**, und dies im Einklang mit den auf nationaler Ebene bestehenden Vorschriften für die Abnahme von Fingerabdrücken;
- 2) Erwähnungen anonymer Daten sollten aus dem Vorschlag gestrichen und durch **sachlich richtige Hinweise auf das Verfahren der Pseudonymisierung** ersetzt werden;
- 3) die **auf nationaler Ebene zu speichernden Daten über verurteilte EU-Bürger und verurteilte Drittstaatsangehörige sollten nicht verschiedenen Kategorien zugeordnet werden**, beispielsweise durch Ausweitung der geltenden Regelung für EU-Bürger (z. B. „fakultative Daten“, „zusätzliche Daten“) auch auf Drittstaatsangehörige;
- 4) **die Nutzung des Indexfiltersystems sollte allein auf personenbezogene Daten von Drittstaatsangehörigen beschränkt werden**, eine Personenkategorie, die EU-Bürger, die auch die Staatsangehörigkeit eines Drittlandes besitzen, nicht umfassen sollte.

39. Darüber hinaus spricht der EDSB folgende Empfehlungen aus, die den Schutz der für Zwecke des ECRIS für Drittstaatsangehörige verarbeiteten personenbezogenen Daten noch verbessern würden:

- 1) In die Präambel des Vorschlags sollte ein **Verweis auf die Datenschutzrichtlinie für Polizei und Justiz** aufgenommen und die Beziehung zwischen den beiden Rechtsakten klargestellt werden.
- 2) Für die Verarbeitung von Fingerabdrücken sollten in den später von der Kommission vorzuschlagenden Durchführungsrechtsakten weitere Garantien vorgesehen werden, und zwar **betreffend das Erfassungsverfahren, die Betonung des Genauigkeitsgrads und die Einführung eines Ausweichverfahrens**.

Geschehen zu Brüssel am 13. April 2016

Giovanni BUTTARELLI

Europäischer Datenschutzbeauftragter

³⁹ „Die Europäische Sicherheitsagenda“ - Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen vom 28. April 2015, COM(2015) 185 final.