



Stellungnahme des Europäischen Datenschutzbeauftragten zum geänderten Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Einrichtung von „EURODAC“ für den Abgleich von Fingerabdruckdaten zum Zwecke der effektiven Anwendung der Verordnung (EU) Nr. [.../...] [...] (Neufassung)

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,¹

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,²

gestützt auf den Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008³ über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden,

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1. EINLEITUNG

1.1. Konsultation des EDSB

1. Am 30. Mai 2012 nahm die Kommission einen Vorschlag für eine Neufassung einer Verordnung des Europäischen Parlaments und des Rates über die Einrichtung von „EURODAC“ für den Abgleich von Fingerabdruckdaten zum Zwecke der effektiven Anwendung der Verordnung (EU) Nr. [.../...] (zur

¹ ABl. L 281 vom 23.11.1995, S. 31.

² ABl. L 8 vom 12.1.2001, S. 1.

³ ABl. L 350 vom 30.12.2008, S. 60.

Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist) und für der Strafverfolgung dienende Anträge der Strafverfolgungsbehörden der Mitgliedstaaten und Europol auf den Abgleich von EURODAC-Daten sowie zur Änderung der Verordnung (EU) Nr. 1077/2011 zur Errichtung einer Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts („Vorschlag“) an.⁴

2. Gemäß Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 wurde der Vorschlag dem EDSB von der Kommission am 5. Juni 2012 übermittelt. Der EDSB empfiehlt, in der Präambel des Vorschlags auf diese Konsultation zu verweisen.
3. Der EDSB bedauert, dass die Dienststellen der Kommission den EDSB vor Annahme des Vorschlags nicht um informelle Kommentare gebeten haben, wie es im Hinblick auf Kommissionsdokumente, in denen es um die Verarbeitung personenbezogener Daten geht, vereinbart wurde.⁵
4. Der Vorschlag wurde den Innenministern während der Tagung der Innen- und Justizminister am 7./8. Juni 2012 vorgestellt und wird derzeit im Rat und im Europäischen Parlament erörtert; eine Verordnung soll nach dem ordentlichen Gesetzgebungsverfahren Ende 2012 angenommen werden. Die vorliegende Stellungnahme des EDSB ist als Beitrag zu diesem Verfahren zu verstehen.

1.2. Hintergrund

5. EURODAC wurde im Jahr 2000 mit der Verordnung (EG) Nr. 2725/2000 über die Einrichtung von „EURODAC“ für den Vergleich von Fingerabdruckdaten zum Zwecke der effektiven Anwendung des Dubliner Übereinkommens eingerichtet⁶. Vorschläge zur Änderung dieser Verordnung wurden von der Kommission 2008⁷ und 2009⁸ vorgelegt. Ziel des Kommissionsvorschlags von 2008 waren eine stärkere Harmonisierung und bessere Schutzstandards für das Gemeinsame Europäische Asylsystem (GEAS), während mit dem Kommissionsvorschlag von 2009 die Verwendung der Fingerabdruckdaten von Asylbewerbern zu Strafverfolgungszwecken angestrebt wurde.
6. Der EDSB hat Stellungnahmen sowohl zum Vorschlag der Kommission von 2008⁹ als auch zum Vorschlag der Kommission von 2009¹⁰ abgegeben. Insbesondere in der zweiten Stellungnahme äußerte sich der EDSB sehr kritisch.

⁴ KOM(2012)254 endgültig.

⁵ Der EDSB wurde zuletzt 2008 von der Kommission informell zu einer Änderung der EURODAC-Verordnung konsultiert.

⁶ ABl. L 316 vom 15.12.2000, S. 1.

⁷ KOM(2008)825 endgültig.

⁸ KOM(2009)342 endgültig und KOM(2009)344 endgültig.

⁹ Stellungnahme vom 18. Februar 2009 zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Einrichtung von „EURODAC“ für den Abgleich von Fingerabdruckdaten zum Zwecke der effektiven Anwendung der Verordnung (EG) Nr. [...] [zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines

7. Nach Inkrafttreten des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) und der Abschaffung der Säulenstruktur nahm die Kommission 2010 einen neuen Vorschlag an, als Ersatz für die alten Vorschläge.¹¹ Im Hinblick auf Fortschritte in den Verhandlungen über das Asylpaket und zur Erleichterung einer Einigung über EURODAC verzichtete der Kommissionsvorschlag von 2010 auf Bestimmungen über den EURODAC-Zugang zu Strafverfolgungszwecken.
8. Mit dem vorliegenden Vorschlag wird der Vorschlag der Kommission aus dem Jahr 2010 zurückgezogen und ersetzt; er nutzt das Verfahren der Neufassung, um
 - einer EntschlieÙung des Europäischen Parlaments sowie den Ergebnissen von Verhandlungen im Rat Rechnung zu tragen;¹²
 - für die Strafverfolgungsbehörden der Mitgliedstaaten und Europol die Möglichkeit einzuführen, zum Zwecke der Verhütung, Aufdeckung und Untersuchung terroristischer und sonstiger schwerer Straftaten auf die zentrale Datenbank von EURODAC zuzugreifen;
 - die erforderlichen Änderungen an der Verordnung (EU) Nr. 1077/2011 des Europäischen Parlaments und des Rates vom 25. Oktober 2011 zur Errichtung einer Europäischen Agentur für das Betriebsmanagement von IT-GroÙsystemen im Raum der Freiheit, der Sicherheit und des Rechts einzuführen.¹³
9. Gemäß der Begründung des Vorschlags ist inzwischen deutlich geworden, dass „bei den Verhandlungen über das Gemeinsame Europäische Asylsystem im Interesse einer ausgewogenen Lösung“ auch der Zugang der Strafverfolgungsbehörden zu EURODAC geregelt werden muss.¹⁴ Es wurde weder eine neue Konsultation noch eine Folgenabschätzung durchgeführt, da, wie es in der Begründung heißt, die Ergebnisse der Folgenabschätzungen von 2008 und 2009¹⁵ für diesen Vorschlag gleichermaßen gelten. Augenscheinlich aus denselben Gründen wurde dem EDSB auch, wie bereits unter Punkt 3 erwähnt, keine Gelegenheit eingeräumt, informelle Kommentare einzubringen.

1.3. Gründe für die Stellungnahme des EDSB und ihre Struktur

10. In der vorliegenden Stellungnahme möchte der EDSB auf folgende Hauptbedenken eingehen:
 - das bisherige Verfahren wird dem grundlegenden Charakter des Vorschlags nicht gerecht; es hätte eine neue Folgenabschätzung vorgenommen werden müssen;

von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist], KOM(2008) 825, ABl. C 229 vom 23.9.2009, S. 6.

¹⁰ Stellungnahme vom 7. Oktober 2009 zum Vorschlag über den Zugang von Strafverfolgungsbehörden zu EURODAC, ABl. C 92 vom 10.4.2010, S. 1.

¹¹ KOM(2010)555 endgültig.

¹² Siehe Begründung, S. 3.

¹³ ABl. L 286 vom 1.11.2011, S. 1.

¹⁴ Siehe Begründung, S. 3.

¹⁵ SEK(2008)2981 und SEK(2009)936.

- die Notwendigkeit und Verhältnismäßigkeit des Zugangs zu EURODAC-Daten zu Strafverfolgungszwecken sind nicht hinreichend nachgewiesen;
- der Vorschlag trägt weder den datenschutzrechtlichen Folgen der Verwendung von EURODAC-Daten zu Strafverfolgungszwecken ausreichend Rechnung, noch berücksichtigt er die neue Rechtsgrundlage für den Datenschutz seit dem Inkrafttreten des Vertrags von Lissabon und die angelaufene Datenschutzreform.

11. Die Stellungnahme ist folgendermaßen aufgebaut:

- Abschnitt 2 enthält kritische Anmerkungen zur Vorgehensweise der Kommission;
- in Abschnitt 3 stehen allgemeine Bedenken im Zusammenhang mit dem Zugang zu EURODAC-Daten zu Strafverfolgungszwecken im Mittelpunkt;
- Abschnitt 4 enthält Bemerkungen zu den für die Erhebung und Verarbeitung von EURODAC-Daten zu Strafverfolgungszwecken geltenden Datenschutzvorschriften;
- in Abschnitt 5 finden sich Anmerkungen zu konkreten Bestimmungen des Vorschlags, in denen es um den Zugang zu EURODAC zu Strafverfolgungszwecken geht;
- Abschnitt 6 enthält einige Kommentare zu anderen Bestimmungen des Vorschlags;
- in Abschnitt 7 sind die Schlussfolgerungen aufgeführt.

12. Die Stellungnahme stützt sich auf Auffassungen, die bereits in früheren Stellungnahmen zur Reform von EURODAC (siehe Punkt 5) sowie in anderen Stellungnahmen in relevanten Bereichen vorgebracht wurden. Sie berücksichtigt ferner die Erfahrungen der Koordinierungsgruppe für die Aufsicht über EURODAC, die eingerichtet wurde, um die in Artikel 20 der derzeitigen EURODAC-Verordnung geregelte Aufsicht zu erleichtern.¹⁶

2. DIE VORGEHENSWEISE DER KOMMISSION

13. Offensichtlich versteht die Kommission diesen Vorschlag als rein technische Übung. Der Begründung ist zu entnehmen, dass er in der Hauptsache einer Wiederbelebung ihres älteren Vorschlags von 2009 dient. In den letzten drei Jahren haben allerdings, beispielsweise als Folge des Inkrafttretens des Vertrags von Lissabon, wichtige institutionelle und inhaltliche Änderungen stattgefunden. Auch die Tatsache, dass 2010 beschlossen wurde, zur Erleichterung der Verhandlungen in Rat und Parlament die Bestimmungen über den Zugang zu Strafverfolgungszwecken herauszunehmen, ist ein eindeutiger Hinweis darauf, dass der jetzige Vorschlag, einschließlich seines Hauptziels Zugang zu Strafverfolgungszwecken, nicht überwiegend technischer Natur ist.

14. Nach Auffassung der Kommission werden mit dem Vorschlag die Bestimmungen aufgegriffen, die bereits in dem Vorschlag für einen Beschluss des Rates aus dem

¹⁶ Zu dieser Gruppe siehe: <http://www.edps.europa.eu/EDPSWEB/edps/lang/de/Supervision/Eurodac>.

Jahr 2009 enthalten waren. Keines der eingeführten Elemente gilt als neu, und sie wurden alle in den früheren Folgenabschätzungen von 2008¹⁷ und 2009¹⁸ bewertet. Die Kommission legt daher keine neue Folgenabschätzung vor, sondern zieht zur Begründung für die Annahme des Vorschlags weiterhin die beiden Folgenabschätzungen von 2008 bzw. 2009 heran. Der EDSB ist mit dieser Vorgehensweise nicht einverstanden und sieht nach wie vor Bedarf an einer neuen Folgenabschätzung.

15. Aus Sichtweise des EDSB gibt es zwei Gründe dafür, dass die beiden vor drei bzw. vier Jahren vorgenommenen Folgenabschätzungen als Beweis der Notwendigkeit und Kohärenz des vorliegenden Vorschlags nicht ausreichen.
16. Erstens waren die Ergebnisse der früheren Folgenabschätzungen nicht erheblich bzw. nicht überzeugend. Die Folgenabschätzung von 2008 ist unerheblich, weil sie keine Bewertung der Einführung des Zugangs zu EURODAC zu Strafverfolgungszwecken vornimmt. Die Folgenabschätzung von 2009 prüft zwar die Möglichkeit der Verwendung von EURODAC-Daten zu Strafverfolgungszwecken, doch fehlt es hier an einer umfassenden Analyse¹⁹.
17. In der Folgenabschätzung von 2009 wurden vier Optionen für die Regulierung des Zugangs zu Daten von Asylbewerbern zu Strafverfolgungszwecken erwogen.²⁰ Die erste Option (Beibehaltung des Status quo) wurde ohne weitere Erläuterung ausgeschlossen. In zwei der drei übrigen Optionen wurde der Frage nachgegangen, warum zur Identifizierung mutmaßlicher Straftäter sowie zur Verhütung, Bekämpfung und Untersuchung einer Straftat der Zugriff auf die EURODAC-Datenbank von Bedeutung ist. In dieser Analyse wurden jedoch keinerlei konkrete Beispiele genannt, die die tatsächliche Notwendigkeit eines solchen Zugriffs belegen.²¹ Nicht berücksichtigt wurde in der Analyse auch, dass Asylbewerber an sich eine gefährdete Gruppe sind, bei der ein besonderer Schutzbedarf geprüft werden müsste.
18. Die vierte Option sah die eventuelle Schaffung eines dezentralen Netzwerks vor, in dem jeder Mitgliedstaat die Möglichkeit hätte, automatisch die nationalen Asylbewerberdatenbanken aller anderen Mitgliedstaaten abzufragen. Diese Option sah vor, dass das neue Netzwerk nur bestehende Instrumente wie den Mechanismus nutzen würde, der im Beschluss 2008/615/JI des Rates vom 23. Juni 2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität („Beschluss von Prüm“) vorgesehen ist.²² Diese Option wurde mit dem Argument verworfen, sie sei kompliziert und kostspielig.

¹⁷ SEK(2008) 2981, 3.12.2008.

¹⁸ SEK(2009) 936, 10.9.2009.

¹⁹ Nähere Einzelheiten hierzu in den Stellungnahmen des EDSB von 2008 und 2009; siehe ferner die Stellungnahme des EDSB vom 15. Dezember 2010 zur Einrichtung von „EURODAC“ für den Abgleich von Fingerabdruckdaten, ABl. C 101 vom 1.4.2011, S. 14.

²⁰ SEK(2009) 936, S. 17.

²¹ Die auf S. 11 f. der Folgenabschätzung aufgeführten Beispiele sind zu allgemein und zu vage. Sie stützen sich nicht auf reale, konkrete Fälle, sondern vielmehr auf hypothetische Situationen, in denen ein Abgleich von Fingerabdruckdaten von Asylbewerbern zu Strafverfolgungszwecken sinnvoll sein könnte. Siehe ferner Punkte 46 bis 48 der Stellungnahme des EDSB von 2009.

²² ABl. L 210 vom 6.8.2008, S. 1.

19. In der Folgenabschätzung von 2009 hieß es wiederholt, die bestehenden Instrumente im Bereich der Strafverfolgung reichen nicht aus und seien in der Praxis für den Abgleich von Fingerabdruckdaten bei der Untersuchung einer Straftat nicht geeignet. So wurde in der Folgenabschätzung insbesondere unterstrichen, dass die Suche nach Fingerabdruckdaten mit Hilfe der nationalen automatisierten Fingerabdruck-Identifizierungssysteme („AFIS“)²³ anderer Mitgliedstaaten unter Berufung auf den Beschluss von Prüm nicht vollständig zuverlässig ist, da einige Mitgliedstaaten Fingerabdrücke von Asylbewerbern unter Umständen nur in ihren nationalen AFIS speichern, wenn sie im Zusammenhang mit einer Straftat stehen.²⁴ Weiter wurde in der Folgenabschätzung darauf hingewiesen, dass der Rahmenbeschluss 2006/960/JI des Rates über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden²⁵ nur für die Erhebung von Daten über Asylbewerber verwendet werden kann, wenn begründeter Anlass zu der Annahme besteht, dass die entsprechenden Informationen in einem bestimmten Mitgliedstaat tatsächlich verfügbar sind.²⁶ Schließlich machte die Folgenabschätzung deutlich, dass gegenseitige Rechtshilfe es erfordern würde, dass ein Ersuchen an all diejenigen Mitgliedstaaten gerichtet werden müsste, von denen angenommen wird, dass sie über einschlägige Informationen verfügen, was sehr zeitaufwändig sei.²⁷
20. Nach Auffassung des EDSB sollte nachgewiesen werden, dass mit der Kombination dieser drei Instrumente und ihrem gleichzeitigen Einsatz nicht alle denkbaren Fälle abgedeckt werden können, in denen die Identität eines Asylbewerbers für Zwecke der Strafverfolgung benötigt wird. In allen, in der Folgenabschätzung von 2009 erwähnten, Beispielen, wurde der Beschluss von Prüm sowie andere Instrumente unberücksichtigt gelassen, in der Annahme, dass sie unzureichend wären, weil in anderen Systemen keineswegs die Fingerabdruckdaten von allen Asylbewerbern hinterlegt sind. Die Folgenabschätzung enthielt aber auch keine schlüssigen und fundierten Argumente für ein weiteres, auf Asylbewerber ausgelegtes Instrument²⁸, während für andere Personengruppen keine vergleichbaren Instrumente vorgesehen und damit vermutlich auch gar nicht erforderlich sind.
21. Der zweite Grund, aus dem eine neue Folgenabschätzung notwendig ist, ist die Tatsache, dass die beiden älteren Folgenabschätzungen überholt sind. Sie wurden vor dem Hintergrund verfasst, dass der Beschluss von Prüm und der Durchführungsbeschluss von Prüm in den Mitgliedstaaten nur teilweise angewandt wurden. Nach Ansicht des EDSB sollten die seit 2009 bei der Anwendung dieser Beschlüsse erzielten Fortschritte in die Beurteilung der Frage

²³ Siehe Beschluss 2008/616/JI des Rates vom 23. Juni 2008 zur Durchführung des Beschlusses 2008/615/JI zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität, ABl. L 210 vom 6.8.2008, S. 12 („Durchführungsbeschluss zum Prüm-Beschluss“).

²⁴ SEK(2009) 936, S. 9.

²⁵ ABl. L 386 vom 29.12.2006, S. 89.

²⁶ SEK(2009) 936, S. 9.

²⁷ a.a.O., S. 9f.

²⁸ Zu Einzelheiten siehe die Punkte 31 und 32.

einfließen, ob ein Zugang zu EURODAC zu Strafverfolgungszwecken tatsächlich erforderlich ist.

22. Der Vorschlag enthält keine Grundrechtsfolgenabschätzung im Einklang mit der Mitteilung der Kommission „Strategie zur wirksamen Umsetzung der Charta der Grundrechte durch die Europäische Union“ aus dem Jahr 2010, die im Zusammenhang mit dem Inkrafttreten des Vertrags von Lissabon angenommen wurde, welcher der Charta der Grundrechte der Europäischen Union den Status eines Instruments des Primärrechts der EU verlieh.²⁹ In der Folgenabschätzung sollten die Auswirkungen des Vorschlags auf die Grundrechte mit Hilfe der in dieser Mitteilung vorgelegten Checkliste geprüft werden.³⁰
23. Diese Checkliste sieht die Beantwortung grundlegender Fragen vor, wie z. B. der Frage, ob sich positive (Förderung der Grundrechte) oder negative Auswirkungen (Einschränkung der Grundrechte) ergeben und/oder Grundrechtseinschränkungen zur Verwirklichung eines Ziels von allgemeinem Interesse oder zum Schutz der Rechte und Freiheiten Dritter erforderlich sind, ob die Maßnahme in einem angemessenen Verhältnis zu dem angestrebten Ziel steht und dem Wesensgehalt der einschlägigen Grundrechte Rechnung trägt.
24. In Anbetracht der bisherigen Ausführungen empfiehlt der EDSB der Kommission nachdrücklich, eine neue Folgenabschätzung vorzulegen, in der alle vier Optionen geprüft werden, in der solide Nachweise und zuverlässige Statistiken bereitgestellt werden und in der eine Grundrechtsfolgenabschätzung vorgenommen wird. Dies sollte unter angemessener Berücksichtigung der seit 2009 eingetretenen praktischen und rechtlichen Entwicklungen geschehen.

3. ZUGANG ZU EURODAC-DATEN ZU STRAFVERFOLGUNG SZWECKEN

3.1. Zweckbindung und die Gefahr der Zweckentfremdung

25. Als die EURODAC-Verordnung angenommen wurde und die Datenbank 2003 ihren Betrieb aufnahm, war ein Zugriff der Polizei auf die Datenbank nicht vorgesehen. Die Fingerabdruckdaten werden zur Bestimmung des Mitgliedstaats, der für die Prüfung eines Asylantrags zuständig ist, ferner zur Verhütung von Mehrfachasylanträgen innerhalb der EU und, eher allgemein, zur leichteren Anwendung der Dublin-Verordnung, erhoben und verarbeitet.³¹ Mit konkreten Garantien wird gewährleistet, dass die EURODAC-Datenbank *nicht* zu anderen Zwecken verwendet wird.

²⁹ KOM(2010)573.

³⁰ Siehe ferner die operativen Leitlinien der Kommission über die Berücksichtigung von Grundrechten in Folgenabschätzungen der Kommission, SEK(2011)567 vom 6. Mai 2011.

³¹ Das Übereinkommen von Dublin wurde 2003 durch die Verordnung (EG) Nr. 343/2003 des Rates vom 18. Februar 2003 zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen in einem Mitgliedstaat gestellten Asylantrags zuständig ist, ersetzt, ABl. L 50 vom 25.2.2003, S. 1 („Dublin-Verordnung“).

26. Der Vorschlag schlägt eine neue rechtliche Regelung vor, in der Daten auch weiterhin zum Zweck der Prüfung von Asylanträgen erhoben werden, in der die Daten aber unter bestimmten Umständen auch für andere Zwecke verwendet werden könnten, nämlich für die Strafverfolgung außerhalb des Bereichs Asyl und Migration. Hier tritt das ein, was häufig als „Zweckentfremdung“ bezeichnet wird, also eine allmähliche Ausdehnung der Nutzung eines Systems oder einer Datenbank über den Zweck hinaus, zu dem es/sie ursprünglich konzipiert wurde.
27. Der EDSB hegt generell starke Vorbehalte gegen diese Tendenz. Er fordert einen vorsichtigen Umgang mit Initiativen, die darauf hinauslaufen, dass möglicherweise Daten oder Systeme zu Zwecken verwendet werden, die mit dem ursprünglichen Zweck nichts zu tun haben. Es sollte nicht einfach hingenommen werden, dass die Daten, da sie nun schon erhoben wurden, auch zu anderen Zwecken, die stärkere Auswirkungen auf das Leben von Menschen haben könnten, verwendet werden können. Die Beurteilung der Frage, ob die Errichtung von EURODAC den Grundsätzen der Notwendigkeit und Verhältnismäßigkeit entspricht, wäre völlig anders ausgefallen, wenn von Anfang an ein Zugriff auch zu Strafverfolgungszwecken vorgesehen gewesen wäre.
28. Darüber hinaus ist diese Ausdehnung der Nutzung eines bestehenden Systems nur schwer mit dem Grundsatz der Zweckbindung zu vereinbaren, der zu den Kerngrundsätzen des Datenschutzrechts gehört.³² Ausnahmen vom Grundsatz der Zweckbindung sind möglich, allerdings nur unter strengen Auflagen. In allererster Linie muss die Verarbeitung der Daten zu dem anderen Zweck erforderlich sein und zu diesem in einem angemessenen Verhältnis stehen.
29. Nach Auffassung des EDSB wurden die Notwendigkeit und Verhältnismäßigkeit, die eine Ausnahme vom Grundsatz der Zweckbindung rechtfertigen könnten, nicht hinreichend nachgewiesen. Es besteht Bedarf an einer besseren Begründung. Darauf wird in den kommenden Abschnitten näher eingegangen.

3.2. Notwendigkeit des Zugangs zu Strafverfolgungszwecken

30. Der Vorschlag wirft Fragen bezüglich der Notwendigkeit eines Zugangs zu EURODAC zu Strafverfolgungszwecken auf, da, wie bereits gesagt, es bereits eine ganze Reihe von Rechtsinstrumenten gibt, denen zufolge ein Mitgliedstaat Fingerabdruck- und andere Strafverfolgungsdaten im Besitz eines anderen Mitgliedstaats abfragen darf.³³
31. Erstens können die Mitgliedstaaten den Beschluss von Prüm heranziehen, dessen Ziel ja die Vertiefung der grenzüberschreitenden Zusammenarbeit zwischen EU-Staaten in Strafsachen ist, und zwar auch durch die Vernetzung

³² Dieser Grundsatz ist in Artikel 5 Buchstabe b des Übereinkommens des Europarates zum Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten, ETS 108, vom 28. Januar 1981 („Übereinkommen Nr. 108“), in Artikel 6 Absatz 1 Buchstabe b der Richtlinie 95/46/EG sowie in Artikel 3 des Rahmenbeschlusses 2008/977/JI verankert.

³³ Einzelheiten hierzu auch in der Stellungnahme des EDSB vom 7. Oktober 2009.

nationaler Datenbanken der Mitgliedstaaten³⁴. Gemäß Artikel 8 des Beschlusses von Prüm gewährleisten die Mitgliedstaaten, dass Fundstellendatensätze aus den nationalen AFIS, die zur Verhinderung und Verfolgung von Straftaten eingerichtet wurden, vorhanden sind. Diese Fundstellendatensätze dürfen nur eine Kennung und daktyloskopische Daten enthalten (d. h. „Fingerabdrücke, Fingerabdruckspuren, Handabdrücke, Handabdruckspuren und Schablonen (Templates) derartiger Abdrücke (codierte Minutien), wenn diese in einer automatisierten Datenbank gespeichert und verarbeitet werden“³⁵).

32. Zweitens könnten andere Instrumente angewandt werden. So könnte bei der Abfrage von Fingerabdruckdaten der Rahmenbeschluss 2006/960/JI herangezogen werden. Die in diesem Instrument vorgesehenen Maßnahmen können vorbehaltlich einiger Bedingungen angewandt werden; so müssen z. B. schwerwiegende Gründe für die Annahme bestehen, dass die Informationen in dem anderen Mitgliedstaat verfügbar sind, und muss eine vorherige Genehmigung einer Justizbehörde eingeholt werden. Auch das Europäische Übereinkommen über die Rechtshilfe in Strafsachen³⁶ könnte von den Justizbehörden der Mitgliedstaaten bemüht werden, um Zugang zu Sammlungen von Fingerabdruckdaten von Straftätern und Nicht-Straftätern, einschließlich Asylbewerbern, zu erhalten. Hat schließlich ein Drittstaatsangehöriger ein Schengen-Visum beantragt, sind seine Fingerabdrücke als diejenigen eines Antragstellers auf ein Visum bereits im Visa-Informationssystem gespeichert;³⁷ und wenn der Drittstaatsangehörige bereits mit Haftbefehl gesucht wird oder zum Zweck der Einreiseverweigerung eine Warnung herausgegeben wurde, ist er im Schengener Informationssystem gespeichert.³⁸
33. Der EDSB schlägt daher vor, nicht gleich ein neues Instrument zu schaffen, das Strafverfolgungsbehörden Zugang zu Daten von Asylbewerbern gewährt, sondern zunächst einmal die vorhandenen Instrumente gründlich und aus aktueller Perspektive daraufhin zu untersuchen, ob eine umfassende Anwendung der bestehenden Instrumente nicht genügen würde. Nach Ansicht des EDSB deutet vieles darauf hin, dass die vorhandenen Instrumente durchaus wirksam und ausreichend sein könnten.
34. Erst vor kurzem hat sich der Rat mit dem Stand der Umsetzung des Beschlusses von Prüm und des dazu gehörigen Durchführungsbeschlusses befasst. Der Rat stellte fest, dass es bei der Umsetzung nach wie vor gewisse Schwierigkeiten gab³⁹ und forderte im Dezember 2011 die Mitgliedstaaten auf, ihre internen rechtlichen und technischen Umsetzungsverfahren abzuschließen, um die Prümer Beschlüsse in vollem Umfang umzusetzen.⁴⁰ Desgleichen forderte der Rat die Mitgliedstaaten auf, die Bewertung der Wirksamkeit und Effizienz der

³⁴ Siehe Artikel 1 und Erwägungsgrund 13 des Beschlusses von Prüm.

³⁵ Artikel 2 Buchstabe i des Durchführungsbeschlusses zum Beschluss von Prüm.

³⁶ Europäisches Übereinkommen über die Rechtshilfe in Strafsachen, SEV Nr. 030, 20. April 1959.

³⁷ Gestützt auf Artikel 8 der Verordnung (EG) Nr. 767/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen den Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt (VIS-Verordnung), ABl. L 218 vom 13.8.2008, S. 60.

³⁸ Gestützt auf Artikel 95 und 96 des Schengen-Übereinkommens.

³⁹ Ministerrat, 18676/11, 20.12.2011.

⁴⁰ Ministerrat, 17762/11, 5.12.2011.

Prümer Beschlüsse als Instrument des Informationsaustauschs vorzubereiten.⁴¹ Dies steht auch mit dem Stockholmer Programm in Einklang, in dem es heißt: „Der vollständigen und wirksamen Umsetzung, Durchsetzung und Bewertung der bestehenden Instrumente ist in den kommenden Jahren verstärkte Aufmerksamkeit zu widmen“.⁴²

35. Der EDSB blickt in diesem Zusammenhang ferner mit großem Interesse der, für 2012 angekündigten Mitteilung der Kommission zum europäischen Modell für den Informationsaustausch entgegen, die sich unter anderem auf die Ergebnisse der, von der Kommission 2010 durchgeführten, „Information Mapping Exercise“ stützen soll.⁴³ Zweck dieser Übung war eine Analyse bestehender Informationssysteme und -kanäle im Hinblick darauf, ob Bedarf an neuen Instrumenten und Maßnahmen besteht. So lange die bestehenden Instrumente nicht in vollem Umfang umgesetzt sind und diese Umsetzung nicht näher analysiert worden ist, hält der EDSB einen Zugriff auf EURODAC-Daten zu Strafverfolgungszwecken für verfrüht.

3.3. Verhältnismäßigkeit des Zugangs zu Strafverfolgungszwecken

36. Der EDSB hegt ferner Zweifel bei der Frage, ob ein Zugang zu EURODAC-Daten für Strafverfolgungsbehörden im Einklang mit dem Erfordernis der Verhältnismäßigkeit stehen würde.
37. Es sei daran erinnert, dass Asylbewerber eine besonders schutzbedürftige Bevölkerungsgruppe darstellen und daher ihre prekäre Lage bei der Beurteilung der Notwendigkeit und Verhältnismäßigkeit der vorgeschlagenen Maßnahme berücksichtigt werden muss.⁴⁴ Dies ist in den Vorschlägen nicht aufgegriffen worden.
38. Bei den vorgeschlagenen Änderungen des derzeitigen Systems würde im Endergebnis herauskommen, dass ein Asylbewerber an einem Tatort identifiziert werden kann, sofern ein Fingerabdruck gefunden wird, während andere Personen nicht identifiziert werden können, da für alle anderen Bevölkerungsgruppen ähnliche Daten nicht verfügbar sind. Für die in dieser Hinsicht unterschiedliche Behandlung von Asylbewerbern und anderen Personen hat die Kommission keinerlei Begründung angeführt. Die Verarbeitung von EURODAC-Daten für Strafverfolgungszwecke könnte daher möglicherweise zu einer Diskriminierung von Asylbewerbern führen, die ohne Begründung nicht als verhältnismäßige Maßnahme angesehen werden kann.
39. Es sei daran erinnert, dass der Gerichtshof der Europäischen Union und der Europäische Gerichtshof für Menschenrechte („EGMR“) Datenbanken verworfen haben, die zu einer ungerechtfertigten Ungleichbehandlung von

⁴¹ a.a.O.

⁴² Stockholmer Programm, Punkt 1.2.2.

⁴³ http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/eixm/index_en.htm.

⁴⁴ Siehe auch die Stellungnahme des EDSB aus dem Jahr 2009, Punkt 29.

Menschen geführt haben.⁴⁵ Im Urteil in der Rechtssache *S. and Marper* unterstrich der EGMR die Gefahr einer Stigmatisierung in diesem Zusammenhang.⁴⁶

40. Auch wenn die Notwendigkeit des Zugangs zu Strafverfolgungszwecken nachgewiesen und eine angemessene Abwägung von Rechten und Interessen vorgenommen wurde, bedeutet Verhältnismäßigkeit, dass dieser Zugang nur unter strengen Auflagen erfolgen darf, wie es auch in Erwägungsgrund 9 des Vorschlags heißt; dazu gehört auch, dass ein begründeter Verdacht besteht, dass der Urheber einer terroristischen oder sonstigen schweren Straftat einen Asylantrag gestellt hat (siehe auch nachstehenden Punkt 56).

4. ANZUWENDENDE DATENSCHUTZVORSCHRIFTEN

41. Derzeit findet die Richtlinie 95/46/EG auf alle von den Mitgliedstaaten im Rahmen des EURODAC-Systems vorgenommenen Datenverarbeitungen Anwendung. Erhalten jedoch Strafverfolgungsbehörden Zugang zu EURODAC-Daten, hat dies zur Folge, dass der gesamte komplizierte Rechtsrahmen anzuwenden ist, der auf der Grundlage der früheren dritten Säule angenommen wurde. Die Verarbeitung personenbezogener Daten durch national zuständige Behörden fällt unter 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 werden⁴⁷, sofern sie in dessen Anwendungsbereich gehört. Die Verarbeitung personenbezogener Daten durch Europol ist im Beschluss 2009/371/JI des Rates zur Errichtung des Europäischen Polizeiamtes (Europol) geregelt⁴⁸.
42. Der Vorschlag enthält mehrere Bestimmungen, in denen es um bestimmte Rechte und Pflichten im Bereich des Datenschutzes geht. Gemäß Erwägungsgrund 32 des Vorschlags handelt es sich hierbei um Ergänzungen oder Klarstellungen der Richtlinie 95/46/EG. Es wird jedoch nicht klar, wie diese Spezifikationen mit dem Rahmenbeschluss 2008/977/JI oder dem Beschluss 2009/371/JI des Rates in Verbindung stehen.⁴⁹ Artikel 33, dem zufolge beide Beschlüsse auf die Verarbeitung von EURODAC-Daten durch Strafverfolgungsbehörden bzw. Europol anzuwenden sind, schafft hier keine größere Klarheit. Damit bleibt die Frage offen, ob bestimmte Spezifikationen im Vorschlag auch als Ergänzung oder Klarstellung dieser beiden Beschlüsse zu sehen sind.
43. Ein wichtiges Beispiel ist Artikel 35, der die Übermittlung personenbezogener Daten an Drittstaaten, internationale Organisationen oder private Stellen ausdrücklich untersagt. Es wird jedoch nicht erläutert, wie dieses Verbot mit der

⁴⁵ Sieh EuGH, Urteil vom 16. Dezember 2008, Rechtssache C-524/06, *Huber*, [2008] Slg. I-09705 und EGMR, Urteil vom 4. Dezember 2008, Rechtssachen 30562/04 und 30566/04, *S. and Marper v. United Kingdom*.

⁴⁶ a.a.O., Randnr. 122.

⁴⁷ ABl. L 350 vom 30.12.2008, S. 60.

⁴⁸ ABl. L 121 vom 15.5.2009, S. 37.

⁴⁹ Beschluss 2009/371/JI des Rates vom 6. April 2009 zur Errichtung des Europäischen Polizeiamtes (Europol), ABl. L 121 vom 15.5.2009, S. 37.

Möglichkeit der Übermittlung personenbezogener Daten gemäß dem Rahmenbeschluss 2008/977/JI in Verbindung steht. In diesem Zusammenhang muss darauf hingewiesen werden, dass der Rahmenbeschluss 2006/960/JI die Übermittlung personenbezogener Daten an Drittstaaten nicht verbietet.⁵⁰ Nach Auffassung des EDSB ist die Übermittlung von EURODAC-Daten sehr wohl verboten, und zwar auch bei der Verwendung von EURODAC-Daten zu Strafverfolgungszwecken, und er empfiehlt dem Gesetzgeber eine diesbezügliche Klarstellung in Artikel 35 des Vorschlags.

44. Artikel 35 enthält eine Ausnahme von dem Verbot. Die Mitgliedstaaten dürfen nämlich personenbezogene Daten an Drittstaaten übermitteln, auf die die Dublin-Verordnung anwendbar ist. Nach Ansicht des EDSB sollte in einem Erwägungsgrund oder in einem Artikel klargestellt werden, dass diese Ausnahme nicht für Übermittlungen an diese besonderen Drittstaaten im Kontext der Strafverfolgung gilt.
45. Ein weiteres Beispiel ist Artikel 29 des Vorschlags, in dem die Rechte der betroffenen Person geregelt sind. Wäre Artikel 29 tatsächlich eine Ergänzung oder Klarstellung des Rahmenbeschlusses 2008/977/JI oder des Beschlusses 2009/371/JI des Rates, sollte er den Rechten der betroffenen Person im Zusammenhang mit dem Zugang und der Weiterverwendung zu Strafverfolgungszwecken besondere Aufmerksamkeit schenken. Gemäß Artikel 29 Absatz 1 Buchstabe b hat die betroffene Person beispielsweise Anspruch auf Unterrichtung über die Zwecke, für die ihre Daten verarbeitet werden. In dieser Bestimmung wird allerdings nur erwähnt, dass eine Beschreibung der Ziele der Dublin-Verordnung beigefügt wird. Sollte ein Zugang zu EURODAC zu Strafverfolgungszwecken beschlossen werden, sollte die betroffene Person hierüber ebenfalls unterrichtet werden.
46. Die Notwendigkeit einer Klarstellung der Beziehungen zwischen den Bestimmungen des Vorschlags und dem Rahmenbeschluss 2008/977/JI sowie dem Beschluss 2009/371/JI des Rates tritt nun sogar noch klarer hervor, da die Vorschläge für einen neuen Datenschutzrahmen vom 25. Januar 2012 beabsichtigen, die Unterscheidung zwischen einem allgemeinen Datenschutzinstrument und einem eigenständigen Instrument für Strafverfolgungszwecke, beizubehalten.⁵¹ Die vorgeschlagenen neuen Bestimmungen befassen sich ferner weder mit den Datenschutzvorschriften für Organe, Einrichtungen und Agenturen der EU, die in der Verordnung (EG) Nr. 45/2001 niedergelegt sind, noch mit den spezifischen Datenschutzvorschriften, die beispielsweise für Europol gelten, oder mit den Datenschutzvorschriften gemäß dem Beschluss von Prüm.⁵²

⁵⁰ ABl. L 386 vom 29.12.2006, S. 89.

⁵¹ KOM(2012)11 endgültig und KOM(2012)10 endgültig.

⁵² Siehe die Stellungnahme des EDSB zum Datenschutzreformpaket, Punkt 26, abrufbar unter http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_DE.pdf. Dem Schutz von Asylbewerbern dienen zwei weitere Rechtstexte. Erstens die Richtlinie 2011/95/EG (ABl. L 337 vom 20.12.2011, S. 9). In ihr ist der Vertraulichkeitsgrundsatz verankert (Artikel 37), und sie regelt den Schutz der Erhebung, Verarbeitung und Weitergabe von Daten über unbegleitete Minderjährige (Artikel 31 Absatz 5). Zweitens die Verordnung (EG) Nr. 343/2003 des Rates (ABl. L 50 vom 25.2.2003, S. 1). Sie bestimmt, dass die von Mitgliedstaaten beantragten, personenbezogenen Daten sachdienlich und relevant sind und nicht über

5. KONKRETE BESTIMMUNGEN DES VORSCHLAGS, IN DENEN ES UM DEN ZUGANG ZU STRAFVERFOLGUNG SZWECKEN GEHT

47. Wie bereits ausgeführt, sollte zuerst nachgewiesen werden, dass der Zugang zu EURODAC zu Strafverfolgungszwecken notwendig und verhältnismäßig ist. Die Bedingungen, unter denen ein solcher Zugang gewährt werden könnte, sind Gegenstand einer weiteren Analyse, die jedoch erst dann stattfinden sollte, wenn die Notwendigkeit und Verhältnismäßigkeit hinreichend nachgewiesen sind. Dabei sollte den nachstehenden Anmerkungen Rechnung getragen werden.

5.1. Benannte Behörden und Prüfstellen

48. Die Mitgliedstaaten sollen „benannte Behörden“ (Artikel 5 des Vorschlags) sowie „Prüfstellen“ (Artikel 6 und 7 des Vorschlags) bestimmen. Beide Arten von Behörden müssen für die Verhütung, Aufdeckung oder Untersuchung terroristischer oder sonstiger schwerer Straftaten zuständig sein. Ihre Zuständigkeiten unterscheiden sich jedoch erheblich.

49. Artikel 5 besagt, dass die benannten Behörden gemäß der vorgeschlagenen Verordnung zum Zugriff auf EURODAC-Daten berechtigt sind. Um uneingeschränkt zu gewährleisten, dass der Zugriff auf Strafverfolgungszwecke beschränkt ist, empfiehlt der EDSB, in Artikel 5 Absatz 1 folgenden Wortlaut hinzuzufügen: „für die in Artikel 1 Absatz 2 genannten Zwecke“.

50. Die in Artikel 6 genannte Prüfstelle überprüft die Rechtmäßigkeit der von den benannten Behörden gestellten Anträge auf Zugriff auf EURODAC-Daten. Sie prüft und validiert⁵³, ob die Voraussetzungen für einen solchen Zugriff erfüllt sind. Nach Auffassung des EDSB bietet der Kontrollmechanismus eine wesentliche Garantie dafür, dass unrechtmäßiger Zugriff verhütet wird. Er unterstreicht, dass aus der Grundrechtsperspektive die beste Option das Erfordernis einer vorherigen richterlichen Genehmigung wäre, die angemessene und zuverlässige Garantien für Unabhängigkeit und Unparteilichkeit böte. Wird keine gerichtliche Genehmigung gefordert, ist auf jeden Fall dafür zu sorgen, dass die Prüfstelle im Sinne einer echten und ordnungsgemäßen Kontrolle von den benannten Behörden vollkommen unabhängig ist, und dass ein umfassendes Kontrollsystem eingerichtet wird.

51. Der EDSB empfiehlt daher als Mindestmaßnahme, in Artikel 6 des Vorschlags aufzunehmen, dass die Prüfstelle ihre Pflichten und Aufgaben unabhängig wahrnimmt und bezüglich der Durchführung der Prüfungen keinerlei Weisungen entgegennimmt.

das erforderliche Maß für die Prüfung des Asylantrags hinausgehen (Artikel 21 Absatz 1), dass die übermittelten Informationen nur zum Zweck der Bestimmung des Mitgliedstaats verwendet werden dürfen, der für die Prüfung eines Asylantrags zuständig ist (Artikel 21 Absatz 7), und dass der Asylbewerber das Recht auf Unterrichtung im Einklang mit der Richtlinie 95/46/EG hat (Artikel 21 Absatz 9).

⁵³ Siehe Artikel 19 Absatz 2 des Vorschlags.

52. Die gleichen Erwägungen gelten auch für Artikel 7 des Vorschlags über den Zugriff auf EURODAC-Daten durch Europol.

5.2. Verfahren und Bedingungen für den Abgleich und die Übermittlung von Daten zu Strafverfolgungszwecken

53. Gemäß Artikel 19 des Vorschlags ist ein Antrag auf Zugang zu EURODAC-Daten zu Strafverfolgungszwecken von der Prüfstelle vorab darauf zu prüfen, ob die Bedingungen für den Zugriff erfüllt sind. Gemäß Absatz 3 ist „in dringenden Ausnahmefällen“ eine Ausnahme von dieser vorherigen Prüfung vorgesehen. In derartigen Fällen wird nachträglich, also nach der Bearbeitung des Antrags, unverzüglich eine Überprüfung vorgenommen. Es wird allerdings kein Hinweis darauf gegeben, was unter „dringenden Ausnahmefällen“ zu verstehen ist. Diese fehlende Klarheit könnte zu unterschiedlichen Auslegungen und zu Unsicherheit bezüglich des Geltungsbereichs der Ausnahmeregelung führen. Der EDSB empfiehlt, in Artikel 19 das Kriterium „Abwendung einer unmittelbaren Gefahr im Zusammenhang mit schweren oder terroristischen Straftaten“ aufzunehmen.⁵⁴

54. Gemäß Artikel 19 Absatz 3 ist die nachträgliche Überprüfung „unverzüglich“ nach der Bearbeitung des Antrags vorzunehmen. Nach Ansicht des EDSB ist der Ausdruck „unverzüglich“ zu vage, weshalb er die Einführung einer konkreten Frist empfiehlt.

55. Im Einklang mit Artikel 20 können die benannten Behörden den Abgleich von Fingerabdruckdaten mit den Daten in der EURODAC-Zentraldatenbank zu Strafverfolgungszwecken nur dann beantragen, wenn der Abgleich mit den Daten der nationalen Fingerabdruck-Datenbanken anderer Mitgliedstaaten nach dem Beschluss von Prüm ergebnislos war und

- der Abgleich für die Verhütung, Aufdeckung oder Untersuchung terroristischer oder sonstiger schwerer Straftaten erforderlich ist (Artikel 20 Absatz 1 Buchstabe a);
- der Abgleich im Einzelfall erforderlich ist, wobei kein systematischer Abgleich stattfindet (Artikel 20 Absatz 1 Buchstabe b), und
- berechnete Gründe für die Annahme vorliegen, dass er zur Verhütung, Aufdeckung oder Untersuchung der fraglichen Straftaten beitragen wird (Artikel 20 Absatz 1 Buchstabe c).

56. Der EDSB begrüßt das Erfordernis einer vorherigen Abfrage nationaler Datenbanken und von Datenbanken anderer Mitgliedstaaten mit Hilfe des im Beschluss von Prüm vorgesehenen Mechanismus. Seiner Auffassung nach sollte jedoch auch eine vorherige Abfrage des Visa-Informationssystems verlangt werden. Des Weiteren stellt er fest, dass in der Aufzählung der Bedingungen die in Erwägungsgrund 9 des Vorschlags sowie in der Begründung genannte Bedingung fehlt, es müsse der begründete Verdacht bestehen, dass der Urheber einer terroristischen oder sonstigen schweren Straftat einen Asylantrag gestellt

⁵⁴ Denkbar wäre auch eine andere, konkretere Formulierung, wie insbesondere in Erwägungsgrund 26 des Vorschlags: „eine konkrete Gefahr im Zusammenhang mit einer terroristischen oder sonstigen schweren Straftat oder mit bestimmten Personen [...], bei denen ernsthafte Gründe für die Annahme bestehen, dass sie terroristische Straftaten oder andere schwere Straftaten begehen werden oder begangen haben“.

hat.⁵⁵ Im Lichte der vorstehenden Ausführungen zur Verhältnismäßigkeit des Zugangs von Strafverfolgungsbehörden zu EURODAC-Daten vertritt der EDSB die Ansicht, dass dieser Bedingung besondere Bedeutung zukommt, und er empfiehlt dem Gesetzgeber nachdrücklich, sie in die Auflistung in Artikel 20 des Vorschlags aufzunehmen. Der Verweis in Erwägungsgrund 9 allein reicht nicht aus, um die Einhaltung dieser Anforderung zu gewährleisten.

57. Nach Auffassung des EDSB ist der Ausdruck „beitragen“ in Artikel 20 Absatz 1 Buchstabe c zu weit gefasst. Wie es in der Begründung heißt, sollte der Abgleich von Daten „wesentlich“ zur Verhütung, Aufdeckung oder Untersuchung der fraglichen schweren Straftaten beitragen.⁵⁶ Der EDSB schlägt vor, Artikel 20 Absatz 1 Buchstabe c entsprechend zu ändern. Im Zusammenhang mit derselben Bestimmung empfiehlt der EDSB eine Klarstellung dessen, was unter „berechtigten Gründen“ zu verstehen ist.⁵⁷
58. Im Hinblick auf Europol wird weder in der Begründung noch in den Erwägungsgründen erläutert, weshalb Europol Zugriff auf EURODAC-Daten haben sollte. In Erwägungsgrund 10 ist lediglich die Rede von der „Schlüsselrolle“ Europol’s „im Rahmen der Zusammenarbeit zwischen den Behörden der Mitgliedstaaten bei Ermittlungen wegen grenzüberschreitender Kriminalität [...] bei der Unterstützung der Kriminalitätsprävention sowie der Analyse und Untersuchung von Straftaten auf Unionsebene“; diese rechtfertigen den Zugang zu EURODAC-Daten bei der Wahrnehmung seiner Aufgaben. Auch die Folgenabschätzung von 2009 enthält nur wenige genaue Aussagen zu dem konkreten Bedarf Europol’s an direktem Zugriff auf die Daten⁵⁸. In der Praxis bedeutet dies, dass eine nationale Strafverfolgungsbehörde vor der Übermittlung von Fingerabdruckdaten an Europol diese gegebenenfalls mit EURODAC-Daten abgleichen darf (und dies höchstwahrscheinlich auch tun wird). Der EDSB empfiehlt daher, zumindest in einem Erwägungsgrund zu beschreiben, in welchen Situationen ein *direkter* Zugriff von Europol auf die EURODAC-Zentraldatenbank gerechtfertigt ist.
59. Der EDSB hält weiter fest, dass das strenge Kriterium für den Zugriff benannter Behörden auf EURODAC-Daten nicht für den Zugriff auf EURODAC-Daten durch Europol gilt. Anträge von Europol auf Abgleich sind für eine spezifische Analyse oder eine Analyse allgemeiner und strategischer Art zulässig. Der EDSB fragt sich, wie die umfangreicheren Möglichkeiten für Europol zur Argumentation der Kommission passen, dass nämlich der Zugang nur in konkreten Fällen, unter bestimmten Umständen und mit strengen Auflagen notwendig ist. In Ermangelung

⁵⁵ Siehe insbesondere Erwägungsgrund 9 und S. 7 der Begründung.

⁵⁶ Siehe S. 7 der Begründung.

⁵⁷ Siehe auch die Stellungnahme des EDSB von 2010, Punkt 49.

⁵⁸ So heißt es in der Folgenabschätzung von 2009: „(...) Europol soll den nationalen Strafverfolgungsbehörden die für den Informationsaustausch zwischen ihnen erforderlichen Instrumente bereitstellen, wie den Informationsaustausch mit Hilfe der nationalen Europol-Stellen. Aus den Antworten Europol’s und der Mitgliedstaaten auf den Fragebogen geht hervor, dass es sich positiv auf den Informationsaustausch zwischen diesen Stellen auswirken würde, wenn Informationen über Fingerabdrücke von Asylbewerbern Bestandteil der zwischen ihnen über Europol ausgetauschten Informationen als Teil einer konkreten Akte über grenzüberschreitende organisierte Kriminalität sein könnten. Da Europol derzeit keinen Zugriff auf Daten über Asylbewerber hat, kann es nicht gewährleisten, dass diese Informationen Teil seiner Analyse- und Untersuchungsaufgaben sind“.

einer gesonderten Erläuterung hierzu empfiehlt der EDSB, Artikel 21 und Artikel 20 aneinander anzupassen.

5.3. Abgleich mit Fingerabdruckspuren

60. Derzeit können EU-Länder durch den Abgleich von Fingerabdruckdaten einer Person mit EURODAC-Daten bestimmen, ob ein Asylbewerber oder ein Ausländer, der sich unrechtmäßig in einem EU-Land aufhält, zuvor Asyl in einem anderen EU-Staat beantragt hat oder ob ein Asylbewerber illegal in das Hoheitsgebiet der EU eingereist ist. In derartigen Fällen ist es erforderlich, dass sich die betreffende Person tatsächlich im Land befindet (zumindest zu einem bestimmten Zeitpunkt), damit die zuständigen nationalen Behörden seine/ihre Fingerabdrücke zwecks Abgleich mit EURODAC-Daten nehmen können. Abgleiche zu Strafverfolgungszwecken unterscheiden sich von ihrem Ansatz her, da Fingerabdrücke an einem Tatort oder in einer anderen Umgebung genommen werden können, ohne dass die betreffende Person anwesend sein muss. Dies bringt neue Bedenken bezüglich möglicherweise nachteiliger Auswirkungen auf Unschuldige mit sich.
61. Der EDSB hegt starke Zweifel bezüglich der Abfrage von Fingerabdruckspuren im EURODAC-System zu Strafverfolgungszwecken, wie sie in Erwägungsgrund 12 erwähnt wird. Vor allem, wenn Fingerabdruckspuren an öffentlich zugänglichen Orten gefunden wurden, kann jede auf Fingerabdruckspuren beruhende Abfrage von EURODAC in Anbetracht zahlreicher möglicher Übereinstimmungen mit Teilen oder Fragmenten von Abdrücken zu einer größeren Zahl möglicher Treffer führen. Fehltreffer können jedoch schwerwiegende Folgen haben und dazu führen, dass Unschuldige fälschlicherweise in strafrechtliche Ermittlungen verwickelt werden. Die Fehlerquote kann durch die Qualität der Fingerabdruckspuren beeinflusst werden, die häufig verzerrt sind; damit wird es noch schwieriger, diese Fingerabdrücke mit den in EURODAC gespeicherten Abdrücken zu vergleichen, die unter besseren Bedingungen genommen wurden.
62. Für den Abgleich von Fingerabdruckdaten zu Strafverfolgungszwecken sollten auf jeden Fall die gleichen Garantien gelten wie die, die bereits in Artikel 25 Absatz 4 des Vorschlags vorgesehen sind.

5.4. Zugang zu personenbezogenen Daten zu Strafverfolgungszwecken und ihre Aufbewahrung

63. Artikel 33 Absatz 4 besagt: „Personenbezogene Daten, die ein Mitgliedstaat oder Europol nach Maßgabe dieser Verordnung von EURODAC erhalten hat, werden nach Ablauf eines Monats aus den Datenbanken des Mitgliedstaats und Euopols gelöscht, wenn die Daten nicht für spezifische laufende strafrechtliche Ermittlungen des Mitgliedstaats oder von Europol benötigt werden“. Der EDSB begrüßt die Aufbewahrungsfrist für Daten, die zu Strafverfolgungszwecken aus EURODAC abgerufen wurden. Er fordert jedoch eine Klarstellung bezüglich der Anforderung, dass die Daten nur gelöscht werden dürfen, wenn keine spezifischen strafrechtlichen Ermittlungen laufen. Der Zugriff auf EURODAC-Daten sollte nur

bei laufenden strafrechtlichen Ermittlungen erlaubt sein. Der EDSB empfiehlt daher, den Rahmen für diese Ausnahme klarer abzustechen oder sie zu streichen.

5.5. Art der Daten, auf die zu Strafverfolgungszwecken zugegriffen wird

64. Artikel 9 Absatz 5, Artikel 15 Absatz 2 und Artikel 17 Absatz 4, in denen es um den Zugang zu EURODAC-Daten im Zusammenhang mit der Anwendung der Dublin-Verordnung geht, besagen, dass bei einem Treffer (wenn also beim Abgleich von im Zentralsystem gespeicherten und den von einem Mitgliedstaat übermittelten Fingerabdruckdaten eine oder mehrere Übereinstimmungen festgestellt wurden), das Zentralsystem zu allen mit dem Treffer in Zusammenhang stehenden Datensätze, die Daten gemäß Artikel 11⁵⁹ übermittelt, gegebenenfalls zusammen mit den markierten Daten gemäß Artikel 18 Absatz 1. Ähnliche Bestimmungen für den Fall, dass ein Abgleich von Fingerabdruckdaten zu Strafverfolgungszwecken beantragt wird, enthält der Vorschlag jedoch nicht.
65. In der Begründung (S. 7) heißt es: „Der Abgleich mit EURODAC-Daten zu Strafverfolgungszwecken erfolgt auf der Grundlage eines „Treffer/kein Treffer“-Systems, d. h. es lässt sich lediglich feststellen, ob ein anderer Mitgliedstaat im Besitz von Daten zu einem bestimmten Asylbewerber ist. Der Vorschlag sieht keine neuen Möglichkeiten zur Verarbeitung zusätzlicher personenbezogener Informationen nach einem „Treffer“ vor“. Der EDSB fragt sich, was es den Strafverfolgungsbehörden bringen würde, nur eine „Treffer/kein Treffer“-Information zu bekommen, also nur zu erfahren, ob eine Übereinstimmung gegeben ist oder nicht. Man kann wohl davon ausgehen, dass die Strafverfolgungsbehörden auch wissen müssten, welcher Mitgliedstaat im Besitz der Daten über den Asylbewerber ist, zu dem die Fingerabdrücke gehören.
66. Dieser mögliche Bedarf an weiteren Informationen sollte geklärt werden. Für den Fall, dass die Übermittlung weiterer Informationen zum „Treffer“ (z. B. Angabe des Mitgliedstaats, der im Besitz der Daten ist) erwogen werden sollte, erinnert der EDSB daran, dass nach Maßgabe der Grundsätze der Notwendigkeit und Verhältnismäßigkeit die zu übermittelnden Informationen auf das für den Zweck, zu dem der Zugang erfolgte, unbedingt erforderliche Mindestmaß beschränkt werden sollte.

5.6. IT-Agentur und Änderungen der Verordnung (EU) Nr. 1077/2011

67. Der EDSB möchte wissen, warum die Geheimhaltungsvorschriften in Artikel 17 Absatz 5 Buchstabe g der Verordnung (EU) Nr. 1077/2011⁶⁰ verschwunden sind (siehe Artikel 38 Absatz 4 Buchstabe a des Vorschlags), und er empfiehlt, sie wieder aufzunehmen.

⁵⁹ Im Vorschlag ist von den in Artikel 8 Buchstabe a erwähnten Daten die Rede. Gegenstand von Artikel 8 Buchstabe a sind jedoch die von der Agentur zu erstellenden Statistiken. Der EDSB entnimmt der EURODAC-Verordnung, dass die hier gemeinte Bestimmung Artikel 11 des Vorschlags ist, in dem die im Zentralsystem gespeicherten Daten aufgelistet sind.

⁶⁰ Verordnung (EU) Nr. 1077/2011 des Europäischen Parlaments und des Rates vom 25. Oktober 2011 zur Errichtung einer Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts, ABl. L 286 vom 1.11.2011, S. 1.

68. Artikel 38 Absatz 2 des Vorschlags führt in Artikel 12 Absatz 1 Buchstabe t die Pflicht für den Verwaltungsrat ein, von den Strafverfolgungsbehörden der Mitgliedstaaten den Abgleich mit EURODAC-Daten zu Strafverfolgungszwecken zu verlangen. Eine nähere Erläuterung dieser Verpflichtung enthält der Vorschlag nicht. Nach dem Verständnis des EDSB hat sie mit den von der Agentur vorzulegenden Berichten und Statistiken zu tun. Er empfiehlt daher, in Artikel 38 Absatz 2 des Vorschlags zur Änderung von Artikel 12 Absatz 1 Buchstabe t der Verordnung (EU) Nr. 1077/2011 den genauen Zweck dieses Ersuchens sowie die Anonymisierung der Daten durch die Strafverfolgungsbehörden vor ihrer Übermittlung an den Verwaltungsrat zu regeln.

6. ANDERE SPEZIFISCHE BESTIMMUNGEN DES VORSCHLAGS

69. Der EDSB hat sich, wie weiter oben unter Punkt 6 ausgeführt, zu anderen Bestimmungen des Vorschlags bereits in seinen Stellungnahmen aus den Jahren 2008 und 2009 geäußert. Diese Ausführungen sollen an dieser Stelle nicht noch einmal vollständig wiederholt werden. In diesem Abschnitt soll vielmehr auf die Hauptbedenken eingegangen und sollen einige neue Änderungen behandelt werden. Bei Bedarf wird auf die tiefer gehenden Analysen in den früheren Stellungnahmen des EDSB verwiesen.

6.1. Artikel 4: Betriebsmanagement

70. Der EDSB begrüßt die Verpflichtung, dafür zu sorgen, dass vorbehaltlich einer Kosten-Nutzen-Analyse jederzeit die beste verfügbare Technologie für das Zentralsystem zum Einsatz kommt (Artikel 4 Absatz 1). Er empfiehlt jedoch, den Ausdruck „beste verfügbare Technologie“ durch „beste verfügbare Techniken“ zu ersetzen, der sowohl die eingesetzte Technologie als auch die Art und Weise abdeckt, in der die Anlage entworfen, gebaut, gewartet und betrieben wird. Dies ist wichtig, da das Konzept „beste verfügbare Techniken“ breiter angelegt ist und verschiedene Aspekte erfasst, die einen Beitrag zum „eingebauten Datenschutz“ leisten, der ja als Schlüsselkonzept bei der Überprüfung des Regelwerks der EU für den Datenschutz gilt.⁶¹

71. In Artikel 3 Absatz 1 ist ein Notfallsystem vorgesehen. In Artikel 4 Absatz 5 ist bestimmt, dass die Plattform 24 Stunden am Tag und sieben Tage in der Woche betriebsbereit zu halten ist. Dies zeigt, dass das System als kritisch gilt. Es werden allerdings keine Einzelheiten zu diesem „Notfallsystem“ oder seiner Sicherheit und zu Datenschutzerfordernissen ausgeführt.

72. Für ein kritisches System sollte es (für den Fall größerer Störungen oder Katastrophen) ein solides und getestetes Notfallsystem geben, das sich allerdings auf Datenschutz, Sicherheit und Kosten auswirkt. Es sollte angemessene Sorgfalt

⁶¹ Siehe Artikel 23 des Vorschlags der Kommission für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Allgemeine Datenschutzverordnung) (KOM(2012) 11 endgültig) und die Punkte 177 bis 182 der Stellungnahme des EDSB vom 7. März 2012. Siehe ferner die Stellungnahme des EDSB vom 15. Dezember 2010 und die Stellungnahme des EDSB vom 18. Februar 2009.

auf die Ermittlung des Bedarfs an Verfügbarkeit des Systems verwandt werden, bei der auch Wartungsbedarf und unvorhersehbare Ausfallzeiten zu berücksichtigen sind. Außerdem sollten die Anforderungen an das Notfallsystem beschrieben werden. Bei der Ausarbeitung von Notfallmaßnahmen sind deren Auswirkungen auf den Datenschutz Rechnung zu tragen. Auswirkungen können sich ergeben aus der Existenz von Dubletten, Backup-Medien und weiteren physischen Orten und Systemen, an denen ein physischer Zugang zu den Daten möglich sein könnte. Der EDSB empfiehlt, anstelle des Notfallsystems in Artikel 3 Absatz 1 und Artikel 4 Absatz 5 einen Notfallplan zu fordern und eine Rechtsgrundlage für Durchführungsvorschriften mit den Modalitäten eines solchen Plans zu schaffen.

6.2. Artikel 9, 14 und 17: Schwierigkeiten bei der Erfassung („Failure to enrol“)

73. Der EDSB ruft das Problem des sogenannten „failure to enrol“ in Erinnerung, also die Situation, in der die Fingerabdrücke einer Person nicht zu gebrauchen sind. Es ist unbedingt darauf zu achten, dass Asylbewerbern wegen Schwierigkeiten bei der Erfassung nicht automatisch Rechte versagt werden. Der Vorschlag befasst sich bereits mit einem Teil der Schwierigkeiten bei der Erfassung in Artikel 9 Absatz 1 und 2. Diese Bestimmungen gehen allerdings von der Hypothese vorübergehender Schwierigkeiten bei der Erfassung aus, während in einigen Fällen dieses Phänomen von Dauer ist. Der EDSB empfiehlt daher, den Artikeln 9, 14 und 17 eine Bestimmung hinzuzufügen, der zufolge die vorübergehende oder dauerhafte Unfähigkeit, verwendbare Fingerabdrücke bereitzustellen, sich nicht nachteilig auf den rechtlichen Status der betreffenden Person auswirken darf. Auf keinen Fall ist dies ein hinreichender Grund, einen Asylantrag nicht zu prüfen oder abzulehnen.⁶²

6.3. Artikel 16: Datenaufbewahrung

74. Der EDSB begrüßt die Änderung in Artikel 16, mit der eine Aufbewahrungsfrist von einem Jahr (anstelle von zwei Jahren im derzeitigen Wortlaut der Verordnung) festgelegt wird. Dies ist eine gute Anwendung des Grundsatzes der Datenqualität, dem zufolge die Daten nicht länger aufbewahrt werden sollten, als für den Zweck, zu dem sie erhoben wurden, erforderlich ist.⁶³

6.4. Artikel 29: Recht auf Information

75. Der EDSB weist darauf hin, dass die betroffene Person so zu unterrichten ist, dass der Asylbewerber seine Lage und den Umfang seiner Rechte vollständig begreift und auch die Verfahrensschritte versteht, die er nach einer Verwaltungsentscheidung in seinem Fall unternehmen kann. In diesem

⁶² Siehe Stellungnahme des EDSB vom 15. Dezember 2010 über die Einrichtung von EURODAC für den Abgleich von Fingerabdruckdaten, Abschnitt IV, ABl. C 101 vom 1.4.2011, S. 14.

⁶³ Siehe Artikel 6 Absatz 1 Buchstabe e der Richtlinie 95/46/EG und Artikel 4 Absatz 1 Buchstabe e der Verordnung (EG) Nr. 45/2001. Siehe ferner Artikel 4 Absatz 2 des Rahmenbeschlusses 2008/977/JI des Rates.

Zusammenhang begrüßt der EDSB die Zusätze in Artikel 29 Absatz 1, die im Einklang mit dem Vorschlag für eine allgemeine Datenschutzverordnung stehen.⁶⁴

76. Der EDSB begrüßt die Erstellung eines gemeinsamen Merkblatts, das in einer klaren und einfachen Sprache die der betroffenen Person zu erteilenden Informationen enthält, und er begrüßt die Verpflichtung für die Mitgliedstaaten, Minderjährige in einer ihrem Alter angemessenen Weise zu unterrichten. Dies trägt zu einer stärkeren Harmonisierung und zur besseren Einhaltung der EURODAC-Verordnung bei und greift überdies Empfehlungen der Koordinierungsgruppe für die Aufsicht über EURODAC auf⁶⁵.

6.5. Artikel 28 und 36: Aufzeichnung der Datenverarbeitungsvorgänge, Protokollierung und Dokumentierung

77. Für Zwecke der Überwachung des Datenschutzes und der Datensicherheit führen die Agentur, die Mitgliedstaaten und Europol Buch über alle Datenverarbeitungsvorgänge in der Zentraleinheit (Artikel 28) sowie über Anträge auf Abgleich mit EURODAC (Artikel 36). Auch wenn die beiden Bestimmungen die gleichen Ziele verfolgen (Datenschutz und Datensicherheit), unterscheiden sie sich doch in ihrem Wortlaut (in Artikel 28 ist z. B. die Rede von Stellen, *die Daten eingegeben oder abgefragt haben*, während in Artikel 36 von der *Behörde, die den Zugriff zwecks Datenabgleichs beantragt hat*, gesprochen wird). Im Sinne der Kohärenz und einer ordnungsgemäßen Überwachung empfiehlt der EDSB die Zusammenlegung der beiden Bestimmungen zu einer, in der dann der präzisere und vollständigere Wortlaut von Artikel 36 verwendet werden sollte.
78. Artikel 36 sieht vor, dass die Mitgliedstaaten und Europol über die von der Agentur geführten Aufzeichnungen hinausgehende Protokolle und Unterlagen zu führen haben. (z. B. die Kennung des Beamten, der die Abfrage vorgenommen hat, sowie des Beamten, der die Abfrage oder Übermittlung angeordnet hat). Der EDSB begrüßt diese Verpflichtung, die im Einklang mit dem Grundsatz der Rechenschaftspflicht steht und zu einer wirksamen Kontrolle beitragen wird.
79. Schließlich stellt der EDSB fest, dass in Artikel 36 noch die Rede vom Zugang nationaler Kontrollbehörden zu diesen Protokollen ist, wohingegen ein ähnlicher Zugang für den EDSB und die Kontrollinstanz von Europol zu den Aufzeichnungen der Agentur bzw. Europols nicht erwähnt wird. Der EDSB empfiehlt eine entsprechende Änderung von Artikel 28.

6.6. Artikel 31 und 32: Überwachungsmodell

⁶⁴ Siehe die Stellungnahme des EDSB vom 15. Dezember 2010 sowie Artikel 11 und 14 des Vorschlags für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Allgemeine Datenschutzverordnung) (KOM(2012) 11 endgültig).

⁶⁵ Siehe Zweite koordinierte Inspektion in Bezug auf die Unterrichtung der betroffenen Personen und die Bestimmung des Alters junger Asylbewerber, abrufbar unter http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Eurodac/09-06-24_Eurodac_report2_EN.pdf.

80. Der EDSB begrüßt das in Artikel 31 und 32 des Vorschlags entworfene Überwachungsmodell. Es ähnelt dem Modell für das Schengener Informationssystem (2. Generation) und für das Visa-Informationssystem.⁶⁶ Es gibt die derzeitige Vorgehensweise wieder, die sich als effizient erwiesen hat, und hat die Zusammenarbeit zwischen dem EDSB und den nationalen Datenschutzbehörden gefördert. Der EDSB begrüßt daher ihre Formalisierung im Vorschlag sowie die Tatsache, dass der Gesetzgeber damit für Kohärenz mit den Kontrollsystemen anderer IT-Großsysteme gesorgt hat.
81. Erwägungsgrund 34 des Vorschlags erwähnt ausdrücklich die Überwachung der Rechtmäßigkeit der Verarbeitungstätigkeiten von Europol durch die mit dem Europol-Beschluss eingerichtete Kontrollinstanz. Der Vorschlag enthält zwar spezifische Bestimmungen über die Aufsicht, wenn Daten von Mitgliedstaaten oder der Agentur verarbeitet werden (siehe Artikel 31 und 32); der EDSB muss allerdings feststellen, dass der Wortlaut keine ähnliche Bestimmung über die Aufsicht der Datenverarbeitungstätigkeiten von Europol enthält, und er empfiehlt, sich diesem Thema zu widmen.

6.7. Artikel 34: Datensicherheit

82. Der EDSB hat eine Reihe von Vorschlägen zu Artikel 34 über Datensicherheit.
- In Artikel 34 Absatz 2 Buchstabe a sollte nicht allgemein von kritischen Infrastrukturen die Rede sein, sondern von der für das System erforderlichen Infrastruktur. Das Wort „kritisch“ sollte durch „*relevant*“ ersetzt werden.
 - In Artikel 34 Absatz 2 Buchstabe f sollte der Ausdruck „personalisierter Zugangsmodus“ näher erläutert werden.
 - Der EDSB empfiehlt, in Artikel 34 Absatz 2 Buchstabe g folgende Passage hinzuzufügen: *„ihre Profile und andere relevante Informationen zur Verfügung stellen, die die Behörden zur Wahrnehmung ihrer Aufsichtsaufgabe benötigen“*. Der EDSB empfiehlt weiter, einen ausdrücklichen Verweis auf Artikel 28 der Richtlinie 95/46/EG aufzunehmen, da die Anforderungen an die Datensicherheit in Artikel 34 sowohl Datenübermittlungen zur Erleichterung der Anwendung der Dublin-Verordnung als auch Übermittlungen zu Strafverfolgungszwecken betreffen.
 - In Artikel 34 Absatz 2 Buchstabe i sollte gewährleistet werden, dass die Protokolle und die Daten, die sie betreffen, geschützt werden.
 - Zur Überwachung der Wirksamkeit der Sicherheitsmaßnahmen empfiehlt der EDSB, in Artikel 34 Absatz 2 Buchstabe k nicht nur Audits (also den Überblick über die Situation zu einem bestimmten Zeitpunkt), sondern auch eine Beobachtung des Systems mit Hilfe besonderer Instrumente beinahe in Echtzeit aufzunehmen.
 - Ferner sollte in Artikel 34 der Notfallplan erwähnt werden⁶⁷. Im Hinblick auf Sicherheitszwischenfälle sollte er Folgendes enthalten:

⁶⁶ Siehe Artikel 41 bis 43 der VIS-Verordnung, Artikel 46 der Verordnung (EG) Nr. 1987/2006 des Europäischen Parlaments und des Rates vom 20. Dezember 2006 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II), ABl. L 381 vom 28.12.2006, S. 4, sowie Artikel 62 des Beschlusses 2007/533/JI des Rates vom 12. Juni 2007 über die Errichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II), ABl. L 205 vom 7.8.2007, S. 63.

⁶⁷ Siehe vorstehende Punkte 72 und 73.

- Die Mitgliedstaaten haben die Agentur über in ihrem System festgestellte Sicherheitszwischenfälle zu unterrichten;
- die Agentur hat bei Sicherheitszwischenfällen alle Beteiligten zu informieren;
- während eines Sicherheitszwischenfalls haben alle Beteiligten zusammenzuarbeiten;
- die nationalen Aufsichtsbehörden und der EDSB sind zu informieren.

6.8. Artikel 40: Eigenkontrolle und Jahresbericht

83. Gemäß Artikel 40 Absatz 1 unterbreitet die Agentur dem Europäischen Parlament und dem Rat jährlich einen Bericht über die Tätigkeit des Zentralsystems. Der EDSB möchte ebenfalls Empfänger des Jahresberichts der Agentur sein.
84. In Artikel 40 Absatz 2 sind die Überwachungsverfahren geregelt. Nach Ansicht des EDSB sollte es bei dieser Überwachung nicht nur um die Aspekte Leistung, Kosteneffizienz und Dienstleistungsqualität gehen, sondern auch um die Einhaltung der gesetzlichen Vorgaben, insbesondere im Bereich des Datenschutzes. Artikel 40 Absatz 2 sollte entsprechend geändert werden.
85. Für diese Eigenkontrolle der Rechtmäßigkeit der Verarbeitung sollte die Kommission die gemäß Artikel 28 des Vorschlags geführten Aufzeichnungen verwenden dürfen. Dementsprechend sollte in Artikel 28 bestimmt werden, dass diese Aufzeichnungen nicht nur zur Überwachung des Datenschutzes und zur Gewährleistung der Datensicherheit, sondern auch für regelmäßige Eigenkontrollen von EURODAC gespeichert werden sollen. Die Eigenkontrollberichte werden dem EDSB und anderen Aufsichtsbehörden bei ihrer Aufsichtstätigkeit helfen, da sie damit leichter ihre diesbezüglichen Schwerpunkte festlegen können.

6.9. Artikel 43: Veröffentlichung der Liste von Behörden

86. Der EDSB begrüßt die Verpflichtung für die Kommission, eine Liste der Behörden zu veröffentlichen, die Zugang zu EURODAC haben (Artikel 43). Im Sinne größerer Transparenz und um ein wirksames, praktisches Instrument für eine bessere Überwachung des Systems (beispielsweise durch die nationalen Datenschutzbehörden) zu schaffen, empfiehlt der EDSB, die Mitgliedstaaten und Europol dazu zu verpflichten, ihre an die Kommission weitergegebenen Angaben ständig zu aktualisieren. Ferner empfiehlt der EDSB, die Kommission zu verpflichten, diese Informationen den Mitgliedstaaten, Europol und der breiten Öffentlichkeit „mit Hilfe einer laufend auf den neuesten Stand gebrachten elektronischen Veröffentlichung“ zur Verfügung zu stellen.

7. SCHLUSSFOLGERUNGEN

87. Der EDSB stellt fest, dass es in den letzten Jahren innerhalb von Kommission, Rat und Europäischem Parlament eine intensive Debatte über den Zugang zu EURODAC-Daten zu Strafverfolgungszwecken gegeben hat. Er sieht auch, dass

eine Fingerabdruckdatenbank ein weiteres hilfreiches Instrument zur Verbrechensbekämpfung sein kann. Der EDSB weist allerdings darauf hin, dass dieser Zugang zu EURODAC schwerwiegende Auswirkungen auf den Schutz der personenbezogenen Daten der Personen hat, deren Daten im EURODAC-System gespeichert sind. Die Notwendigkeit eines solchen Zugangs kann nur anerkannt werden, wenn sie klar und unstrittig belegt wird und die Verhältnismäßigkeit der Verarbeitung nachgewiesen ist. Dies gilt umso mehr im Fall des im Vorschlag vorgesehenen Eingreifens in die Rechte von Menschen, die zu einer gefährdeten und besonders schutzbedürftigen Bevölkerungsgruppe gehören.

88. Die bisher vorliegenden Nachweise sind, auch in Anbetracht des vorstehend beschriebenen Kontexts, nach Auffassung des EDSB nicht ausreichend und aktuell genug, um die Notwendigkeit und Verhältnismäßigkeit der Gewährung des Zugriffs auf EURODAC-Daten zu Strafverfolgungszwecken zu belegen. Es gibt bereits eine Reihe von Rechtsinstrumenten, denen zufolge ein Mitgliedstaat Fingerabdruck- und andere Strafverfolgungsdaten im Besitz eines anderen Mitgliedstaats abfragen darf. Voraussetzung für den Zugang zu Strafverfolgungszwecken ist eine deutlich bessere Begründung.
89. Vor diesem Hintergrund empfiehlt der EDSB der Kommission, eine neue Folgenabschätzung vorzulegen, in der alle relevanten Optionen geprüft werden, in der solide Nachweise und zuverlässige Statistiken bereitgestellt werden und in der eine Grundrechtsfolgenabschätzung vorgenommen wird.

90. Der EDSB hat folgende problematische Punkte herausgearbeitet:

Anzuwendende Datenschutzvorschriften

91. Der EDSB fordert eine Klarstellung der Beziehungen zwischen den Bestimmungen des Vorschlags, in denen es um bestimmte Datenschutzrechte und -pflichten geht, und dem Rahmenbeschluss 2008/977/JI des Rates sowie dem Beschluss 2009/371/JI des Rates (siehe Abschnitt 4).

Bedingungen für den Zugang zu Strafverfolgungszwecken

Wie bereits ausgeführt, sollte zuerst nachgewiesen werden, dass der Zugang zu EURODAC zu Strafverfolgungszwecken notwendig und verhältnismäßig ist. Dabei sollte den nachstehenden Anmerkungen Rechnung getragen werden.

92. Der EDSB empfiehlt,

- klarzustellen, dass die Übermittlung von EURODAC-Daten an Drittländer auch bei Verwendung von EURODAC-Daten zu Strafverfolgungszwecken untersagt ist (siehe Punkte 43 und 44);
- die Strafverfolgungszwecke den der betroffenen Person mitgeteilten Informationen hinzuzufügen (siehe Punkt 45);
- eindeutig zu gewährleisten, dass der Zugang der benannten Behörden zu EURODAC-Daten auf Strafverfolgungszwecke beschränkt ist (siehe Punkt 49);
- den Zugriff auf EURODAC-Daten zu Strafverfolgungszwecken von einer vorherigen gerichtlichen Genehmigung abhängig zu machen oder zumindest

vorzusehen, dass die Prüfstelle ihren Pflichten und Aufgaben unabhängig nachkommt und keinerlei Weisungen bezüglich der Durchführung der Prüfung entgegennimmt (siehe Punkte 50 und 51);

- das Kriterium „Notwendigkeit der Abwendung einer unmittelbaren Gefahr im Zusammenhang mit schweren oder terroristischen Straftaten“ im Ausnahmefall zur Rechtfertigung einer Abfrage von EURODAC-Daten ohne vorherige Prüfung durch die Prüfstelle aufzunehmen und eine konkrete Frist für die nachträgliche Überprüfung festzulegen (siehe Punkt 53 und 54);

- bei den Zugangsbedingungen folgende Bedingungen hinzuzufügen: i) vorherige Abfrage des Visa-Informationssystems, ii) ein „begründeter Verdacht, dass der Urheber einer terroristischen oder sonstigen schweren Straftat einen Asylantrag gestellt hat“, und iii) der „wesentliche“ Beitrag zu Strafverfolgungszwecken und die Klarstellung dessen, was unter „berechtigten Gründen“ zu verstehen ist (siehe Punkte 56 und 57);

- in einem Erwägungsgrund zu beschreiben, in welchen Situationen ein *direkter* Zugriff von Europol auf die EURODAC-Zentraldatenbank gerechtfertigt ist, und vorzusehen, dass die strengen Zugangsbedingungen für die nationalen, benannten Behörden auch für Europol gelten (siehe Punkte 58 und 59);

- dafür zu sorgen, dass für den Abgleich von Fingerabdruckdaten zu Strafverfolgungszwecken mindestens die gleichen Garantien gelten, wie sie für Zwecke der Dublin-Verordnung gelten (siehe Punkt 62);

- die Vorschriften über die Aufbewahrung bzw. Löschung von Daten klarer zu fassen (siehe Punkt 64);

- klarzustellen, welche weiteren Angaben zum „Treffer“ gegebenenfalls an Europol übermittelt werden (siehe Punkte 65 und 66);

- genau den Zweck/die Zwecke des Antrags des Verwaltungsrats der Agentur auf Abgleich mit EURODAC-Daten durch Strafverfolgungsbehörden der Mitgliedstaaten zu bestimmen sowie die Anonymisierung der Daten durch die Strafverfolgungsbehörden vor ihrer Übermittlung an den Verwaltungsrat vorzusehen und die Vorschriften über die Verschwiegenheitspflicht wieder einzuführen (siehe Punkte 67 und 68);

- für den EDSB und die Kontrollinstanz von Europol den Zugang zu den von der Agentur bzw. Europol geführten Aufzeichnungen sowie die Verpflichtung zur Speicherung von Aufzeichnungen auch für regelmäßige Eigenkontrollen von EURODAC vorzusehen (siehe Punkte 79 und 85);

- die Überwachung der Datenverarbeitungstätigkeiten von Europol klarzustellen (siehe Punkt 81).

Sonstige Bestimmungen

93. Der EDSB empfiehlt,

- das Notfallsystem durch einen Notfallplan zu ersetzen und eine Rechtsgrundlage für Durchführungsvorschriften mit den Modalitäten eines solchen Plans zu schaffen (siehe Punkt 72);

- dafür zu sorgen, dass sich die vorübergehende oder dauerhafte Unfähigkeit zur Bereitstellung verwendbarer Fingerabdrücke nicht nachteilig auf die rechtliche Situation der Person auswirkt und dass sie auf keinen Fall ein hinreichender Grund ist, einen Asylantrag nicht zu prüfen oder abzulehnen (siehe Punkt 73);

- für Kohärenz zwischen den Verpflichtungen von Agentur, Mitgliedstaaten und Europol zur Führung von Aufzeichnungen und Unterlagen über Datenverarbeitungsvorgänge zu sorgen (siehe Punkt 77);
- die Bestimmungen über Datensicherheit zu verbessern (siehe Punkt 82);
- den EDSB auf die Verteilerliste des Jahresberichts der Agentur zu setzen (siehe Punkt 83);
- in Artikel 43 eine Verpflichtung für die Mitgliedstaaten und Europol hinzuzufügen, die der Kommission zur Verfügung gestellten Informationen laufend zu aktualisieren, und zu verlangen, dass die Kommission diese Informationen den Mitgliedstaaten, Europol und der breiten Öffentlichkeit „mit Hilfe einer laufend auf den neuesten Stand gebrachten elektronischen Veröffentlichung“ zur Verfügung stellt (siehe Punkt 86).

Brüssel, den 5. September 2012

(unterzeichnet)

Peter HUSTINX
Europäischer Datenschutzbeauftragter