

EURODAC 2.0? Anmerkungen zur bevorstehenden Öffnung von EURODAC für Strafverfolgungsbehörden aus politikwissenschaftlicher Perspektive

Jonathan P. Aus

[jonathan.aus@gmail.com]

Vortrag [überarbeitete Fassung mit Anlagen]

im Rahmen der Tagung "Biometrische Identitäten und ihre Rolle in den
Diskursen um Sicherheit und Grenzen"

Humboldt-Universität zu Berlin, Institut für Informatik

1. Dezember 2012, 14:30 – 15:30 Uhr

Thema und Fragestellung des Vortrages

THEMA:

Die – gegenwärtig noch andauernden – politischen Verhandlungen auf EU-Ebene zum polizeilichen Zugriff auf das EU-AFIS EURODAC (in Betrieb seit Anfang 2003; Datenbestand Ende 2011: rund 2 Millionen Asylantragsteller/-innen und irreguläre Grenzgänger/-innen) bzw. juristisch präzise formuliert: zum „geänderten Vorschlag der Europäischen Kommission für eine Verordnung des Europäischen Parlaments und des Rates über die Einrichtung von ‚EURODAC‘ ... für der Strafverfolgung dienende Anträge der Strafverfolgungsbehörden der Mitgliedstaaten und Europol auf den Abgleich mit EURODAC-Daten...“ vom 30. Mai 2012 [Anlage 1].

FRAGESTELLUNG:

Wie kann diese – vermutlich Anfang 2013 abgeschlossene – Entwicklung aus politischer/politikwissenschaftlicher Perspektive eingeordnet/erklärt werden?

Gliederung des Vortrages

1. Rückblick auf EURODAC 1.0 sowie kurze Zusammenfassung von „Eurodac: A Solution Looking for a Problem?“ (Aus 2006)

1.1 Fragestellung und zentrale Befunde

1.2 Entwicklung der Datenbank 2003-2011 und nicht-intendierte Nebenfolgen

2. Empirische Analyse der gegenwärtigen politischen Verhandlungen auf EU-Ebene zu EURODAC 2.0

2.1 Relevante EU-Institutionen (Überblicksdarstellung)

2.2 Treibende Mitgliedstaaten im Rat (und außerhalb des Rates)

2.3 Umsetzung von Prüm / Schengen III (Stand: 12. Oktober 2012)

2.4 Verhandlungstaktiken der Europäischen Kommission

2.5 Worum geht es der befürwortenden „konservativen“ Mehrheit im EP?

2.6 Worum geht es der skeptischen aber letztlich kompromissbereiten „sozial-liberalen“ Minderheit/Mehrheit im EP?

2.7 Worum geht es der ablehnenden „grün-linken“ Minderheit im EP?

2.8 Verhandlungspartner/-innen im Rahmen der bevorstehenden EURODAC-„Trilogues“

3. Kritik von Datenschutzbeauftragten, Rechtsanwaltsverbänden, Akademikern und Flüchtlingsschutzorganisationen an EURODAC 2.0


3.1 Europäischer Datenschutzbeauftragter und Bundesrechtsanwaltskammer

3.2 Meijers Committee

3.3 UNHCR

4. Fazit

5. Anlagenverzeichnis / Anlagen



1. Rückblick auf EURODAC 1.0 sowie kurze Zusammenfassung von
„Eurodac: A Solution Looking for a Problem?“ (Aus 2006)

[<http://eiop.or.at/eiop/texte/2006-006a.htm>]

1.1 Fragestellung und zentrale Befunde

- Versuch einer Erklärung der Institutionalisierung von EURODAC zwischen 1990-2005

- Rationalistische und Institutionalistische Perspektiven: Probleme, die nach Lösungen suchen vs. Lösungen, die nach Problemen suchen

- Empirische Analyse der Verhandlungen zu EURODAC 1.0 (Verordnung des Rates vom 11. Dezember 2000) unterstreicht die Bedeutung
 - a) von polizeispezifischen Lösungen (hier: „erkennungsdienstliche Behandlung“) für gesellschaftliche Probleme (hier: Flucht und Migration) und deren politischer Artikulation durch Akteure wie den ehem. BMI-Staatssekretär Kurt Schelter
 - b) von kommerziellen Anbietern entsprechender Systeme wie *Morpho* (AFIS Deutschland, Frankreich, Österreich ...) und *Sterea* (EURODAC, VIS, SIS II ...)
 - c) von Schengen- bzw. Dublin-bezogenen Zentrum/Peripherie-Konflikten zwischen den EU-Mitgliedstaaten (Deutschland, Frankreich, Niederlande etc. versus Italien, Griechenland etc.)
 - d) der relativen Macht einzelner Mitgliedstaaten (hier insbesondere der deutschen Schengen- und Ratspräsidentschaft) bei der Institutionalisierung supranationaler AFIS und anschließenden Ausweitung von deren persönlichem Anwendungsbereich (hier: von Asylantragsteller/-innen auf irreguläre Grenzgänger/-innen und *sans-papiers*)

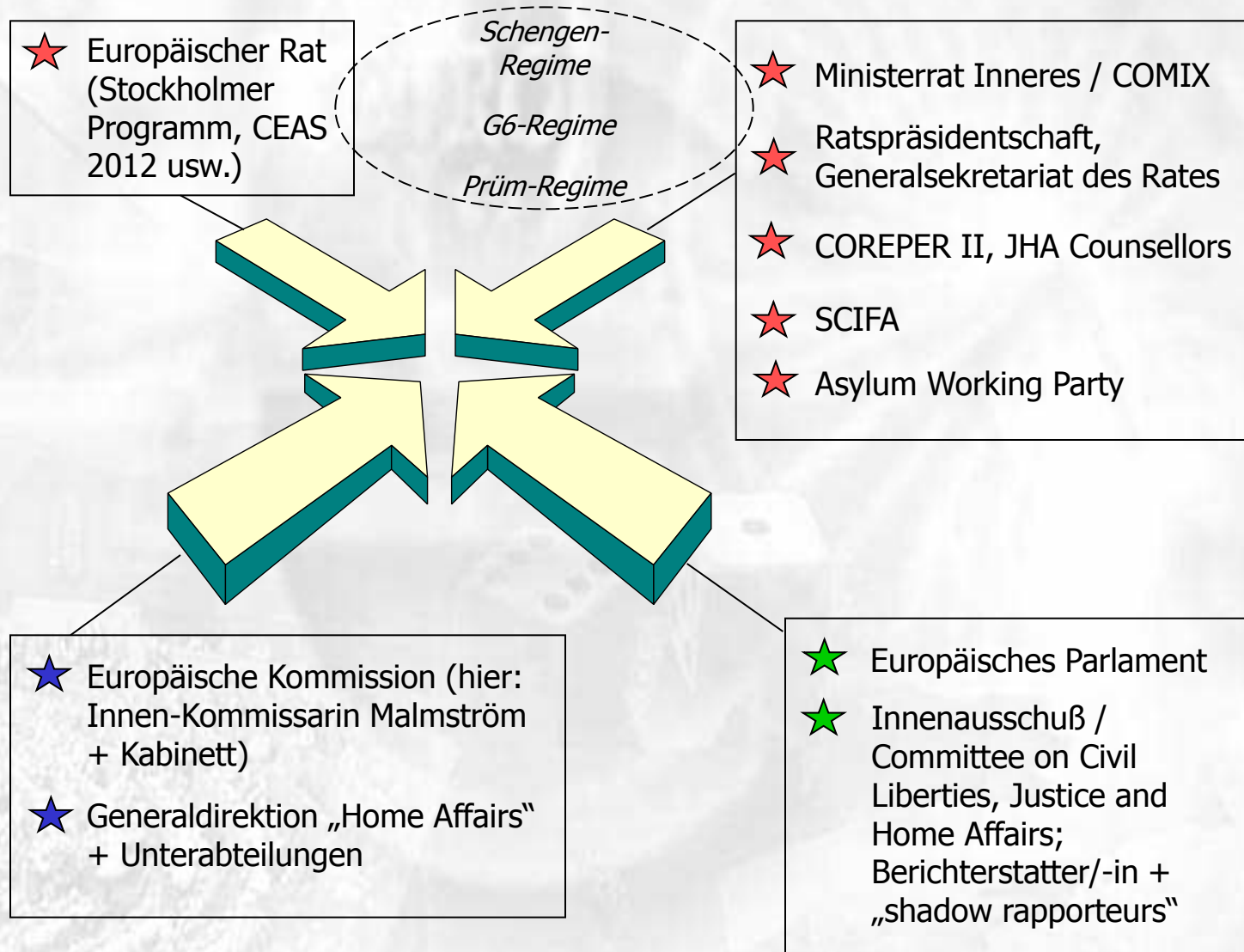
1.2 Entwicklung der Datenbank 2003-2011 und nicht-intendierte Nebenfolgen

- Fingerabdruckdatenbestand der EURODAC-Zentraleinheit steigt bis Ende 2011 auf knapp 2 Millionen Personen (1,995,065; Stand: 31.12.2011)
- Bemerkenswert dabei: nicht „KAT. 1“ / „KAT. 1 gesperrt“-Einträge (FR 317,952 / 0; UK 253,529 / 30,765; DE 247,074 / 14,862; usw.), sondern der vergleichsweise geringe Umfang der „KAT. 2“-Einträge (IT 53,008; ES 5,860; GR 2,904; usw.): Indiz für „Verweigerungshaltung“ und/oder systematische Überforderung von MS wie Griechenland
- Offenbar zunehmendes Problem in einzelnen MS (FR, DK, DE, LU, MT, NL, UK, SE): Selbstverstümmelung bzw. „voluntary mutilations“ / „wilful alteration“ und damit von EURODAC nicht verwertbare Fingerabdrücke. Zahlen für Frankreich 2005: 9% aller Asylantragsteller/-innen, 2011: 14%, insbesondere bei Flüchtlingen aus Somalia (85%) und Eritrea (89%).



2. Empirische Analyse der gegenwärtigen politischen Verhandlungen auf EU-Ebene zu EURODAC 2.0

2.1 Relevante EU-Institutionen: Überblicksdarstellung



2.2 Treibende Mitgliedstaaten im Rat (und außerhalb des Rates)

- Initiatoren des polizeilichen Zugriffs auf EURODAC: G6-Regime der Innenminister DE, FR, UK, IT, ES, PL in Heiligendamm, 22./23. März 2006: Forderung nach „police access to EURODAC and full access of authorities responsible for internal security to the VIS“. Letzteres bereits (seit Oktober 2011) effektiv umgesetzt: polizeilicher Zugriff auf das Visa-Informationssystem (VIS) „für Datenabfragen zum Zwecke der Verhütung, Aufdeckung und Ermittlung terroristischer und sonstiger schwerwiegender Straftaten“ (Ratsbeschuß vom 23. Juni 2008). Zu EURODAC bislang lediglich Schlußfolgerungen des Rates vom 19. Juni 2007: „Council Conclusions on Access to Eurodac by Member States' Police and Law Enforcement Authorities as well as Europol“ und besagter Kommissionsvorschlag.
- Enge politische und auch rechtliche (vgl. Art. 20 EURODAC-Vorschlag KOM 2012) Verbindung zum Vertrag vom Prüm („Schengen III“) vom 27. Mai 2005 (DE, FR, ES, AT, BENELUX) zum Austausch von DNA und Fingerabdrücken bzw. zum entsprechenden Ratsbeschluss vom 23. Juni 2008 „zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität“: Polizeilicher EURODAC-Abgleich („hit“/„no hit“) vermutlich erst, wenn Prüm-Abgleich(e) ergebnislos („no hit“).

2.3 Umsetzung von Prüm / Schengen III (Stand: 12.10.2012) [Anlage 2]

a) FINGERABDRÜCKE / Vernetzung nationaler AFIS

- Bislang noch *keine* technische Umsetzung in 16 von 27 Mitgliedstaaten!
- Vorreiter der Umsetzung hingegen: Österreich (10 von 27). Umsetzung zudem in: Bulgarien (10), Deutschland (8), Slowakei (7), Frankreich (6), Luxemburg (6), Litauen (5), Slowenien (5), Spanien (4), Niederlande (4), Tschechische Republik (3).

Vgl. dazu wiederum die intergouvernementalen *Verhandlungen* zu Eurodac 2.0, z.B. Asylum Working Party 12. Juli 2012: „AT suggested expanding the scope of the [EURODAC] proposal in order to cover all crimes and entered a reservation on all the relevant provisions. ... FI, AT oppose the obligation to have national and Prüm comparisons as a precondition for the EURODAC comparison.“ [Anlage 3; vgl. Anlage 4 zu COREPER II]

b) DNA / Vernetzung nationaler DNA-Datenbanken wie der vom BKA betriebenen „DNA-Analyse-Datei“

- Bislang noch *keine* technische Umsetzung in 14 von 27 Mitgliedstaaten!
- Vorreiter der Umsetzung hingegen erneut: Österreich (13 von 27). Umsetzung zudem in: Niederlande (12), Deutschland (9), Frankreich (9), Spanien (9), Rumänien (9), Slowenien (9), Lettland (8), Slowakei (8), Luxemburg (7), Litauen (5), Bulgarien (4), Finnland (4).

2.4 Verhandlungstaktiken der Europäischen Kommission

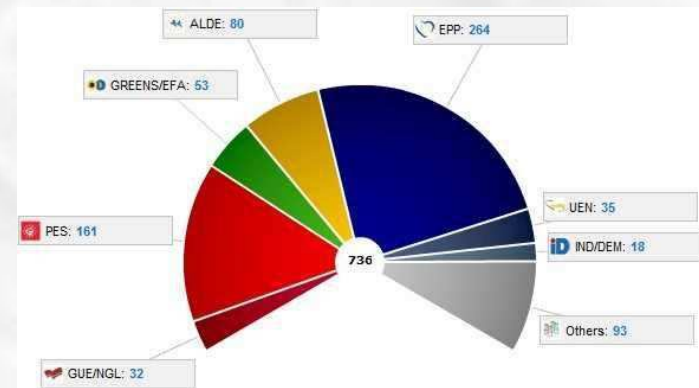
„Um [die] Verhandlungen über das Asylpaket voranzubringen und eine Einigung über die EURODAC-Verordnungen erzielen zu können, war es im Jahr 2010 nach Ansicht der Kommission sinnvoller, diejenigen Bestimmungen aus dem Vorschlag [vom September 2009] für eine EURODAC-Verordnung zu streichen, die sich auf den EURODAC-Zugang zu Strafverfolgungszwecken beziehen. (...) Inzwischen ist jedoch 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, damit die Verhandlungen bis Ende 2012 abgeschlossen werden können“ (Kommission 2012: 3).

- Keine klare Linie der Kommission erkennbar, lediglich machtpolitischer Opportunismus gegenüber dem Rat!
- Polizeilicher Zugriff auf EURODAC als „Preis“ für „package deals“ bzw. politische Einigungen in anderen Bereichen (Verfahrens- und Aufnahme-Richtlinien, Dublin II-Verordnung), aus Sicht der Kommission insbesondere auch für „Fortschritte“ im Bereich der neuen *EU Agency for large-scale IT systems* (für das „Management“ von zunächst nur EURODAC, VIS und SIS II)

2.5 Worum geht es der befürwortenden "konservativen" Mehrheit im Europäischen Parlament?

Gegenwärtige Machtverhältnisse im Europäischen Parlament: *Europäische Volkspartei (EVP/EPP)* als dominierende politische Kraft (ca. 36% Stimmenanteil)

Exemplarisch dazu MEP Hubert Pirker, Sicherheitssprecher der ÖVP (AT) im Europäischen Parlament: „Wir wollen, dass nationale Polizei und Europol die schon gespeicherten Daten zur Verfolgung bereits begangener schwerer Verbrechen nutzen können. ... Wir haben die Daten. Wenn der Datenschutz gesichert ist, sollten wir sie auch zur Kriminalitätsbekämpfung nutzen können. [Alles andere ist eine] groteske Realitätsverweigerung der Linken“ (Pressemitteilung vom 12.10.2012).



Vgl. auch die Begründung von EURODAC-Berichterstatterin Macovei (EVP RO): „Organised crime networks from third countries seek to abuse the asylum system to bring criminal members of a network into an EU Member State as contacts for their criminal business. Once within the territory of an EU Member State, these members of the organised crime network ask for asylum with false identities in order to get a legitimate stay in the EU without any criminal record“ (2012: 20) [Anlage 5].

2.6 Worum geht es der skeptischen aber letztlich kompromissbereiten "sozial-liberalen" Minderheit/Mehrheit im Europäischen Parlament?

- EURODAC-Änderungsanträge der Liberalen, hier: „shadow rapporteur“ Baroness Sarah Ludford (UK LibDem), vertreten durch Nils Torvalds: „We do need considerably greater safeguards than in the Commission proposal. ... The police should have grounds to believe that searches within the context of a specific investigation have a chance to be successful given the circumstances of the case. Just saying that there exists a security risk and that all available databases should have been gone through is not good enough ...“ (Stellungnahme LIBE 26.11.2012).
- EURODAC-Änderungsanträge der Sozialdemokraten, hier: „shadow rapporteur“ Claude Moraes (UK Labour), vertreten durch Birgit Sippel: „From the amendments I think it becomes clear that we have real concerns at least on one issue, which is access to EURODAC by law enforcement authorities. Nevertheless, if, and I underline this, if law enforcement access was to be allowed, we have some additional concerns: ... the issue of latent fingerprints, the transfer of data to third countries, and of course information to asylum seekers on what will or could happen with their data“ (Stellungnahme LIBE 26.11.2012).

2.7 Worum geht es der ablehnenden "grün-linken" Minderheit im Europäischen Parlament?

- EURODAC-Änderungsanträge der Grünen, hier: „shadow rapporteur“ Franziska Keller (DE Grüne): „[Der polizeiliche Zugriff auf EURODAC] leistet einer Stigmatisierung von Asylbewerbern und –bewerberinnen Vorschub. [Er] stellt sie in eine Ecke mit Schwerverbrechern und Terroristen. ... Menschen, die in Europa Schutz vor Verfolgung suchen, werden unter den Generalverdacht gestellt, potentielle Straftäter zu sein“ (Pressemitteilung vom 26.10.2012). „Der Polizeizugriff auf die Fingerabdrücke von AsylbewerberInnen ist ein unverhältnismäßiger Eingriff in die Datenschutzrechte und eine Zweckentfremdung von EURODAC. ... Wir Grüne werden alles versuchen, um das zu verhindern“ (www.ska-keller.de, 27.11.2012)
- EURODAC-Änderungsanträge von Linken wie Cornelis de Jong, stellvertretend für MEP Cornelia Ernst (DE Linke): Kommentarlos Streichung aller Bestimmungen zum polizeilichen Zugriff auf EURODAC. Linke MEPs in entsprechender LIBE-Ausschußsitzung vom 26.11.2012 jedoch nicht anwesend / keine Wortmeldungen.

Vgl. Anlage 6 zu den Änderungsanträgen; Videomitschnitt der LIBE-Sitzung vom 26.11.2012 unter www.europarl.europa.eu/ep-live/;
Abstimmung im LIBE-Ausschuss zur Verhandlungsposition des EP gegenüber Rat und Kommission am 17./18. Dezember 2012

2.8 Verhandlungspartner/-innen im Rahmen der bevorstehenden EURODAC-„Trilogues“



Ioannis Papageorgiou

Rat der Europäischen Union
Vorsitzender der Asylum Working Group
während der zypriotischen
Ratspräsidentschaft (bis Ende 2012)



Matthias Oel

Europäische Kommission
DG Home Affairs
Head of Unit B2/Asylum

ZIELSETZUNG:
Möglichst zeitnahe
informelle inter-
institutionelle politische
Einigung über das
„Asylpaket“ (einschließlich
der EURODAC-
Verordnung)



Monica Luisa Macovei

MEP, EVP
EURODAC-Berichterstatlerin



3. Kritik von Datenschutzbeauftragten, Rechtsanwaltsverbänden, Akademikern und Flüchtlingschutzorganisationen an EURODAC 2.0

3.1 Europäischer Datenschutzbeauftragter und Bundesrechtsanwaltskammer

- Stellungnahme des Europäischen Datenschutzbeauftragten, Peter Hustinx, vom 5. September 2012: „Nur weil die Daten bereits gesammelt worden sind, sollten sie nicht für einen anderen Zweck verwendet werden, da dies einen weitreichenden negativen Effekt auf das Leben von Einzelnen haben kann. Ein solcher Eingriff in die Privatsphäre von Einzelnen und das damit verbundene Risiko der Stigmatisierung verlangen eine starke Rechtfertigung. Die Kommission hat einfach keine ausreichenden Gründe vorgelegt, warum Asylsuchende für eine solche Behandlung ausgesondert werden sollten“.
- Stellungnahme der Bundesrechtsanwaltskammer, November 2012: „Die Erhebung der Daten im Asylprozess und deren sachfremde Verwendung dürfte im Hinblick auf Art. 2 Abs. 1 GG bzw. Art. 7 und Art. 8 der Europäischen Grundrechte Charta (GRC) problematisch sein und ebenso gegen Art. 3 Abs. 1 GG bzw. Art. 20 GRC verstoßen. ... Es bestehen erhebliche Bedenken, dass die Änderungen der EUODAC-Verordnung einer verfassungsgerichtlichen Überprüfung standhalten und der besonderen Schutzbedürftigkeit diese sensiblen Personengruppe gerecht werden“.

[Anlagen 7 und 8]

3.2 Meijers Committee

- Stellungnahme des Meijers Committee – Standing committee of experts on international immigration, refugee and criminal law vom 10. Oktober 2012: „The proposal to give law enforcement authorities and Europol access to Eurodac will change this database into a criminal law investigation tool which is contrary to the limited purpose of this system. ... [The] necessity and proportionality of access for law enforcement authorities and Europol have not been demonstrated. ... The Meijers Committee strongly opposes this access to law enforcement authorities, because it breaches fundamental rights of asylum seekers, including their right to privacy and data protection, the right to asylum and protection against torture and inhuman treatment. Furthermore, the extended use of Eurodac data involves the risk of stigmatisation of a particular group of persons, namely asylum seekers“.

[Anlage 9]

3.3 UNHCR

- Stellungnahme des UNHCR, Bureau for Europe, November 2012: „In UNHCR's view, this [legislative proposal] may not only lead to interference with the right to privacy and family life of asylum-seekers and refugees, but it may also place a refugee and his/her family at significant risk of harm, if the information is shared with countries of origin. It may also result in stigmatisation of asylum-seekers as a group by associating them with criminal activity. ... This increased exposure of asylum-seekers to investigation, simply because their fingerprints are in an accessible database, could fuel misperceptions that there is a link between asylum-seekers and crime, and feed xenophobia and racism. ... UNHCR recalls that many persons in need of international protection ... may have suffered persecution, violence and human rights abuses inflicted by authorities in their countries of origin. In some cases, this may have been at the hands of police. Increased scrutiny by law enforcement authorities may therefore cause disproportionate pressure and potentially harm to people whose data is available, although they are not suspected or not charged with any crime“.

[Anlage 10]




4. Fazit

- Biometrie-bezogene politische Diskurse um Sicherheit und Grenzen auf EU-Ebene lassen sich teilweise durchaus nach dem gängigen Links/Rechts- bzw. GAL/TAN-Schema einordnen (vgl. Abschnitte 2.5 – 2.7 zum EP), doch vieles bleibt aus dieser Sicht leider auch im Dunklen.
- Unterbelichtet bleiben dabei insbesondere die neuen Möglichkeiten des „venue-shopping“ für polizeilich-sicherheitspolitische exekutive Akteure innerhalb und außerhalb des institutionellen Rahmens der EU (vgl. Abschnitte 2.2 – 2.4 zu Rat und Kommission)!
- Unterbelichtet bleibt zudem die aus institutionalistischer Sicht offenkundige Verbindung zwischen institutionellem Kontext (z.B. Datenschutzbeauftragter, Rechtsanwaltsverband, UNHCR – vgl. Abschnitt 3) und konkreter rechtspolitischer Stellungnahme (im Erfolgsfalle: legislativem „output“) getreu dem kognitionspsychologischen Motto: „If the only tool you have is a hammer, you tend to see every problem as a nail!“

- Identitätsbezogene Frage „Wer bin ich?“ aus institutionalistischer Sicht also zunächst stets beantwortet mit „Ich bin ein Polizist“ [„eine Hochschullehrerin“, „ein Datenschützer“, „eine Ärztin“ usw.] (institutionelle *hardware*) – und der sich anschließenden Handlungsmaxime: „Verhalte Dich so, wie sich ein Polizist [„eine Hochschullehrerin“, „ein Datenschützer“, „eine Ärztin“ usw.] in einer Situation wie dieser verhalten sollte!“ (institutionelle *software*). Vgl. dazu March and Olsen: „Much of the behavior we observe in organizations is ‚intuitive‘ in the sense that it occurs immediately upon recognition of a situation. The relevant cognitive and organizational processes are recognition and categorization processes more than they are processes of evaluating consequences“ (1993: 13).

- Europas historische zivilisatorische Errungenschaft besteht sicherlich nicht darin, dass wir unsere Identität aus der Vermessung unserer Körper gewannen, sondern die Ideen von Menschenrechten und Demokratie zu institutionalisieren wussten. Im Sinne einer solchen Identität wäre heute zu fragen, wie wir denjenigen Menschen, die aufgrund von Menschenrechtsverletzungen ihre mutmaßlich undemokratischen Herkunftstaaten verlassen haben bzw. verlassen mussten, in Europa effektiven Schutz gewährleisten können – und wie wir uns auf europäischer Ebene selbst regieren möchten!



Vielen Dank für Ihre / eure Aufmerksamkeit!

5. Anlagenverzeichnis

Anlage 1: Europäische Kommission (2012): *Geänderter Vorschlag – Verordnung des Europäischen Parlaments und des Rates über die Einrichtung von „EURODAC“ für den Abgleich von Fingerabdruckdaten ...*, Kommissions-Dokument COM (2012) 254 final, Brüssel, den 30. Mai 2012.

Anlage 2: Rat der Europäischen Union (2012a): *Note from the Presidency to the Working Group on Information Exchange and Data Protection (DAPIX): Implementation of the Provisions on Information Exchange of the “Prüm Decisions”*, Rats-Dokument 5086/7/12 REV 7, Brüssel, den 12. Oktober 2012.

Anlage 3: Rat der Europäischen Union (2012b): *Outcome of Proceedings of the Asylum Working Party on 12 July 2012*, Rats-Dokument 12207/12, Brüssel, den 26. Juli 2012.

Anlage 4: Rat der Europäischen Union (2012c): *Outcome of Proceedings of the Permanent Representatives Committee (Part II) on 10 October 2012*, Rats-Dokument 14847/12, Brüssel, den 18. Oktober 2012.

Anlage 5: Europäisches Parlament (2012a): *Draft Report on the Amended Proposal for a Regulation ... on the Establishment of ‘EURODAC’ ...*, Committee on Civil Liberties, Justice and Home Affairs, Rapporteur: Monica Luisa Macovei, EP-Dokument PE450.875v03-00, Brüssel und Straßburg, den 26. September 2012.

Anlage 6: Europäisches Parlament (2012b): *Amendments 21 – 182, Draft Report Monica Luisa Macovei (PE450.875v03-00) on the Amended Proposal for a Regulation ... on the Establishment of ‘EURODAC’ ...*, Committee on Civil Liberties, Justice and Home Affairs, EP-Dokument PE500.400v01-00, Brüssel und Straßburg, den 12. November 2012.

Anlage 7: European Data Protection Supervisor (2012): *Opinion of the European Data Protection Supervisor on the Amended Proposal for a Regulation ... on the Establishment of ‘EURODAC’ ...*, Rats-Dokument 13420/12, Brüssel, den 5. September 2012.

Anlage 8: Bundesrechtsanwaltskammer (2012): *Stellungnahme Nr. 47 zum Änderungsvorschlag der Europäischen Kommission vom 30.05.2012 zur EURODAC-Verordnung (COM (2012) 254)*, Berlin und Brüssel, November 2012.

Anlage 9: Meijers-Ausschuss – Ständiger Ausschuss von Experten im internationalen Ausländer-, Flüchtlings- und Strafrecht (2012): *Note on the Proposal for a Regulation on the Establishment of Eurodac (COM (2012) 254)*, Utrecht, den 10. Oktober 2012.

Anlage 10: UNHCR - Der Hohe Flüchtlingskommissar der Vereinten Nationen (2012): *An Efficient and Protective Eurodac: UNHCR Comments on the Commission’s Amended Proposal for a Regulation ... on the Establishment of ‘EURODAC’...*, Bureau for Europe, Brüssel, November 2012.

Anlage 1



EUROPÄISCHE KOMMISSION

Brüssel, den 30.5.2012
COM(2012) 254 final

2008/0242 (COD)

Geänderter Vorschlag

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 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 mit 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

BEGRÜNDUNG

1. HINTERGRUND DES VORSCHLAGS

EURODAC wurde mit der Verordnung (EG) Nr. 2725/2000 über die Einrichtung von „Eurodac“ für den Vergleich von Fingerabdrücken zum Zwecke der effektiven Anwendung des Dubliner Übereinkommens¹ geschaffen. Im Dezember 2008 nahm die Kommission einen Vorschlag für die Neufassung der EURODAC-Verordnung² (nachstehend: Vorschlag vom Dezember 2008) an.

Mit der Neufassung sollte erreicht werden, dass die Anwendung des Dubliner Übereinkommens³ effizienter unterstützt und Datenschutzbelangen gebührend Rechnung getragen wird. Die Neufassung beinhaltete auch die Angleichung des IT-Managementrahmens an den der SIS II- und VIS-Verordnungen, indem sie vorsah, dass die künftige Agentur für das Betriebsmanagement von IT-Großsystemen im Bereich Freiheit, Sicherheit und Recht⁴ (nachstehend: IT Agentur) die Betriebsmanagementaufgaben von EURODAC wahrnimmt. Des Weiteren sah der Vorschlag vom Dezember 2008 die Aufhebung der Durchführungsverordnung und die Übernahme ihres Inhalts in die EURODAC-Verordnung vor. Schließlich wurden Änderungen eingeführt, die den Entwicklungen im Asylbesitzstand und den seit der Annahme der Verordnung im Jahr 2000 erfolgten technischen Fortschritten Rechnung tragen.

Am 3. Dezember 2008 wurde der Vorschlag dem Europäischen Parlament und dem Rat übermittelt. Das Europäische Parlament leitete den Vorschlag an seinen Ausschuss für bürgerliche Freiheiten, Justiz und Inneres weiter. Das Europäische Parlament nahm auf seiner Sitzung vom 7. Mai 2009 eine legislative Entschließung⁵ an, in der es den Kommissionsvorschlag vorbehaltlich einiger Änderungen unterstützte.

Die Kommission nahm im September 2009 einen geänderten Vorschlag an; zum einen sollte damit der Entschließung des Europäischen Parlaments und den Ergebnissen der Verhandlungen im Rat Rechnung getragen, zum anderen sollte der Zugang der Strafverfolgungsbehörden der Mitgliedstaaten und von Europol zur EURODAC-Zentraldatenbank zum Zwecke der Verhütung, Aufdeckung und

¹ ABl. L 62 vom 5.3.2002, S. 1.

² 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 von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist] – KOM(2008) 825 endg.

³ 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, ABl. L 50 vom 25. 2. 2003, S. 1.

⁴ Der Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Errichtung einer Agentur für das Betriebsmanagement von IT-Großsystemen im Bereich Freiheit, Sicherheit und Recht [KOM(2009) 293 endg.] wurde am 24. Juni 2009 angenommen. Am 19. März 2010 wurde ein geänderter Vorschlag angenommen: Geänderter Vorschlag für eine Verordnung (EU) Nr. .../... des Europäischen Parlaments und des Rates zur Errichtung einer Agentur für das Betriebsmanagement von IT-Großsystemen im Bereich Freiheit, Sicherheit und Recht (KOM(2010) 93).

⁵ Einrichtung von „Eurodac“ für den Abgleich von Fingerabdrücken (Neufassung), P6_TA(2009)0378.

Untersuchung terroristischer und sonstiger schwerer Straftaten ermöglicht werden (Vorschlag vom September 2009)⁶.

Mit diesem Vorschlag wurden insbesondere eine sogenannte Brückenklausel und die dazugehörigen Bestimmungen eingeführt, die die Abfrage von EURODAC zu Strafverfolgungszwecken erlauben sollten. Der Vorschlag vom September 2009 wurde zeitgleich mit dem Vorschlag für einen Beschluss des Rates über die Beantragung eines Abgleichs mit EURODAC-Daten durch Strafverfolgungsbehörden der Mitgliedstaaten und Europol zu Strafverfolgungszwecken⁷ (nachstehend: Ratsbeschluss) vorgelegt, in dem die Zugangsmodalitäten für die Strafverfolgungsbehörden im Einzelnen festgelegt sind.

Zu den Vorschlägen vom September 2009 nahm das Europäische Parlament keine legislative EntschlieÙung an.

Mit dem Inkrafttreten des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) und der Abschaffung des Säulensystems wurde der Vorschlag für den Ratsbeschluss hinfällig. Wie in der Mitteilung über die Auswirkungen des Inkrafttretens des Vertrags von Lissabon auf die laufenden interinstitutionellen Beschlussfassungsverfahren⁸ dargelegt, müssen die Vorschläge förmlich zurückgezogen und durch einen neuen Vorschlag ersetzt werden, der den neuen rechtlichen Gegebenheiten des AEUV Rechnung trägt.

Um jedoch die Verhandlungen über das Asylpaket voranbringen und eine Einigung über die EURODAC-Verordnung erzielen zu können, war es im Jahr 2010 nach Ansicht der Kommission sinnvoller, diejenigen Bestimmungen aus dem Vorschlag für eine EURODAC-Verordnung zu streichen, die sich auf den EURODAC-Zugang zu Strafverfolgungszwecken beziehen. Am 11.10.2010 legte die Kommission einen neuen Vorschlag⁹ vor, der sich in weiten Teilen auf den Neufassungsvorschlag von 2008 stützte.

In ihrer Begründung des Vorschlags von 2010 stellte die Kommission fest, dass eine schnellere Annahme der neuen EURODAC-Verordnung auch die rechtzeitige Einrichtung der Agentur für das Betriebsmanagement von IT-GroÙsystemen im Bereich Freiheit, Sicherheit und Recht, die ab dem 1.12.2012 mit der Verwaltung von EURODAC betraut werden soll, erleichtern würde.

Inzwischen ist jedoch 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, damit die Verhandlungen bis Ende 2012 abgeschlossen werden können. Die Kommission hat daher beschlossen, erneut Vorschläge vorzulegen, die den Zugang der Strafverfolgungsbehörden zu EURODAC vorsehen. Dieses Mal hat sie die Vorschläge aber in einer einzigen neuen EURODAC-Verordnung zusammengefasst, da dies seit dem Inkrafttreten des AEUV möglich ist. Zudem ist die Vorlage eines einzigen Rechtsakts bessere legislative Praxis.

Nach 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-

⁶ Der Rat hatte in seinen Schlussfolgerungen vom 12./13. Juni 2007 über den Zugang der Polizei- und Strafverfolgungsbehörden sowie von Europol zu EURODAC einen solchen Vorschlag gefordert.

⁷ KOM(2009) 344.

⁸ KOM(2009) 665 endg./2.

⁹ KOM(2010) 555 endg.

Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts nimmt die Agentur diejenigen Aufgaben im Zusammenhang mit EURODAC wahr, die der Kommission als der für das Betriebsmanagement von EURODAC zuständigen Behörde im Einklang mit der Verordnung (EG) Nr. 2725/2000 und der Verordnung (EG) Nr. 407/2002 übertragen worden waren, sowie Aufgaben im Zusammenhang mit der Kommunikationsinfrastruktur, namentlich Kontrolle, Sicherheit des Datenverkehrs und Koordinierung der Beziehungen zwischen den Mitgliedstaaten und dem Betreiber. Die Agentur sollte die ihr übertragenen Aufgaben wahrnehmen und die einschlägigen Bestimmungen der Verordnung (EU) Nr. 1077/2001 sollten entsprechend angepasst werden. Außerdem sollte Europol bei Sitzungen des Verwaltungsrats der Agentur Beobachterstatus haben, wenn Angelegenheiten im Zusammenhang mit EURODAC auf der Tagesordnung stehen.

Der Vorschlag von 2010 wird somit zurückgezogen und durch einen neuen Vorschlag ersetzt, der der Entschließung des Europäischen Parlaments und den Ergebnissen der Verhandlungen im Rat Rechnung trägt, den Strafverfolgungsbehörden der Mitgliedstaaten und Europol den Zugang zur EURODAC-Zentraldatenbank zum Zwecke der Verhütung, Aufdeckung und Untersuchung terroristischer und sonstiger schwerer Straftaten ermöglicht und die Verordnung (EU) Nr. 1077/2011, soweit nötig, ändert.

Der Vorschlag behandelt ein strukturelles Informations- und Überprüfungsproblem, das darauf zurückzuführen ist, dass es derzeit kein System gibt, mit dem die Strafverfolgungsbehörden den Mitgliedstaat ermitteln können, der Daten über einen Asylbewerber gespeichert hat. Während die Strafverfolgungsbehörden in der Regel auf die in vielen verschiedenen Datenbanken der Mitgliedstaaten gespeicherten Daten über EU-Bürger zugreifen können, besteht für sie nicht die Möglichkeit, Informationen über Asylbewerber auszutauschen.

Der neue Vorschlag soll sicherstellen, dass die Strafverfolgungsbehörden zum Zwecke der Verhütung, Aufdeckung und Untersuchung terroristischer und sonstiger schwerer Straftaten EURODAC abfragen können. Den Strafverfolgungsbehörden soll die Möglichkeit gegeben werden, den Abgleich von Fingerabdruckdaten mit den Daten in der EURODAC-Zentraldatenbank zu beantragen, wenn sie die Identität eines Verbrechenopfers oder einer Person, die einer schweren Straftat verdächtigt wird, feststellen oder weitere Informationen zu der Person einholen wollen. Da sich anhand von Fingerabdrücken die genaue Identität einer Person feststellen lässt, sind diese als wichtige Informationsquelle zur Verhütung, Aufdeckung und Untersuchung terroristischer und sonstiger schwerer Straftaten generell anerkannt. Auf der Grundlage eines „Treffer/kein Treffer“-Systems wird der ersuchenden Strafverfolgungsbehörde mitgeteilt, ob in der nationalen Datenbank eines anderen Mitgliedstaats Informationen über die Person verfügbar sind. In diesem Fall können mithilfe der bestehenden Instrumente für den Informationsaustausch (z. B. Rahmenbeschluss 2006/960/JI über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten) weitere Informationen über die Person von diesem Mitgliedstaat angefordert werden.

Der Abgleich von Fingerabdruckdaten, die im Besitz der benannten Strafverfolgungsbehörden der Mitgliedstaaten und von Europol sind, mit den in EURODAC gespeicherten Daten wird nur im Einzelfall bei dringendem Bedarf eines derartigen Abgleichs und unter genau festgelegten Bedingungen möglich sein. Die Bestimmungen für den Datenzugang und die Datensicherheit regeln auch den Datenzugang zu Strafverfolgungszwecken. Um diese zusätzliche Zweckbestimmung aufzunehmen, bedarf es einer Änderung der EURODAC-Verordnung.

Allgemeiner Kontext

Im Haager Programm ist festgelegt, dass der grenzüberschreitende Datenaustausch zwischen den Strafverfolgungsbehörden u. a. durch Ausweitung des Zugangs zu den bestehenden Datenbanken der Europäischen Union zu verbessern ist. Im Stockholmer Programm wurden eine gezielte Datenerhebung und die den Anforderungen der Strafverfolgung entsprechende Weiterentwicklung des Informationsaustauschs und der dazugehörigen Instrumente angemahnt.

Der gemischte Ausschuss des Rates „Justiz und Inneres“ forderte die Kommission in seinen Schlussfolgerungen vom 12./13. Juni 2007 zur möglichst raschen Vorlage von Vorschlägen zur Verwirklichung des Ziels auf, den Strafverfolgungsbehörden der Mitgliedstaaten und Europol unter bestimmten Voraussetzungen Zugang zu EURODAC zu gewähren, um sie bei ihrer Arbeit im Zusammenhang mit der Verhütung, Aufdeckung und Untersuchung terroristischer und sonstiger schwerer Straftaten zu unterstützen.

Die Auswirkungen des in dem geänderten Vorschlag vorgesehenen EURODAC-Zugangs zu Strafverfolgungszwecken wurden in einer dem Vorschlag beigefügten Folgenabschätzung untersucht.

Der Vorschlag ändert auch die Verordnung (EU) Nr. 1077/2011 (die Agentur-Verordnung) dahingehend, dass sie an die vorliegende Verordnung angeglichen wird.

2. KOHÄRENZ MIT ANDEREN POLITIKBEREICHEN

Dieser Vorschlag steht in jeder Hinsicht im Einklang mit dem Haager Programm von 2004, dem Stockholmer Programm von 2009, dem Europäischen Pakt zu Einwanderung und Asyl, den der Europäische Rat auf seiner Tagung vom 15./16. Oktober 2008 gebilligt hat, und der Grundrechte-Charta der Europäischen Union, insbesondere mit dem Recht auf Asyl und auf Schutz personenbezogener Daten.

Darüber hinaus entspricht dieser Vorschlag inhaltlich der Mitteilung der Kommission an den Rat und das Europäische Parlament über die Verbesserung der Effizienz der europäischen Datenbanken im Bereich Justiz und Inneres und die Steigerung ihrer Interoperabilität sowie der Synergien zwischen ihnen.¹⁰ Wie der Rat und die Strafverfolgungsorgane feststellten, stellt der Umstand, dass die für die innere Sicherheit zuständigen Behörden weder Zugriff auf VIS, die einwanderungsbezogenen Daten des SIS II noch auf EURODAC-Daten haben, einen ernsthaften Mangel bei der Identifizierung von Personen dar, die terroristischer oder sonstiger schwerer Straftaten verdächtigt werden. In der Folge dieser Mitteilung aus dem Jahre 2005 wurde der VIS-Beschluss erlassen, um den Zugang der Strafverfolgungsbehörden und von Europol zu dieser Datenbank zu gewährleisten.

3. EINHALTUNG DER GRUNDRECHTE-CHARTA

Die Achtung der Grundrechte ist gesetzlich vorgeschrieben und wird durch den Europäischen Gerichtshof kontrolliert. Die Organe, Einrichtungen, Ämter und Agenturen der Europäischen Union und ihrer Mitgliedstaaten sind bei der Anwendung des Unionsrechts zur Einhaltung der EU-Grundrechte-Charta verpflichtet, die in gleicher Weise rechtsverbindlich ist wie die Verträge. Die Achtung der Grundrechte ist eine Voraussetzung für die Rechtmäßigkeit des Handelns der EU. Bei der Ausarbeitung des Vorschlags wurden die Auswirkungen auf die Grundrechte umfassend berücksichtigt,

¹⁰ KOM(2005) 597.

um sicherzustellen, dass der Vorschlag im Einklang mit den durch die Charta geschützten Grundrechten steht. In der Folgenabschätzung zu dem Vorschlag wurde umfassend geprüft, ob das Recht auf Asyl und das Recht auf den Schutz personenbezogener Daten gebührend berücksichtigt ist¹¹.

Aufgrund der Änderungen der Verordnungsbestimmungen, die sich auf die Information der Asylbewerber über die Anwendung des Dublin-Systems beziehen, können die Asylbewerber ihr Recht auf Asyl gemäß Artikel 18 der Charta wirksam geltend machen. Die neue Bestimmung, der zufolge die Mitgliedstaaten in der EURODAC-Datenbank angeben müssen, dass sie die Ermessensklauseln der Dublin-Verordnung anwenden, erleichtert die Kommunikation zwischen den Mitgliedstaaten und schafft für die Asylbewerber Klarheit darüber, welcher Mitgliedstaat für die Bearbeitung ihres Falls zuständig ist. Was die besondere Situation von internationalen Schutz suchenden Personen anbelangt, wurden dahingehend Bedenken geäußert, dass Daten, die zwecks Strafverfolgung in EURODAC abgefragt werden, in den Besitz von Ländern gelangen könnten, aus denen die Antragsteller geflohen sind und von denen sie Verfolgung befürchten. Dies könnte nachteilige Auswirkungen auf die Antragsteller, ihre Familienangehörigen und Freunde haben und Flüchtlinge davon abhalten, förmlich um internationalen Schutz nachzusuchen. Diese Überlegung führte dazu, dass der Vorschlag um das Verbot ergänzt wurde, im Einklang mit diesem Vorschlag abgefragte personenbezogene Daten an Drittstaaten, Organisationen oder private Stellen weiterzugeben. Des Weiteren ist ein umfassendes Verfahren zur Kontrolle und Evaluierung des Vorschlags vorgesehen. Im Rahmen der Evaluierung wird bewertet, ob die Datenabfrage zu Strafverfolgungszwecken zur Stigmatisierung von um internationalen Schutz nachsuchenden Personen geführt hat. Somit wird das in Artikel 18 der Charta garantierte Recht auf Asyl durch den Vorschlag nicht eingeschränkt.

Im Hinblick auf den Schutz personenbezogener Daten gemäß Artikel 8 der Charta sorgt der Vorschlag dafür, dass die Löschung der Daten wirksam überwacht wird. Dadurch wird sichergestellt, dass Daten nicht länger als zu dem Zweck der Erhebung erforderlich in einer Form aufbewahrt werden, die die Identifizierung der betroffenen Person ermöglicht. Aus diesem Grund wird auch die Aufbewahrungszeit für Daten von Drittstaatsangehörigen oder Staatenlosen, deren Fingerabdrücke im Zusammenhang mit dem illegalen Überschreiten einer Außengrenze abgenommen wurden, dem Zeitraum angeglichen, für den die Dublin-Verordnung die Zuständigkeit auf der Grundlage dieser Information zuweist.

Der Abgleich mit EURODAC-Daten zum Zwecke der Verhütung, Aufdeckung oder Untersuchung terroristischer oder sonstiger schwerer Straftaten stellt eine Einschränkung des Rechts auf den Schutz personenbezogener Daten da, da die Daten ursprünglich nicht zu diesem Zweck erhoben wurden und EURODAC nicht hierfür eingerichtet wurde. Darüber hinaus enthält EURODAC Daten von Einzelpersonen, die in der Regel nicht einer Straftat verdächtigt werden.

Die Nutzung der EURODAC-Daten zu Strafverfolgungszwecken bedeutet eine Änderung der Zweckbestimmung der verarbeiteten Daten und stellt einen „Eingriff“ in das Recht auf Datenschutz dar.¹² In Artikel 52 Absatz 1 der Grundrechte-Charta ist festgelegt, dass jede Einschränkung des Rechts auf den Schutz personenbezogener Daten gesetzlich vorgesehen sein und den Wesensgehalt dieses Rechts achten muss. Unter Wahrung des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen nur vorgenommen werden, wenn sie erforderlich sind und den von der Union anerkannten, dem

¹¹ Siehe Seiten 15 und 16 und S. 57 der Folgenabschätzung zum Vorschlag von 2009, SEK(2009) 936.

¹² Siehe Bezugnahme auf „Eingriff“ im Urteil des EuGH vom 20. Mai 2003, Österreichischer Rundfunk und andere. Verbundene Rechtssachen C-465/2000, C-138/01 und C-139/01, Slg. 2003, I-4989, Rn. 83.

Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen.

Rechtsvorschriften, die eine derartige Einschränkung vorsehen, müssen so präzise formuliert sein, dass der Einzelne sein Verhalten danach ausrichten kann; sie müssen den Einzelnen vor Willkür schützen und den Ermessensspielraum, den die zuständigen Behörden haben, und die Art und Weise, wie dieser genutzt werden darf, ganz klar festlegen.¹³ Die Verhütung, Aufdeckung, Untersuchung terroristischer oder anderer schwerer Straftaten trägt zum Aufbau eines Raums der Freiheit, der Sicherheit und des Rechts bei und wird von der Union gemäß Artikel 3 Absatz 2 EU-Vertrag als im Allgemeininteresse liegendes Ziel anerkannt. Artikel 8 Absatz 2 der Europäischen Menschenrechtskonvention erkennt zudem an, dass ein Eingriff einer Behörde in das Recht auf Privatsphäre im Interesse der nationalen oder öffentlichen Sicherheit oder zur Verhütung von Straftaten gerechtfertigt sein kann. Der Vorschlag ermöglicht es den zuständigen Strafverfolgungsbehörden, effizienter und mit weniger Eingriffen festzustellen, ob ein anderer Mitgliedstaat im Besitz von Asylbewerber-Daten ist. Nach den derzeitigen Vorschriften müssen die Strafverfolgungsbehörden der Mitgliedstaaten alle an EURODAC beteiligten Mitgliedstaaten kontaktieren, um festzustellen, ob ein anderer Mitgliedstaat Daten zu einem bestimmten Asylbewerber gespeichert hat. Dieses ineffiziente Vorgehen zur Aufklärung von Straftaten nach den derzeitigen Vorschriften erfordert, dass die Strafverfolgungsbehörden auf mehr personenbezogene Daten oder auf Daten von mehr Personen zugreifen als nötig, um festzustellen, ob die betreffenden Informationen existieren.

Der Vorschlag sieht wirksame Schutzklauseln für die Einschränkung des Rechts auf den Schutz personenbezogener Daten vor. Für den Abgleich von EURODAC-Daten zu Strafverfolgungszwecken ist ein zweistufiger Ansatz vorgesehen: Der Abgleich darf erst durchgeführt werden, nachdem eine Überprüfung nach den Prüm-Kriterien gemäß dem Ratsbeschluss 2008/615/JI durchgeführt wurde und nachdem diese Überprüfung keine Treffer ergeben hat. Das bedeutet, dass Mitgliedstaaten, die den Ratsbeschluss 2008/615/JI nicht umgesetzt haben, nicht befugt sind, EURODAC-Abfragen zu Strafverfolgungszwecken durchzuführen.

Darüber hinaus darf der Abgleich mit EURODAC-Daten zu Strafverfolgungszwecken nur dann durchgeführt werden, wenn er für die Verhütung, Aufdeckung oder Untersuchung terroristischer oder sonstiger schwerer Straftaten erforderlich ist und einem der im Rahmenbeschluss 2002/475/JI zur Terrorismusbekämpfung und im Rahmenbeschluss 2002/584/JI über den Europäischen Haftbefehl genannten Fälle entspricht. Dies schließt zum einen den Abgleich mit EURODAC-Daten bei Straftaten, die keine schweren Straftaten sind, aus; zum anderen erlaubt es keinen systematischen oder Massen-Datenabgleich. Darüber hinaus dürfen die benannten Strafverfolgungsbehörden den Abgleich mit EURODAC-Daten nur beantragen, wenn berechtigte Gründe zu der Annahme bestehen, dass die Abfrage von EURODAC-Daten wesentlich zur Verhütung, Aufdeckung oder Untersuchung einer der genannten Straftaten beitragen würde. Nach Eingang eines Antrags einer benannten Strafverfolgungsbehörde überprüft eine Prüfstelle, ob die strengen Bedingungen für die Beantragung eines Abgleichs mit den EURODAC-Daten zu Strafverfolgungszwecken erfüllt sind. Wenn die Prüfstelle dem Antrag stattgibt, übermittelt sie ihn an die nationale Zugangsstelle, die ihn ihrerseits an das EURODAC-Zentralsystem weiterleitet. Die Mitgliedstaaten dürfen nicht systematisch und routinemäßig Abfragen durchführen. Als zusätzliche Sicherung sieht der Vorschlag in Bezug auf die Behörden, die zu einer EURODAC-Abfrage befugt sind, ein dreistufiges Vorgehen vor. Der Abgleich mit EURODAC-Daten zu Strafverfolgungszwecken erfolgt auf der Grundlage eines „Treffer/kein

¹³ Miteinander verbundene Anträge 30562/04 und 30566/04, *S. und Marper gg. Vereinigtes Königreich*, Urteil vom 4. Dezember 2008.

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.

Des Weiteren legt der Vorschlag strikte Sicherheitsmaßnahmen zur Gewährleistung des Schutzes der verarbeiteten personenbezogenen Daten fest. Er sieht vor, dass die Datenverarbeitung durch unabhängige Datenschutzbehörden überwacht und sämtliche Abfragen schriftlich festgehalten werden. Ferner ist festgelegt, dass die Verarbeitung sämtlicher personenbezogener Daten aus der EURODAC-Datenbank durch Strafverfolgungsbehörden den Bestimmungen des Rahmenbeschlusses des Rates 2008/977/JI unterliegt.

Einzelpersonen sollte das Recht auf Auskunft, Berichtigung und Rechtsschutz eingeräumt werden, insbesondere das Recht auf einen gerichtlichen Rechtsbehelf. Die Überwachung der Datenverarbeitung durch unabhängige Behörden sollte gewährleistet sein. Der Europäische Datenschutzbeauftragte (zuständig für die Verarbeitung der EURODAC-Daten) und nationale Datenschutzbehörden werden die Einhaltung der Datenschutzvorschriften überwachen und gegebenenfalls durchsetzen. Die Einschränkung des Rechts auf Schutz personenbezogener Daten durch den Abgleich mit den EURODAC-Daten gemäß diesem Vorschlag ist mit Schutzklauseln zur Gewährleistung der Achtung der Grundrechte verbunden.

Asylbewerber-Datenbanken können Fingerabdruckdaten von Minderjährigen ab 14 Jahre enthalten; Kinder in diesem Alter können aber nicht in allen Mitgliedstaaten strafrechtlich zur Verantwortung gezogen werden. Die Mitgliedstaaten müssen gewährleisten, dass die bei der Abfrage dieser Datenbanken erlangten Daten von Kindern, die nach ihrem innerstaatlichen Recht strafrechtlich nicht zur Verantwortung gezogen werden können, auf rechtlich korrekte und nichtdiskriminierende Weise (wie die Daten von Kindern, die Staatsbürger des betreffenden Mitgliedstaats sind) zum Wohl des Kindes verarbeitet werden.

Insofern steht dieser Vorschlag insbesondere im Hinblick auf das Asylrecht (Artikel 18) und den Schutz personenbezogener Daten (Artikel 8) vollständig im Einklang mit der Grundrechte-Charta der Europäischen Union. Der Vorschlag steht auch im Einklang mit Artikel 16 AEUV, wonach jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten hat.

4. ERGEBNISSE DER KONSULTATIONEN DER INTERESSIERTEN KREISE UND DER FOLGENABSCHÄTZUNGEN

Der geänderte Vorschlag führt zu einem alle Bestimmungen des hinfällig gewordenen Ratsbeschlusses von 2009 wieder ein sowie zwei technische Bestimmungen im Zusammenhang mit den Asylbestimmungen. Keine dieser Bestimmungen ist neu¹⁴; sie wurden bereits eingehend in den Folgenabschätzungen zu den Vorschlägen von 2008 und 2009 bewertet. Daher wurde weder eine neue Konsultation noch eine Folgenabschätzung für den vorliegenden Vorschlag durchgeführt. Die Ergebnisse der Folgenabschätzungen von 2008 und 2009¹⁵ gelten für diesen Verordnungsvorschlag gleichermaßen.

¹⁴ Eine dieser Änderungen soll die Vereinbarkeit mit der Dublin-Verordnung gewährleisten, die andere soll das Erfordernis einer Überprüfung des automatischen positiven Abgleichs durch einen Fachmann für Daktyloskopie präzisieren.

¹⁵ SEK(2008) 2981 und SEK(2009) 936.

Die Kommission veröffentlichte im Juni 2007 das Grünbuch über das künftige Gemeinsame Europäische Asylsystem¹⁶, in dem verschiedene Optionen zur weiteren Gestaltung der Dublin- und der EURODAC-Verordnung vorgeschlagen wurden. Im Rahmen einer umfassenden öffentlichen Anhörung zum Grünbuch gingen 89 Beiträge unterschiedlicher Interessengruppen ein.

Die Kommissionsdienststellen diskutierten im März 2008 mit den Mitgliedstaaten im Ausschuss für Einwanderung und Asyl (CIA) sowie im Oktober 2007 und April 2008 bei zwei informellen Expertentreffen mit Angehörigen der Rechtsberufe aus den Mitgliedstaaten das Ergebnis des Bewertungsberichts und die geplanten Änderungen der Verordnung.

Der UNHCR, der Europäische Rat für Flüchtlinge und im Exil lebende Personen (ECRE) und der Europäische Datenschutzbeauftragte (EDSB) wurden ebenfalls während der Arbeiten zur Änderung der Verordnung informell konsultiert.

Während der Ausarbeitung der Vorschläge von 2008 (verbesserte Funktionsweise von EURODAC) und der geänderten Vorschläge von 2009 (Zugang der Strafverfolgungsbehörden zu EURODAC) konsultierte die Kommission die Staaten, die den Dublin-Besitzstand anwenden, d. h. die EU-Mitgliedstaaten, Island, Norwegen und die Schweiz sowie Europol, mit Hilfe von zwei Fragebögen; sie veranstaltete außerdem am 25./26. September 2007 ein Expertentreffen in Brüssel, bei dem die Experten die Antworten auf die Fragebögen und ihre Standpunkte erläutern konnten. Am 8. Oktober 2007 fand in Brüssel eine Anhörung mehrerer zwischenstaatlicher Organisationen, regierungsunabhängiger Organisationen und anderer in den Bereichen Asyl- und Grundrechte tätiger Sachverständigen statt. Die Vertreter der nationalen Datenschutzbehörden der Länder, die den Dublin-Besitzstand anwenden, die Gemeinsame Kontrollinstanz von Europol und der Europäische Datenschutzbeauftragte kamen am 11. Oktober 2007 zu einer Anhörung in Brüssel zusammen. Da Liechtenstein den Dublin-Besitzstand erst seit kurzer Zeit anwendet, bot sich noch nicht die Gelegenheit, Liechtenstein zu diesem Vorschlag zu konsultieren.

Die Folgenabschätzung zu dem Vorschlag von 2009 enthält ein ausführliches Verzeichnis der konsultierten Kreise.

5. RECHTLICHE ASPEKTE DES VORSCHLAGS

Dieser Vorschlag ändert den geänderten Vorschlag der Kommission von 2010 für eine Verordnung des Europäischen Parlaments und des Rates über die Einrichtung von „EURODAC“ für den Abgleich von Fingerabdruckdaten zum Zweck der effektiven Anwendung der Verordnung (EG) Nr. [...] [zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrag auf internationalen Schutz zuständig ist] - (KOM(2010) 555).

Des Weiteren ändert dieser Vorschlag die 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

Bei dem vorliegenden geänderten Vorschlag dient Artikel 78 Absatz 2 Buchstabe e des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) als Rechtsgrundlage für die Kriterien und Verfahren

¹⁶ KOM(2007) 301.

zur Bestimmung des Mitgliedstaats, der für die Prüfung eines in einem Mitgliedstaat gestellten Antrags auf Asyl oder subsidiären Schutz zuständig ist. Dieser Artikel des AEUV entspricht der Rechtsgrundlage des ursprünglichen Vorschlags (Artikel 63 Absatz 1 Buchstabe a des Vertrags zur Gründung der Europäischen Gemeinschaft). Des Weiteren dienen Artikel 87 Absatz 2 Buchstabe a AEUV als Rechtsgrundlage für die Zusammenstellung, Speicherung, Verarbeitung, Auswertung und den Austausch relevanter Daten zu Strafverfolgungszwecken und Artikel 88 Absatz 2 Buchstabe a als Rechtsgrundlage für den Tätigkeitsbereich und die Aufgaben von Europol, einschließlich der Sammlung, Speicherung, Verarbeitung, Auswertung und den Austausch von Informationen.

Entsprechend dem Protokoll über die Position des Vereinigten Königreichs und Irlands im Anhang zum Vertrag über die Europäische Union (EU-Vertrag) und zum AEUV gilt Titel V AEUV nicht für das Vereinigte Königreich und Irland, sofern diese beiden Staaten nichts anderes beschließen.

Für das Vereinigte Königreich und Irland ist die Verordnung (EG) Nr. 2725/2000 des Rates bindend, da sie ihren Wunsch mitgeteilt haben, auf der Grundlage des genannten Protokolls an der Annahme und Anwendung dieser Verordnung beteiligt zu werden. Die Position dieser beiden Mitgliedstaaten hinsichtlich der geltenden Verordnung lässt ihre mögliche Beteiligung im Hinblick auf die geänderte Verordnung unberührt.

Nach dem Protokoll über die Position Dänemarks im Anhang zum EU-Vertrag und zum AEUV beteiligt sich dieser Mitgliedstaat nicht an der Annahme von Maßnahmen durch den Rat, die unter Titel V AEUV fallen (dies gilt allerdings nicht für „Maßnahmen zur Bestimmung derjenigen Drittländer, deren Staatsangehörige beim Überschreiten der Außengrenzen der Mitgliedstaaten im Besitz eines Visums sein müssen,“ sowie für „Maßnahmen zur einheitlichen Visumgestaltung“). Dänemark wird sich daher nicht an der Annahme dieser Verordnung beteiligen, die für diesen Mitgliedstaat somit nicht bindend und ihm gegenüber nicht anwendbar ist. Da Dänemark jedoch die derzeitige EURODAC-Verordnung aufgrund eines 2006 mit der EG geschlossenen völkerrechtlichen Abkommens¹⁷ anwendet, muss Dänemark der Kommission gemäß Artikel 3 des Abkommens mitteilen, ob es die geänderte Verordnung inhaltlich umsetzen wird.

Dieser Vorschlag übernimmt die Änderungen des vorherigen Vorschlags in Bezug auf die Abschaffung des in Artikel 22 der Verordnung vorgesehenen Ausschusses.

6. AUSWIRKUNGEN DES VORSCHLAGS AUF AM DUBLIN-SYSTEM BETEILIGTE DRITTSTAATEN

Parallel zu der Assoziierung einiger Nichtmitgliedstaaten der EU am Schengen-Besitzstand hat die Gemeinschaft/EU mehrere Abkommen zur Assoziierung dieser Länder am Dublin-EURODAC-Besitzstand geschlossen bzw. ist im Begriff, solche Abkommen zu schließen:

¹⁷ Abkommen zwischen der Europäischen Gemeinschaft und dem Königreich Dänemark über die Kriterien und Verfahren zur Bestimmung des Staates, der für die Prüfung eines in Dänemark oder in einem anderen Mitgliedstaat der Europäischen Union gestellten Asylantrags zuständig ist, sowie über EURODAC für den Vergleich von Fingerabdrücken zum Zwecke der effektiven Anwendung des Dubliner Übereinkommens (ABl. L 66 vom 8.3.2006).

- Übereinkommen über die Assoziierung Islands und Norwegens von 2001¹⁸;
- Abkommen über die Assoziierung der Schweizerischen Eidgenossenschaft vom 28. Februar 2008¹⁹;
- Protokoll über die Assoziierung Liechtensteins, unterzeichnet am 18. Juni 2011²⁰.

Um zwischen Dänemark, das im Wege eines internationalen Abkommens dem Dublin-EURODAC-Besitzstand assoziiert wurde, und den anderen vorgenannten assoziierten Ländern Rechte und Pflichten zu schaffen, wurden zwei weitere Instrumente zwischen der Gemeinschaft und den assoziierten Ländern geschlossen²¹.

Entsprechend diesen drei Übereinkommen übernehmen die assoziierten Länder den Dublin-EURODAC-Besitzstand und seine Weiterentwicklung uneingeschränkt. Sie nehmen zwar an der Annahme von Rechtsakten, die den Dublin-Besitzstand ändern oder fortentwickeln, nicht teil (d. h. auch nicht an diesem Vorschlag), sie müssen der Kommission aber, sobald das Europäische Parlament und der Rat den Rechtsakt erlassen haben, innerhalb einer bestimmten Frist mitteilen, ob sie diesen Rechtsakt umsetzen. Falls Norwegen, Island, die Schweiz oder Liechtenstein einen Rechtsakt zur Änderung oder Erweiterung des Dublin-EURODAC-Besitzstands nicht annehmen, kommt die „Guillotinenklausel“ zur Anwendung, d.h. die entsprechenden Abkommen treten außer Kraft, es sei denn, der durch die Abkommen eingerichtete gemeinsame/gemischte Ausschuss beschließt einstimmig anders.

Der Zugang der Strafverfolgungsbehörden zu EURODAC-Daten fällt weder unter die genannten Abkommen mit Island, Norwegen, der Schweiz und Liechtenstein noch unter das parallel geschlossene Abkommen mit Dänemark.

Die Kommission stellt in ihrem derzeitigen Vorschlag – wie bereits im Vorschlag von 2009 – fest, dass der Abgleich von Fingerabdruckdaten mit Daten in EURODAC erst zulässig ist, nachdem der Abgleich mit den Daten einer nationalen Fingerabdruck-Datenbank und die Abfrage der automatisierten daktyloskopischen Identifizierungssysteme anderer Mitgliedstaaten gemäß dem Beschluss 2008/615/JI (Beschluss von Prüm) nicht zu einem Treffer geführt hat. Dies bedeutet, dass ein Mitgliedstaat, der den Beschluss von Prüm nicht umgesetzt hat und somit keine Überprüfung nach den Prüm-Kriterien

¹⁸ Übereinkommen zwischen der Europäischen Gemeinschaft, der Republik Island und dem Königreich Norwegen über die Kriterien und Regelungen zur Bestimmung des zuständigen Staates für die Prüfung eines in einem Mitgliedstaat, in Island oder Norwegen gestellten Asylantrags (ABl. L 93 vom 3.4.2001, S. 40).

¹⁹ Abkommen zwischen der Europäischen Gemeinschaft und der Schweizerischen Eidgenossenschaft über die Kriterien und Regelungen zur Bestimmung des zuständigen Staates für die Prüfung eines in einem Mitgliedstaat oder in der Schweiz gestellten Asylantrags (ABl. L 53 vom 27.2.2008, S. 5).

²⁰ Protokoll zwischen der Europäischen Gemeinschaft, der Schweizerischen Eidgenossenschaft und dem Fürstentum Liechtenstein über den Beitritt des Fürstentums Liechtenstein zum Abkommen zwischen der Europäischen Gemeinschaft und der Schweizerischen Eidgenossenschaft über die Kriterien und Verfahren zur Bestimmung des zuständigen Staates für die Prüfung eines in einem Mitgliedstaat oder in der Schweiz gestellten Asylantrags (ABl. L 160 vom 18.6.2011, S. 39).

²¹ Protokoll zwischen der Europäischen Gemeinschaft, der Schweizerischen Eidgenossenschaft und dem Fürstentum Liechtenstein zum Abkommen zwischen der Europäischen Gemeinschaft und der Schweizerischen Eidgenossenschaft über die Kriterien und Verfahren zur Bestimmung des zuständigen Staates für die Prüfung eines in einem Mitgliedstaat oder in der Schweiz gestellten Asylantrags (2006/257 CNS, geschlossen am 24.10.2008, noch nicht im Amtsblatt veröffentlicht) und Protokoll zum Übereinkommen zwischen der Europäischen Gemeinschaft, der Republik Island und dem Königreich Norwegen über die Kriterien und Regelungen zur Bestimmung des zuständigen Staates für die Prüfung eines in einem Mitgliedstaat oder in Island oder Norwegen gestellten Asylantrags (ABl. L 93 vom 3.4.2001).

durchführen kann, auch nicht befugt ist, eine EURODAC-Abfrage zu Strafverfolgungszwecken durchzuführen. Ähnliches gilt für die assoziierten Länder: Wenn sie den Beschluss von Prüm nicht umgesetzt haben oder sich nicht an dem Prümer Vertrag beteiligen, sind sie nicht befugt, eine EURODAC-Abfrage durchzuführen.

7. AUSFÜHRLICHE ERLÄUTERUNG DES VORSCHLAGS

In der Neufassung von 2008 wurde der Begriff der „Sperrung von Daten“ durch den der „Markierung“ gespeicherter Daten von Personen, die internationalen Schutz genießen, ersetzt. In der ursprünglichen Verordnung war vorgesehen, dass die Daten von Personen, die internationalen Schutz genießen, zwar im EURODAC-System gespeichert wurden, aber gesperrt waren. So zeichnete das EURODAC-System die Treffer beim Abgleich von Fingerabdruckdaten von Personen, die internationalen Schutz genießen mit EURODAC-Daten zwar auf, setzte die Mitgliedstaaten aber nicht davon in Kenntnis. Im neuen Vorschlag war vorgesehen, diese Daten zu „markieren“, um die Mitgliedstaaten im Falle eines Treffers informieren zu können. Auf diese Weise sollten die Mitgliedstaaten informiert werden, wenn eine Person, die internationalen Schutz genießt, versucht, einen neuen Asylantrag zu stellen.

Mehrere Änderungen des Vorschlags von 2010 wurden direkt aus dem hinfällig gewordenen Vorschlag von 2009 in Bezug auf den Zugang der Strafverfolgungsbehörden zu EURODAC übernommen. Dieser Abschnitt wurde aufgeteilt in die Bereiche, die den Rest des Vorschlags ändern, und die Änderungen, die sich weitgehend auf den Vorschlag vom September 2009 stützen. Zur Erleichterung des Vergleichs wurden die jeweiligen Artikel aufgeführt.

Folgende Artikel wurden aus dem Vorschlag vom September 2009 übernommen:

Artikel 1 Absatz 2: Festlegung der Bedingungen – übernommen aus Artikel 1 Vorschlag vom September 2009.

Artikel 5: Benennung der Behörden, die zum Zugang zu EURODAC-Daten befugt sind - übernommen aus Artikel 3 des Vorschlags vom September 2009, außer dem Titel, der präziser formuliert wurde.

Artikel 6: Prüfstellen, die dafür Sorge tragen, dass die Bedingungen für die Beantragung eines Abgleichs von Fingerabdruckdaten mit EURODAC-Daten erfüllt sind - übernommen aus Artikel 4 des Vorschlags vom September 2009.

Artikel 7: Europol – übernommen aus Artikel 5 des Vorschlags vom September 2009.

Kapitel VI (Artikel 19-22): Verfahren für den Abgleich und die Übermittlung von Daten zu Strafverfolgungszwecken - übernommen aus den Artikeln 6 bis 9 des Vorschlags vom September 2009.

Artikel 33: Datenschutz, Artikel 34: Datensicherheit, Artikel 35: Verbot der Übermittlung von Daten, Artikel 36: Protokollierung und Dokumentierung - übernommen aus den Artikeln 10 bis 13 des Vorschlags vom September 2009.

Artikel 39 Absatz 3: Kosten im Zusammenhang mit der Verhütung, Aufdeckung oder Untersuchung von Straftaten im Sinne dieser Verordnung – übernommen aus Artikel 14 des Vorschlags vom September 2009.

Artikel 40 Absätze 8 und 9: Vorlage von Jahresberichten über den Zugang der Strafverfolgungsbehörden zu EURODAC-Daten – in geänderter Fassung des Artikels 17 Absätze 1 und 3 des Vorschlags vom September 2009.

Artikel 43: Meldung der benannten Behörden und Prüfstellen – übernommen aus Artikel 16 des Vorschlags vom September 2009.

Folgende Artikel waren weder im Vorschlag vom September 2009 noch im Vorschlag von 2010 enthalten:

Artikel 2 Absatz 1: enthält weitere Definitionen der IT-Agentur und von Europol sowie der terroristischen und sonstigen schweren Straftaten.

Artikel 2 Absätze 2 und 4: legen fest, wann die Richtlinie 95/46/EG und wie der Rahmenbeschluss 2008/977/JI aus Datenschutzgründen anzuwenden sind.

Artikel 29: der Text auf dem Merkblatt wurde so umformuliert, dass er für Asylbewerber verständlich ist.

Kapitel VIII Artikel 38: mehrere Änderungen 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-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts; Artikel 41: die Worte „und Europol“ wurden im Artikel über Sanktionen hinzugefügt.

In der gesamten Neufassung wurden die Bezüge auf die „Verwaltungsbehörde“ ersetzt durch die „Agentur“.

8. AUSWIRKUNGEN AUF DEN HAUSHALT

Der Vorschlag hat eine technische Änderung des EURODAC-Zentralsystems zur Folge, die den Datenabgleich zu Strafverfolgungszwecken ermöglichen soll. Außerdem wird eine neue Funktion vorgeschlagen, die die Abfrage auf der Grundlage von Fingerabdruckspuren ermöglicht.

Der vorliegende Vorschlag übernimmt die Verbesserungen aus dem Vorschlag von 2010, also die neuen Funktionen für Asylangelegenheiten (Informationen über die Rechtsstellung der betroffenen Person, wie in den Verhandlungen im Rat beschlossen). Der dem Vorschlag beigefügte Finanzbogen, der diese Änderungen widerspiegelt, gilt auch für den Vorschlag für einen Beschluss über die Berechtigung der Strafverfolgungsbehörden der Mitgliedstaaten und von Europol, einen Abgleich mit EURODAC-Daten zu Strafverfolgungszwecken zu beantragen [KOM(2009) 344].

Der geschätzte Finanzbedarf von 2 415 Mio. EUR (2 771 Mio. EUR einschließlich der Kosten für Verwaltung und Humanressourcen) würde neben der Systemwartung für einen Zeitraum von drei Jahren auch IT-bezogene Dienste, Software und Hardware sowie die Umrüstung und Anpassung des Systems abdecken, um Abfragen zu Strafverfolgungszwecken und Änderungen an der ursprünglichen Asyl-Zweckbestimmung, die keinen Bezug zum Datenzugang zu Strafverfolgungszwecken aufweist, zu ermöglichen. Der im derzeitigen Finanzbogen veranschlagte Finanzbedarf entspricht weitgehend dem des EURODAC-Vorschlags vom 10. September 2009. Lediglich die Kosten für das Personal in der IT-Agentur wurden geringfügig höher veranschlagt. Angesichts der relativ geringen Gesamtkosten werden weder zusätzliche Ressourcen noch eine Berichtigung des Haushalts für den Bereich Inneres

beantragt werden. Die erforderlichen Mittel werden aus den bestehenden Haushaltslinien (der für die IT-Agentur) oder aus den Haushaltsmitteln für den Bereich Inneres aufgebracht werden.

9. SUBSIDIARITÄTSPRINZIP

Aufgrund des grenzübergreifenden Charakters des Schutzes von Asylbewerbern und Flüchtlingen ist die EU die geeignete Instanz, um im Rahmen des Gemeinsamen Europäischen Asylsystems Lösungen für die genannten Probleme im Zusammenhang mit der EURODAC-Verordnung vorzuschlagen. Obgleich durch die im Jahr 2000 angenommene Verordnung ein hoher Harmonisierungsgrad erreicht wurde, kann die Anwendung der Dublin-Verordnung durch EURODAC noch umfassender unterstützt werden. Es ist deutlich geworden, dass die EU im Hinblick auf die Verwaltung einer EU-Datenbank, die geschaffen wurde, um die Durchführung einer Verordnung über Grenzübertritte von Asylbewerbern zu unterstützen, tätig werden muss.

Es bedarf einer Änderung der EURODAC-Verordnung, um sie um eine zweite Zweckbestimmung zu ergänzen: die Gewährung des Zugangs zu Daten in der EURODAC-Zentraldatenbank zum Zwecke der Bekämpfung terroristischer und sonstiger Straftaten. Eine derartige Änderung kann nur von der Kommission vorgeschlagen werden; dieses Ziel kann daher von den Mitgliedstaaten nicht in ausreichendem Maße verwirklicht werden.

10. GRUNDSATZ DER VERHÄLTNISSMÄßIGKEIT

In den gemeinsam mit den Vorschlägen von 2008 und 2009 veröffentlichten Folgenabschätzungen²² wurden alle Optionen untersucht, um das beste Verhältnis zwischen dem praktischen Nutzen und den notwendigen Anstrengungen zu ermitteln. Es wurde festgestellt, dass die vorgeschlagenen Maßnahmen der EU nicht über das für die Lösung der Probleme erforderliche Maß hinausgehen.

Die Autoren der Folgenabschätzung kamen zu dem Schluss, dass nur durch den Zugang der Strafverfolgungsbehörden zu EURODAC-Daten fristgerecht, präzise, sicher und kostenwirksam festgestellt werden kann, ob – und wenn ja – wo in den Mitgliedstaaten Daten zu Asylbewerbern verfügbar sind. Es gibt keine halbwegs effiziente Alternative zu EURODAC, um die genaue Identität eines Asylbewerbers festzustellen oder zu überprüfen, und die es den Strafverfolgungsbehörden ermöglicht, zum gleichen Ergebnis zu gelangen.

²² SEK(2008) 2981 und SEK(2009) 936.

↓ 2725/2000/EC (angepasst)

⇒ neu

2008/0242 (COD)

Geänderter Vorschlag

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 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 Europols auf den Abgleich mit 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

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION –

~~gestützt auf den Vertrag zur Gründung der Europäischen Gemeinschaft, insbesondere auf Artikel 63 Nummer 1 Buchstabe a) über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 78 Absatz 2 Buchstabe e⇒, Artikel 87 Absatz 2 Buchstabe a und Artikel 88 Absatz 2 Buchstabe a ⇐,~~

auf Vorschlag der Kommission,²³

nach Stellungnahme des Europäischen Datenschutzbeauftragten²⁴,

~~nach Stellungnahme des Europäischen Parlaments,²⁵~~

☒ nach dem ordentlichen Gesetzgebungsverfahren, ☒

in Erwägung nachstehender Gründe:

²³ COM(2012) XXX.

²⁴ ABl. L 92 vom 10.4.2010, S. 1.

²⁵ ~~ABl. C 189 vom 7.7.2000, S. 105 und S. 227 sowie Stellungnahme vom 21. September 2000 (noch nicht im Amtsblatt veröffentlicht).~~

↓ neu

- (1) Die Verordnung (EG) Nr. 2725/2000 des Rates vom 11. Dezember 2000 über die Einrichtung von „Eurodac“ für den Vergleich von Fingerabdrücken zum Zwecke der effektiven Anwendung des Dubliner Übereinkommens²⁶ und die Verordnung (EG) Nr. 407/2002 des Rates vom 28. Februar 2002 zur Festlegung von Durchführungsbestimmungen zur Verordnung (EG) Nr. 2725/2000 über die Einrichtung von „Eurodac“ für den Vergleich von Fingerabdrücken zum Zwecke der effektiven Anwendung des Dubliner Übereinkommens²⁷ müssen in einigen wesentlichen Punkten geändert werden. Aus Gründen der Klarheit empfiehlt sich eine Neufassung der Verordnungen.
-

↓ 2725/2000/EG Erwägungsgrund 1

- ~~(1) Die Mitgliedstaaten haben das Genfer Abkommen vom 28. Juli 1951 über die Rechtsstellung der Flüchtlinge in der Fassung des New Yorker Protokolls vom 31. Januar 1967 ratifiziert.~~
-

↓ 2725/2000/EG Erwägungsgrund 2
(angepasst)

- ~~(2) Die Mitgliedstaaten haben am 15. Juni 1990 in Dublin das Übereinkommen über die Bestimmung des zuständigen Staates für die Prüfung eines in einem Mitgliedstaat der Europäischen Gemeinschaften gestellten Asylantrags (nachfolgend: Dubliner Übereinkommen) geschlossen.~~
-

↓ neu

- (2) Eine gemeinsame Asylpolitik, einschließlich eines Gemeinsamen Europäischen Asylsystems, ist wesentlicher Bestandteil des Ziels der Europäischen Union, schrittweise einen Raum der Freiheit, der Sicherheit und des Rechts aufzubauen, der allen offen steht, die wegen besonderer Umstände rechtmäßig in der Union um internationalen Schutz nachsuchen.
- (3) Der Europäische Rat nahm auf seiner Tagung vom 4. November 2004 das Haager Programm an, das die Ziele im Bereich des Raums der Freiheit, der Sicherheit und des Rechts für den Zeitraum 2005-2010 vorgibt. Auf seiner Tagung vom 15./16. Oktober 2008 nahm der Europäische Rat den Europäischen Pakt über Einwanderung und Asyl an, der die Vollendung der Einführung eines Gemeinsamen Europäischen Asylsystems durch Schaffung eines einheitlichen Asylverfahrens mit gemeinsamen Garantien und einem einheitlichen Status für Flüchtlinge und Personen, die subsidiären Schutz genießen, fordert.

²⁶ ABl. L 316 vom 15.12.2000, S. 1.

²⁷ ABl. L 62 vom 5.3.2002, S. 1.

↓ 2725/2000/EG Erwägungsgrund 3
(angepasst)
⇒ neu

- (4) ~~Zum Zwecke der~~ Die Anwendung ~~des Dubliner Übereinkommens~~ ☒ der Verordnung (EU) Nr. [...] [zur 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,]²⁸ ☒ ~~ist es erforderlich, setzt voraus, dass die Identität von der Asylbewerbern~~ ⇒ Personen, die internationalen Schutz beantragen, ☐ und ~~der Personen festzustellen, die in Verbindung mit dem beim~~ rechtswidrigen Überschreiten der Außengrenzen der ~~Gemeinschaft~~ ☒ Europäischen Union ☒ aufgegriffen ~~werden wurden, festgestellt wird. Zur effektiven~~ Im Sinne einer ~~wirksamen~~ Anwendung ~~des Dubliner Übereinkommens~~ ☒ der Verordnung (EG) Nr. [...] [zur 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 insbesondere des Artikels 1018 Absatz 1 Buchstaben e) und e), b und d sollte außerdem wäre es darüber hinaus wünschenswert, dass jeder Mitgliedstaat prüfen können in Erfahrung bringen kann, ob ein Ausländer~~ ☒ Drittstaatsangehöriger oder Staatenloser ☒, der sich ~~illegal unrechtmäßig~~ in seinem Hoheitsgebiet aufhält, ~~bereits in einem anderen Mitgliedstaat Asyl beantragt hat~~ ⇒ einen Antrag auf internationalen Schutz gestellt hat ☐.

↓ 2725/2000/EG Erwägungsgrund 4

- (5) ~~Fingerabdrücke sind ein wichtiges Mittel zur genauen Identifizierung dieser Personen. Es bedarf eines Systems zum Vergleich der Fingerabdruckdaten. Da sich die Identität der genannten Personen anhand von Fingerabdrücken genau feststellen lässt, sollte ein System zum Abgleich ihrer Fingerabdruckdaten eingerichtet werden.~~

↓ 2725/2000/EG Erwägungsgrund 5
⇒ neu

- (6) ~~Zu diesem Zweck ist ein System Es ist ein europaweites Fingerabdruck-Identifizierungssystem mit dem Namen „EurodacEURODAC“ einzurichten, bestehend aus einer bei der Kommission anzusiedelnden Zentraleinheit, die eine computergestützte zentrale Datenbank für Fingerabdruckdaten betreiben wird, das aus~~ ⇒ einem Zentralsystem ☐, ~~das eine computergestützte Zentraldatenbank für Fingerabdruckdaten betreibt, und elektronischen Einrichtungen für die Datenübertragung zwischen den Mitgliedstaaten und der zentralen Datenbank~~ ⇒ dem Zentralsystem („Kommunikationsinfrastruktur“) ☐ ~~besteht.~~

²⁸ KOM(2008)XXX.

- (7) Im Haager Programm ist festgelegt, dass der Zugang zu den bestehenden Datenbanken der Europäischen Union zu verbessern ist. Im Stockholmer Programm wurde darüber hinaus die gezielte Datenerhebung und die den Anforderungen der Strafverfolgung entsprechende Entwicklung des Informationsaustauschs und der dazugehörigen Instrumente gefordert.
- (8) Für die Bekämpfung terroristischer und sonstiger schwerer Straftaten ist es unerlässlich, dass die Strafverfolgungsbehörden über möglichst umfassende und aktuelle Informationen verfügen, um ihren Aufgaben gerecht werden zu können. Die in EURODAC enthaltenen Informationen sind für die Verhütung, Aufdeckung und Untersuchung terroristischer und sonstiger schwerer Straftaten notwendig. Daher sollten die EURODAC-Daten den benannten Behörden der Mitgliedstaaten und Europol unter den in dieser Verordnung festgelegten Bedingungen für den Abgleich von Fingerabdruckdaten zur Verfügung stehen.
- (9) Die Kommission erklärte in ihrer Mitteilung an den Rat und das Europäische Parlament über die Verbesserung der Effizienz der europäischen Datenbanken im Bereich Justiz und Inneres und die Steigerung ihrer Interoperabilität sowie der Synergien zwischen ihnen²⁹ vom 24. November 2005, dass die für die innere Sicherheit zuständigen Behörden in genau bestimmten Fällen Zugang zu EURODAC erhalten könnten, wenn der begründete Verdacht besteht, dass der Urheber einer schweren Straftat einen Asylantrag gestellt hat. In der Mitteilung stellt die Kommission auch fest, dass diese Datenbanken nach dem Grundsatz der Verhältnismäßigkeit nur abgefragt werden dürfen, wenn ein überwiegendes öffentliches Sicherheitsinteresse besteht, d. h. wenn die von dem Straftäter oder Terroristen begangene Straftat so gravierend ist, dass die Abfrage einer Datenbank, in der Personen ohne kriminelle Vergangenheit registriert sind, gerechtfertigt ist; die Schwelle für die Abfrage von EURODAC durch die für die innere Sicherheit zuständigen Behörden müsse deshalb stets signifikant höher sein als die Schwelle für die Abfrage strafrechtlicher Datenbanken.
- (10) Darüber hinaus kommt Europol im Rahmen der Zusammenarbeit zwischen den Behörden der Mitgliedstaaten bei Ermittlungen wegen grenzüberschreitender Kriminalität eine Schlüsselrolle bei der Unterstützung der Kriminalitätsprävention sowie der Analyse und Untersuchung von Straftaten auf Unionsebene zu. Daher sollte Europol im Einklang mit dem Beschluss 2009/371/JI über die Errichtung eines Europäischen Polizeiamts (Europol)³⁰ bei der Wahrnehmung seiner Aufgaben ebenfalls Zugang zu den EURODAC-Daten haben.
- (11) Da EURODAC eingerichtet wurde, um die Anwendung der Verordnung (EU) Nr. [.../...] des Rates [zur 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,] zu erleichtern, stellt der Zugang zu EURODAC zum Zweck der Verhütung, Aufdeckung und Untersuchung terroristischer und sonstiger schwerer Straftaten eine Änderung der ursprünglichen Zweckbestimmung von EURODAC dar, die das Recht auf Achtung der Privatsphäre der Personen, deren personenbezogene Daten in EURODAC verarbeitet werden, beeinträchtigt. Jede derartige

²⁹ KOM(2005) 597 endg. vom 24.11.2005.

³⁰ ABl. L 121 vom 15.5.2009, S. 37.

Einschränkung muss mit Rechtsvorschriften konform sein, die so präzise formuliert sein müssen, dass der Einzelne sein Verhalten danach ausrichten kann; sie müssen den Einzelnen vor Willkür schützen und den Ermessensspielraum, den die zuständigen Behörden haben, und die Art und Weise, wie dieser genutzt werden darf, ganz klar festlegen. Jede Einschränkung muss in einer demokratischen Gesellschaft für die Durchsetzung eines rechtmäßigen und angemessenen Interesses notwendig und im Hinblick auf das verfolgte legitime Ziel verhältnismäßig sein.

- (12) Zwar war ursprünglich bei der Einrichtung von EURODAC nicht beabsichtigt, eine Funktion für die Beantragung eines Abgleichs mit Daten aus der Datenbank auf der Grundlage einer Fingerabdruckspur vorzusehen, die gegebenenfalls an einem Tatort gefunden wurde, doch ist eine solche Funktion für die Zusammenarbeit der Polizeibehörden von wesentlicher Bedeutung. Die Möglichkeit eines Abgleichs von Fingerabdruckspuren mit Fingerabdruckdaten in EURODAC wird den benannten Behörden der Mitgliedstaaten bei der Verhütung, Aufdeckung und Untersuchung terroristischer und sonstiger schwerer Straftaten große Dienste leisten, wenn an einem Tatort beispielsweise als einziger Beweis Fingerabdruckspuren gefunden wurden.
- (13) In dieser Verordnung sind die Bedingungen, unter denen Anträge auf einen Abgleich von Fingerabdruckdaten mit Daten in EURODAC zwecks Verhütung, Aufdeckung und Untersuchung terroristischer und sonstiger schwerer Straftaten gestellt werden können, sowie Schutzklauseln festgelegt, um das Grundrecht auf Achtung der Privatsphäre der Personen, deren Daten in EURODAC verarbeitet werden, zu garantieren.
- (14) Im Interesse der Gleichbehandlung aller Personen, die internationalen Schutz beantragt haben oder genießen, und um die Übereinstimmung mit dem geltenden Asylrecht der EU zu wahren, insbesondere mit der Richtlinie 2004/83/EG des Rates vom 29. April 2004 über Mindestnormen für die Anerkennung und den Status von Drittstaatsangehörigen oder Staatenlosen als Flüchtlinge oder als Personen, die anderweitig internationalen Schutz benötigen, und über den Inhalt des zu gewährenden Schutzes³¹ und mit der Verordnung (EU) Nr. [.../...] [zur 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], empfiehlt es sich, den Anwendungsbereich dieser Verordnung auf Personen auszudehnen, die subsidiären Schutz beantragt haben oder genießen.

↓ 2725/2000/EG Erwägungsgrund 6
(angepasst)
⇒ neu

- (15) ~~Den Mitgliedstaaten ist die Verpflichtung aufzuerlegen. Des Weiteren sind die Mitgliedstaaten zu verpflichten, allen Asylbewerbern~~ ⇒ Personen, die internationalen Schutz beantragen, ⇐ und allen ~~Ausländern~~ ⊗ Drittstaatsangehörigen oder Staatenlosen ⊗, die mindestens 14 Jahre alt sind und beim in-Verbindung-mit-dem illegalen Überschreiten einer Außengrenze eines Mitgliedstaats aufgegriffen ~~werden~~ wurden, unverzüglich die Fingerabdrücke abzunehmen

³¹ ABl. L 304 vom 30.9.2004, S. 12.

⇒ und die Daten dem Zentralsystem zu übermitteln ⇐; ~~wenn diese Personen mindestens vierzehn Jahre alt sind.~~

↓ 2725/2000/EG Erwägungsgrund 7
(angepasst)
⇒ neu

- (16) ~~Es sind genaue Regeln für~~ Für die Übermittlung ~~dieser der~~ Fingerabdruckdaten an ~~die Zentraleinheit~~ ⇒ das Zentralsystem ⇐, die Speicherung ~~der Fingerabdruckdaten dieser~~ und sonstiger relevanter Daten ~~in der zentralen Datenbank~~ ⇒ im Zentralsystem ⇐, ihre Aufbewahrung, den ~~Vergleich Abgleich~~ mit anderen Fingerabdruckdaten, die Übermittlung der ~~Vergleichsergebnisse Abgleichsergebnisse~~ sowie die ~~Sperrung~~ ⇒ Markierung ⇐ und Löschung von gespeicherten Daten ~~sind klar umrissene Regeln~~ aufzustellen. Diese Regeln ~~können, die für verschiedene die einzelnen~~ Kategorien von ~~Ausländern~~ ⇐ Drittstaatsangehörigen oder Staatenlosen ⇐ unterschiedlich gestaltet werden ~~können, und~~ sollten auf die spezifische Situation dieser Personen zugeschnitten sein.
-

↓ neu

- (17) Treffermeldungen von EURODAC sollten von einem Fachmann für Daktyloskopie (Fingerabdruckidentifizierung) überprüft werden, um zu gewährleisten, dass die Bestimmung der Zuständigkeit nach der Verordnung (EU) Nr. [...] [zur 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,] korrekt ist.
-

↓ 2725/2000/EG Erwägungsgrund 8
(angepasst)
⇒ neu

- (18) ~~Ausländer~~ ⇐ Drittstaatsangehörige oder Staatenlose ⇐, die in einem Mitgliedstaat ~~Asyl~~ ⇒ internationalen Schutz ⇐ beantragt haben, können während eines ~~langen~~ mehrere Jahre ~~umfassenden~~ Zeitraums auch in einem anderen Mitgliedstaat einen ~~Asylantrag~~ ⇒ Antrag auf internationalen Schutz ⇐ stellen. Daher sollte ~~der maximale Zeitraum, in dem Fingerabdrücke die maximale Dauer der Aufbewahrung von Fingerabdruckdaten in der Zentraleinheit~~ ⇒ im Zentralsystem ⇐ ~~aufbewahrt werden, sehr lang sein~~ großzügig bemessen werden. Da die meisten ~~Ausländer~~ ⇐ Drittstaatsangehörigen oder Staatenlosen ⇐ nach mehrjährigem Aufenthalt in der ~~Gemeinschaft~~ ⇐ Europäischen Union ⇐ einen dauerhaften Status erlangt oder sogar die ~~Staatsangehörigkeit~~ Staatsbürgerschaft eines Mitgliedstaats erworben haben ~~werden dürften~~, sollte ein Zeitraum von zehn Jahren als ~~angemessener Zeitraum~~ angemessen für die Aufbewahrung von Fingerabdruckdaten angesehen werden.

↓ 2725/2000/EG Erwägungsgrund 9
(angepasst)

- (19) ~~Der Aufbewahrungszeitraum sollte in~~ In bestimmten Fällen, in denen es nicht nötig ist, die Fingerabdruckdaten so lange aufzubewahren, ~~kürzer sein sollte der Zeitraum kürzer bemessen sein.~~ Die Fingerabdruckdaten sollten umgehend gelöscht werden, wenn ~~ein Ausländer~~ Drittstaatsangehörige oder Staatenlose die Staatsbürgerschaft ~~Staatsangehörigkeit~~ eines Mitgliedstaats erworben ~~hat~~ haben.
-

↓ neu

- (20) Es ist zweckmäßig, die Daten derjenigen Personen zu speichern, deren Fingerabdruckdaten in EURODAC erfasst worden sind, nachdem sie einen Antrag auf internationalen Schutz gestellt hatten und ihnen dieser in einem Mitgliedstaat gewährt worden war. Ziel ist es, einen Abgleich dieser Daten und der im Rahmen von Anträgen auf internationalen Schutz gespeicherten Daten vorzunehmen.
- (21) Die mit der Verordnung (EU) Nr. 1077/2011 des Europäischen Parlaments und des Rates vom 25. Oktober 2011 errichtete Europäische Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts³² („Agentur“) wird ab dem 1. Dezember 2012, dem Zeitpunkt, zu dem die Agentur ihre Arbeit aufnimmt, im Einklang mit dieser Verordnung mit der Erfüllung der Aufgaben der Kommission im Zusammenhang mit dem Betriebsmanagement von EURODAC sowie mit bestimmten Aufgaben betreffend die Kommunikationsinfrastruktur betraut. Die Agentur sollte die ihr mit dieser Verordnung übertragenen Aufgaben wahrnehmen; die einschlägigen Bestimmungen der Verordnung (EU) Nr. 1077/2001 sollten entsprechend geändert werden. Außerdem sollte Europol bei den Sitzungen des Verwaltungsrats der Agentur Beobachterstatus haben, wenn auf der Tagesordnung Angelegenheiten im Zusammenhang mit der Anwendung dieser Verordnung betreffend die EURODAC-Abfrage durch benannte Behörden der Mitgliedstaaten und Europol zum Zweck der Verhütung, Aufdeckung und Untersuchung terroristischer und sonstiger schwerer Straftaten stehen. Europol sollte einen Vertreter in die EURODAC-Beratergruppe der Agentur entsenden können.
- (22) Das Statut der Beamten der Europäischen Union („Beamtenstatut“) und die Beschäftigungsbedingungen für die sonstigen Bediensteten der Europäischen Union („Beschäftigungsbedingungen“), niedergelegt in der Verordnung (EWG, Euratom, EGKS) Nr. 259/68 (gemeinsam „Statut“), sollte für alle Beschäftigten gelten, die in der Agentur in Angelegenheiten tätig sind, die diese Verordnung betreffen.

³² ABl. L 286 vom 1.11.2011, S. 1.

↓ 2725/2000/EG Erwägungsgrund 10
(angepasst)
⇒ neu

- (23) ~~Es gilt, die Verantwortung~~ Die Aufgaben der Kommission ⇒ und der Agentur ⇐ in Bezug auf ~~die Zentraleinheit~~ ⇒ das Zentralsystem ⇐ ⇒ und die Kommunikationsinfrastruktur ⇐ ~~und die Verantwortung~~ sowie die Aufgaben der Mitgliedstaaten in Bezug auf die ~~Verwendung~~ Verarbeitung der Daten, die Datensicherheit, den ~~Zugang zuden~~ Datenzugang und die Berichtigung gespeicherter Daten ~~genau festzulegen~~ müssen eindeutig festgelegt werden.
-

↓ neu

- (24) Es ist notwendig, dass die Mitgliedstaaten die zuständigen Behörden und eine zentrale nationale Zugangsstelle, über die Anträge auf Abgleich mit EURODAC-Daten gestellt werden können, benennen und eine Liste der operativen Stellen innerhalb der benannten Behörden führen, die zum Zwecke der Verhütung, Aufdeckung und Untersuchung terroristischer Straftaten im Sinne des Rahmenbeschlusses 2002/475/JI vom 13. Juni 2002 zur Terrorismusbekämpfung³³ und sonstiger schwerer Straftaten im Sinne des Rahmenbeschlusses 2002/584/JI des Rates vom 13. Juni 2002 über den Europäischen Haftbefehl und die Übergabeverfahren zwischen den Mitgliedstaaten³⁴ zur Beantragung eines solchen Abgleichs berechtigt sind.
- (25) Anträge auf Abgleich mit Daten der EURODAC-Zentraldatenbank müssen unter Angabe von Gründen von den operativen Stellen innerhalb der benannten Behörden über die Prüfstelle bei der nationalen Zugangsstelle gestellt werden. Die zum Stellen von Anträgen auf einen Abgleich mit den EURODAC-Daten befugten operativen Stellen innerhalb der benannten Behörden dürfen nicht als Prüfstellen fungieren. Die Prüfstellen sollten damit betraut werden, die genaue Einhaltung der in dieser Verordnung festgelegten Zugangsbedingungen zu gewährleisten. Sie sollten prüfen, ob alle Voraussetzungen für den Zugang erfüllt sind und den Antrag auf Abgleich anschließend über die nationale Zugangsstelle an das EURODAC-Zentralsystem weiterleiten. In dringenden Ausnahmefällen, in denen der Zugang frühzeitig erfolgen muss, um auf eine konkrete akute Bedrohung im Zusammenhang mit terroristischen Straftaten oder schwerer Kriminalität reagieren zu können, sollte die Prüfstelle den Antrag unverzüglich bearbeiten und die Überprüfung erst nachträglich durchführen.
- (26) Aus Datenschutzgründen und um einen systematischen Abgleich, der verboten werden sollte, auszuschließen, sollten EURODAC-Daten nur im Einzelfall verarbeitet werden, wenn dies zur Verhütung, Aufdeckung und Untersuchung terroristischer und sonstiger schwerer Straftaten unbedingt erforderlich ist. Darüber hinaus sollte der Zugang nur dann gestattet sein, wenn Abgleiche mit den Daten der nationalen Datenbanken des Mitgliedstaats und der automatisierten daktyloskopischen Identifizierungssysteme der anderen Mitgliedstaaten nach dem Beschluss 2008/615/JI des Rates vom 23. Juni 2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und

³³ ABl. L 164 vom 22.6.2002, S. 3.

³⁴ ABl. L 190 vom 18.7.2002, S. 1.

der grenzüberschreitenden Kriminalität,³⁵ ergebnislos waren. Diese Voraussetzung erfordert die vorherige Umsetzung des Ratsbeschlusses, da eine EURODAC-Abfrage für Strafverfolgungszwecke unzulässig ist, wenn die genannten Schritte nicht zuvor unternommen wurden. Ein besonderer Fall ist insbesondere dann gegeben, wenn der Antrag auf Abgleich ein bestimmtes konkretes Vorkommnis oder eine konkrete Gefahr im Zusammenhang mit einer terroristischen oder sonstigen schweren Straftat oder mit bestimmten Personen betrifft, bei denen ernsthafte Gründe für die Annahme bestehen, dass sie terroristische Straftaten oder andere schwere Straftaten begehen werden oder begangen haben. Ein Sonderfall ist auch dann gegeben, wenn der Antrag auf Abgleich eine Person betrifft, die Opfer einer terroristischen oder sonstigen schweren Straftat ist. Die benannten Behörden und Europol sollten daher nur dann den Abgleich mit in EURODAC gespeicherten Daten beantragen, wenn sie Grund zu der Annahme haben, dass dieser Abgleich Informationen erbringt, die einen wesentlichen Beitrag zur Verhütung, Aufdeckung oder Untersuchung einer terroristischen oder sonstigen schweren Straftat leisten.

- (27) Kann der antragstellende Mitgliedstaat nachweisen, dass die EURODAC-Daten einem Minderjährigen zuzuordnen sind, so dürfen diese Daten vom antragstellenden Mitgliedstaat nur in Einklang mit den in diesem Staat geltenden Gesetzen für Minderjährige und mit der Verpflichtung, dem Wohl des Kindes Vorrang einzuräumen, für Strafverfolgungszwecke verwendet werden.

↓2725/2000/EG Erwägungsgrund 11
(angepasst)

- (28) ~~Während die~~ Die außervertragliche Haftung der ~~Gemeinschaft~~ Europäischen Union im Zusammenhang mit dem Betrieb des ~~Eurodac~~ EURODAC-Systems ist in den einschlägigen Bestimmungen des ~~EG-Vertrags~~ geregelt ~~ist, sind spezifische Regeln für~~. Für die außervertragliche Haftung der Mitgliedstaaten im Zusammenhang mit dem Betrieb des Systems hingegen sind entsprechende Regeln aufzustellen.

↓2725/2000/EG Erwägungsgrund 12
(angepasst)

- (29) ~~Entsprechend~~ Im Einklang mit dem in Artikel 5 des Vertrags niedergelegten Subsidiaritätsprinzip kann das Ziel der vorgeschlagenen Maßnahmen, nämlich die ~~Schaffung~~ Einrichtung ~~innerhalb der Kommission~~ ~~eines Systems zum Vergleich von~~ Fingerabdruckdaten ~~eines Fingerabdruckidentifizierungssystems~~ zur Unterstützung ~~der~~ Durchführung der Asylpolitik der ~~Gemeinschaft~~ Europäischen Union, auf der Ebene der Mitgliedstaaten aufgrund seiner Natur nicht ausreichend aufgrund seiner Dimension von den Mitgliedstaaten nicht in ausreichendem Maße sichergestellt und kann daher besser auf Unionsebene verwirklicht werden; dieses Ziel kann daher besser auf Gemeinschaftsebene erreicht werden. Entsprechend dem in demselben Artikel niedergelegten

³⁵ ABl. L 210 vom 6.8.2008, S. 1.

Verhältnismäßigkeitsprinzip geht diese Verordnung nicht über das für die Erreichung ~~dieses~~
~~Ziels~~ dieser Ziele erforderliche Maß hinaus.

↓2725/2000/EG Erwägungsgrund 15
(angepasst)
⇒ neu

- (30) 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 Datenverkehr³⁶ findet Anwendung auf die ☒ nach Maßgabe dieser Verordnung durchgeführte ☒ Verarbeitung personenbezogener Daten durch die Mitgliedstaaten ~~im Rahmen des Eurodac-Systems Anwendung~~ ⇒, es sei denn, diese Verarbeitung erfolgt zum Zweck der Verhütung, Aufdeckung und Untersuchung terroristischer oder sonstiger schwerer Straftaten durch die benannten Behörden der Mitgliedstaaten ⇐.
-

↓ neu

- (31) Der 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,³⁷ gilt für jegliche Verarbeitung personenbezogener Daten durch die benannten Behörden der Mitgliedstaaten zum Zweck der Verhütung, Aufdeckung und Untersuchung terroristischer und sonstiger schwerer Straftaten nach Maßgabe dieser Verordnung.
-

↓2725/2000/EG Erwägungsgrund 16

- ~~(16) Gemäß Artikel 286 des Vertrags findet die Richtlinie 95/46/EG auch auf die Organe und Einrichtungen der Gemeinschaft Anwendung. Da die Zentraleinheit in der Kommission eingerichtet wird, wird die genannte Richtlinie auch auf die Verarbeitung personenbezogener Daten durch diese Einheit Anwendung finden.~~
-

↓2725/2000/EG Erwägungsgrund 17

- (32) Die Grundsätze der Richtlinie 95/46/EG betreffend den Schutz der Rechte und Freiheiten von Personen, namentlich den Schutz der Privatsphäre, bei der Verarbeitung personenbezogener Daten sollten - insbesondere in Bezug auf bestimmte Bereiche - durch spezifische Vorschriften ergänzt oder geklärt werden.

³⁶ ABl. L 281 vom 23.11.1995, S. 31.

³⁷ ABl. L 350 vom 30.12.2008, S. 60.

↓ neu

- (33) Die Übermittlung von Daten, die auf der Grundlage dieser Verordnung erlangt wurden, an Drittstaaten, internationale Organisationen oder private Stellen sollte verboten werden, um das Recht auf Asyl zu garantieren und zu verhindern, dass Daten von Personen, die internationalen Schutz beantragen, an Drittstaaten weitergegeben werden. Dieses Verbot lässt das Recht der Mitgliedstaaten auf Weitergabe solcher Daten an Drittstaaten, auf die die Verordnung (EU) Nr. [...] [...] [zur 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] anwendbar ist, unberührt, damit sichergestellt ist, dass die Mitgliedstaaten für die Zwecke dieser Verordnung mit solchen Drittstaaten zusammenarbeiten können.
- (34) Nationale Stellen, die für die Beaufsichtigung der Verarbeitung personenbezogener Daten zuständig sind, sollten die Rechtmäßigkeit der Verarbeitung personenbezogener Daten durch die Mitgliedstaaten überwachen, während die Rechtmäßigkeit der Datenverarbeitung durch Europol von der mit dem Europol-Beschluss eingerichteten Kontrollinstanz überwacht werden sollte.
- (35) 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,³⁸ insbesondere die Artikel 21 und 22 über die Vertraulichkeit und die Sicherheit der Verarbeitung, finden Anwendung auf die in Anwendung dieser Verordnung erfolgende Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen, Ämter und Agenturen der Union. Allerdings sollten im Vorfeld Fragen im Zusammenhang mit der Zuständigkeit für die Datenverarbeitung und mit der Datenschutzaufsicht geklärt werden.
- (36) Nationale Kontrollbehörden sollten die Rechtmäßigkeit der Verarbeitung personenbezogener Daten durch die Mitgliedstaaten überwachen, während der in Artikel 41 der Verordnung (EG) Nr. 45/2001 genannte Europäische Datenschutzbeauftragte die Tätigkeiten der Organe, Einrichtungen sowie Ämter und Agenturen der Union in Bezug auf die Verarbeitung personenbezogener Daten gemäß dieser Verordnung kontrollieren sollte.

↓ 2725/2000/EG Erwägungsgrund 18

⇒ neu

- (37) Die Leistung ~~von Eurodac~~ des EURODAC-Systems sollte überwacht und ⇒ in regelmäßigen Abständen ⇐ bewertet werden.

³⁸ ABl. L 8 vom 12.1.2001, S. 1.

↓ 2725/2000/EG Erwägungsgrund 19
(angepasst)
⇒ neu

- (38) Die Mitgliedstaaten sollten ~~eine Sanktionsregelung~~ ⇒ ein System wirksamer, verhältnismäßiger und abschreckender Sanktionen ⇐ festlegen, um eine dem Zweck von ~~Eurodac~~ EURODAC zuwiderlaufende ~~Verwendung~~ Verarbeitung von ~~in der Zentraleinheit~~ ⊗ im Zentralsystem ⊗ ~~erfassten~~ ⊗ eingegebenen ⊗ Daten ahnden zu können.

↓ neu

- (39) Die Mitgliedstaaten sollten sich gegenseitig über den Stand besonderer Asylverfahren informieren, um die adäquate Anwendung der Verordnung (EU) Nr. [...] [zur 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,] zu erleichtern.
- (40) Diese Verordnung steht im Einklang mit den in der Charta der Grundrechte der Europäischen Union anerkannten Grundrechten und Grundsätzen und ist entsprechend anzuwenden. Mit dieser Verordnung soll insbesondere die uneingeschränkte Beachtung des Rechts von Einzelpersonen auf den Schutz ihrer Daten und des Rechts auf Asyl gewährleistet werden.
- (41) Gemäß den Artikeln 1 und 2 des dem Vertrag über die Europäische Union und dem Vertrag über die Arbeitsweise der Europäischen Union beigefügten Protokolls über die Position Dänemarks beteiligt sich Dänemark nicht an der Annahme dieser Verordnung, die somit nicht für Dänemark bindend und Dänemark gegenüber nicht anwendbar ist. In Bezug auf Dänemark stellt diese Verordnung mit Ausnahme des Verfahrens für den Abgleich und die Datenübermittlung zu Strafverfolgungszwecken gemäß Artikel 5, Artikel 6, Artikel 19 bis 22, Artikel 33, Artikel 36, Artikel 39 Absatz 3, Artikel 40 Absatz 8 und Artikel 43 eine Änderung der EURODAC-Verordnung im Sinne des Abkommens zwischen der Europäischen Gemeinschaft und dem Königreich Dänemark über die Kriterien und Verfahren zur Bestimmung des Staates, der für die Prüfung eines in Dänemark oder in einem anderen Mitgliedstaat der Europäischen Union gestellten Asylantrags zuständig ist, sowie über EURODAC für den Vergleich von Fingerabdrücken zum Zwecke der effektiven Anwendung des Dubliner Übereinkommens³⁹ dar. Folglich muss Dänemark der Kommission gemäß Artikel 3 des Abkommens mitteilen, ob es den Inhalt dieser Verordnung umsetzen will. Sollte dies der Fall sein, begründet diese Verordnung gegenseitige völkerrechtliche Verpflichtungen zwischen Dänemark und der Europäischen Union. Sobald die Neufassung dieser Verordnung erlassen ist und vorbehaltlich einer Empfehlung der Kommission für einen Beschluss des Rates über die Ermächtigung zur Aufnahme von Verhandlungen wird Dänemark gefragt, ob es an Verhandlungen über ergänzende Abkommen teilnehmen möchte, die sich auch auf das Verfahren für den Abgleich und die Datenübermittlung zu Strafverfolgungszwecken gemäß Artikel 5, Artikel 6, Artikel 19 bis 22, Artikel 33, Artikel 36, Artikel 39 Absatz 3, Artikel 40 Absatz 8 und Artikel 43 erstrecken.

³⁹ ABl. L 66 vom 8.3.2006, S. 38.

- (42) Gemäß Artikel 3 des dem Vertrag über die Europäische Union und dem Vertrag über die Arbeitsweise der Europäischen Union beigefügten Protokolls über die Position des Vereinigten Königreichs und Irlands hinsichtlich des Raums der Freiheit, der Sicherheit und des Rechts und unbeschadet des Artikels 4 dieses Protokolls *[beteiligt sich das Vereinigte Königreich nicht an der Annahme dieser Verordnung, die somit nicht für das Vereinigte Königreich bindend und ihm gegenüber nicht anwendbar ist / hat das Vereinigte Königreich mitgeteilt, dass es sich an der Annahme und Anwendung dieser Verordnung beteiligen will]*.
- (43) Gemäß Artikel 3 des dem Vertrag über die Europäische Union und dem Vertrag über die Arbeitsweise der Europäischen Union beigefügten Protokolls über die Position des Vereinigten Königreichs und Irlands hinsichtlich des Raums der Freiheit, der Sicherheit und des Rechts und unbeschadet des Artikels 4 dieses Protokolls *[beteiligt sich Irland nicht an der Annahme dieser Verordnung, die somit für Irland nicht bindend und Irland gegenüber nicht anwendbar ist / hat Irland mitgeteilt, dass es sich an der Annahme und Anwendung dieser Verordnung beteiligen will]*.
- (44) In Bezug auf die Republik Island und das Königreich Norwegen stellt diese Verordnung mit Ausnahme des Verfahrens für den Abgleich und die Datenübermittlung zu Strafverfolgungszwecken gemäß Artikel 5, Artikel 6, Artikel 19 bis 22, Artikel 33, Artikel 36, Artikel 39 Absatz 3, Artikel 40 Absatz 8 und Artikel 43 eine neue Maßnahme in Verbindung mit EURODAC im Sinne des Übereinkommens zwischen der Europäischen Gemeinschaft und der Republik Island und dem Königreich Norwegen über die Kriterien und Regelungen zur Bestimmung des zuständigen Staates für die Prüfung eines in einem Mitgliedstaat oder in Island oder Norwegen gestellten Asylantrags⁴⁰ dar. Vorbehaltlich des Beschlusses der Republik Island und des Königreichs Norwegen, diese Verordnung in innerstaatliches Recht umzusetzen, gilt sie zwischen der Republik Island und dem Königreich Norwegen für ihre gegenseitigen Beziehungen und für ihre Beziehungen mit den Mitgliedstaaten der Europäischen Union. Sobald die Neufassung dieser Verordnung erlassen ist und vorbehaltlich einer Empfehlung der Kommission für einen Beschluss des Rates über die Ermächtigung zur Aufnahme von Verhandlungen werden die Republik Irland und das Königreich Norwegen gefragt, ob sie an Verhandlungen über ergänzende Abkommen teilnehmen möchten, die sich auch auf das Verfahren für den Abgleich und die Datenübermittlung zu Strafverfolgungszwecken gemäß Artikel 5, Artikel 6, Artikel 19 bis 22, Artikel 33, Artikel 36, Artikel 39 Absatz 3, Artikel 40 Absatz 8 und Artikel 43 erstrecken.
- (45) In Bezug auf die Schweizer Eidgenossenschaft stellt diese Verordnung mit Ausnahme des Verfahrens für den Abgleich und die Datenübermittlung zu Strafverfolgungszwecken gemäß Artikel 5, Artikel 6, Artikel 19 bis 22, Artikel 33, Artikel 36, Artikel 39 Absatz 3, Artikel 40 Absatz 8 und Artikel 43 eine neue Maßnahme in Verbindung mit EURODAC im Sinne des Abkommens zwischen der Europäischen Gemeinschaft und der Schweizerischen Eidgenossenschaft über die Kriterien und Verfahren zur Bestimmung des zuständigen Staates für die Prüfung eines in einem Mitgliedstaat oder in der Schweiz gestellten Asylantrags⁴¹ dar. Vorbehaltlich des Beschlusses der Schweizerischen Eidgenossenschaft, diese Verordnung in innerstaatliches Recht umzusetzen, ist diese Verordnung demnach zwischen der Schweizerischen Eidgenossenschaft und den Mitgliedstaaten der Europäischen Union

⁴⁰ ABl. L 93 vom 3.4.2001, S. 40.

⁴¹ ABl. L 53 vom 27.2.2008, S. 5.

anwendbar. Sobald die Neufassung dieser Verordnung erlassen ist und vorbehaltlich einer Empfehlung der Kommission für einen Beschluss des Rates über die Ermächtigung zur Aufnahme von Verhandlungen wird die Schweizerische Eidgenossenschaft vorbehaltlich eines gesonderten Abkommens über die Anwendung der einschlägigen Bestimmungen des Ratsbeschlusses 2008/615/JI zur Vertiefung der grenzüberschreitenden Zusammenarbeit gefragt, ob sie an Verhandlungen über ergänzende Abkommen teilnehmen möchte, die sich auch auf das Verfahren für den Abgleich und die Datenübermittlung zu Strafverfolgungszwecken gemäß Artikel 5, Artikel 6, Artikel 19 bis 22, Artikel 33, Artikel 36, Artikel 39 Absatz 3, Artikel 40 Absatz 8 und Artikel 43 erstrecken.

- (46) In Bezug auf das Fürstentum Liechtenstein stellt diese Verordnung mit Ausnahme des Verfahrens für den Abgleich und die Datenübermittlung zu Strafverfolgungszwecken gemäß Artikel 5, Artikel 6, Artikel 19 bis 22, Artikel 33, Artikel 36, Artikel 39 Absatz 3, Artikel 40 Absatz 8 und Artikel 43 eine neue Maßnahme in Verbindung mit EUODAC im Sinne des Protokolls zwischen der Europäischen Gemeinschaft, der Schweizerischen Eidgenossenschaft und dem Fürstentum Liechtenstein über den Beitritt des Fürstentums Liechtenstein zu dem Abkommen zwischen der Europäischen Gemeinschaft und der Schweizerischen Eidgenossenschaft über die Kriterien und Verfahren zur Bestimmung des zuständigen Staates für die Prüfung eines in einem Mitgliedstaat oder in der Schweiz gestellten Asylantrags⁴² dar. Vorbehaltlich des Beschlusses des Fürstentums Liechtenstein, diese Verordnung in innerstaatliches Recht umzusetzen, ist diese Verordnung demnach im Verhältnis zwischen der Schweizerischen Eidgenossenschaft und den Mitgliedstaaten der Europäischen Union anwendbar. Sobald die Neufassung dieser Verordnung erlassen ist und vorbehaltlich einer Empfehlung der Kommission für einen Beschluss des Rates über die Ermächtigung zur Aufnahme von Verhandlungen wird das Fürstentum Liechtenstein vorbehaltlich eines gesonderten Abkommens über die Anwendung der einschlägigen Bestimmungen des Ratsbeschlusses 2008/615/JI zur Vertiefung der grenzüberschreitenden Zusammenarbeit gefragt, ob es an Verhandlungen über ergänzende Abkommen teilnehmen möchte, die sich auch auf das Verfahren für den Abgleich und die Datenübermittlung zu Strafverfolgungszwecken gemäß Artikel 5, Artikel 6, Artikel 19 bis 22, Artikel 33, Artikel 36, Artikel 39 Absatz 3, Artikel 40 Absatz 8 und Artikel 43 erstrecken.

↓ 2725/2000/EG Erwägungsgrund 22
(angepasst)

- (47) Es empfiehlt sich, den territorialen Anwendungsbereich der Verordnung ~~in der Weise~~ so zu begrenzen, dass er dem territorialen Anwendungsbereich ~~des Dubliner Übereinkommens~~ der Verordnung (EU) Nr. [.../...] [zur 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,] entspricht –

⁴² ABl. L 160 vom 18.6.2011, S. 39.

~~HAT~~ ☒ HABEN ☒ FOLGENDE VERORDNUNG ERLASSEN:

KAPITEL I

ALLGEMEINE BESTIMMUNGEN

Artikel 1

Zweck ~~von „Eurodac“~~ des Systems „EURODAC“

1. Hiermit wird ~~ein „Eurodac“ genanntes System~~ das Fingerabdruckidentifizierungssystem „EURODAC“ eingerichtet, ~~das~~ EURODAC soll nach Maßgabe dieser Verordnung bei der Bestimmung des Mitgliedstaats, der gemäß ~~dem~~ Dubliner Übereinkommen ☒ der Verordnung (EU) Nr. [.../...] [zur 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,] ☒ für die Prüfung eines ⇒ von einem Drittstaatsangehörigen oder Staatenlosen ⇐ in einem Mitgliedstaat gestellten ~~Asylantrags~~ ⇒ Antrags auf internationalen Schutz ⇐ zuständig ist, herangezogen werden und die Anwendung ~~des~~ Dubliner Übereinkommens ☒ der Dublin-Verordnung ☒ unter den in dieser Verordnung festgelegten Bedingungen ~~anderweitig~~ erleichtern soll.
2. ~~Eurodac umfasst:~~
 - (a) ~~die Zentraleinheit nach Artikel 3,~~
 - (b) ~~eine computergestützte zentrale Datenbank, in der die Daten nach Artikel 5 Absatz 1, Artikel 8 Absatz 2 und Artikel 11 Absatz 2 zum Vergleich der Fingerabdruckdaten von Asylbewerbern und von den in Artikel 8 Absatz 1 und Artikel 11 Absatz 1 genannten Kategorien von Ausländern verarbeitet werden, sowie~~
 - (c) ~~die zwischen den Mitgliedstaaten und der zentralen Datenbank bestehenden Übermittlungseinrichtungen.~~
2. Mit dieser Verordnung werden die Bedingungen festgelegt, unter denen die benannten Behörden der Mitgliedstaaten und das Europäische Polizeiamt (Europol) den Abgleich von Fingerabdruckdaten mit Daten der EURODAC-Zentraldatenbank zum Zwecke der Verhütung, Aufdeckung und Untersuchung terroristischer und sonstiger schwerer Straftaten beantragen können.

↓ 2725/2000/EG (angepasst)

⇒ neu

3. Unbeschadet der ~~Verwendung~~ Verarbeitung der für ~~Eurodac~~ EURODAC bestimmten Daten durch den Herkunftsmitgliedstaat in nach seinem nationalen Recht eingerichteten Datenbanken dürfen die Fingerabdruckdaten und ~~die anderen~~ personenbezogenen Daten nur für die ~~⇒ in dieser Verordnung und ⇐ in Artikel 15 Absatz 1 32 Absatz 1 des Dubliner Übereinkommens~~ ⇒ in dieser Verordnung und ⇐ in Artikel 32 Absatz 1 der Dublin-Verordnung ~~☒~~ ☒ genannten Zwecke in ~~Eurodac~~ EURODAC verarbeitet werden.

↓ 2725/2000/EG (angepasst)

⇒ neu

Artikel 2

Begriffsbestimmungen Definitionen

1. ~~Für die Zwecke dieser Verordnung gelten folgende Begriffsbestimmungen:~~ Im Sinne dieser Verordnung bezeichnet der Ausdruck
- (a) ~~„Dubliner Übereinkommen ☒ Dublin-Verordnung ☒“ ist das am 15. Juni 1990 in Dublin unterzeichnete Übereinkommen über die Bestimmung des zuständigen Staates für die Prüfung eines in einem Mitgliedstaat der Europäischen Gemeinschaften gestellten Asylantrags. ☒ die Verordnung (EU) Nr. [.../...] [zur 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]; ☒~~
- (b) ~~„Asylbewerber“ ⇒ „Person, die internationalen Schutz beantragt“, ⇐ ist jeder Ausländer, der einen Asylantrag gestellt hat oder in dessen Namen ein Asylantrag gestellt worden ist. ☒ einen Drittstaatsangehörigen oder Staatenlosen ☒, der einen Antrag auf ⇒ internationalen Schutz gemäß Artikel 2 Buchstabe g der Richtlinie 2004/83/EG des Rates gestellt hat, über den noch keine rechtskräftige Entscheidung ergangen ist; ⇐~~
- (c) ~~„Herkunftsmitgliedstaat“ ist~~
- (i) ~~im Zusammenhang mit einem Asylbewerber ☒ einer unter Artikel 6 fallenden Person ☒ der den Mitgliedstaat, der die personenbezogenen Daten an die Zentraleinheit ⇒ das Zentralsystem ⇐ übermittelt und die Vergleichsergebnisse Ableichsergebnisse erhält;~~
- (ii) ~~im Zusammenhang mit einer unter Artikel 8 11 fallenden Person der den Mitgliedstaat, der die personenbezogenen Daten an die Zentraleinheit ⇒ das Zentralsystem ⇐ übermittelt;~~

- (iii) im Zusammenhang mit einer unter Artikel ~~11~~ 14 fallenden Person ~~der den~~ Mitgliedstaat, der ~~solche~~ die personenbezogenen Daten an ~~die Zentraleinheit~~ ⇒ das Zentralsystem ⇐ übermittelt und die Vergleichsergebnisse Abgleichsergebnisse erhält;

↓ 2725/2000/EG (angepasst)
⇒ neu

- (d) „Flüchtling“ ⇒ „Person, der internationaler Schutz gewährt wird“ ⇐ ~~ist eine Person, die nach der Genfer Flüchtlingskonvention vom 28. Juli 1951 in der Fassung des New Yorker Protokolls vom 31. Januar 1967 als Flüchtling anerkannt ist.~~ ☒ einen Drittstaatsangehörigen oder Staatenlosen, ☒ ⇒ der Anspruch auf internationalen Schutz gemäß Artikel 2 Buchstabe a der Richtlinie 2004/83/EG des Rates hat; ⇐
- (e) „Treffer“ ~~ist bzw. sind~~ die aufgrund eines Abgleichs durch ~~die Zentraleinheit~~ ⇒ das Zentralsystem ⇐ festgestellte Übereinstimmung oder festgestellten Übereinstimmungen zwischen den in der ~~Datenbank~~ ☒ Zentraldatenbank ☒ gespeicherten Fingerabdruckdaten und den von einem Mitgliedstaat übermittelten Fingerabdruckdaten zu einer Person, unbeschadet der Verpflichtung der Mitgliedstaaten, die Ergebnisse des Vergleichs Abgleichs gemäß Artikel 4 ~~Absatz 6~~ 18 Absatz 4 ~~des Übereinkommens~~ sofort zu prüfen;

↓ neu

- (f) „nationale Zugangsstelle“ die benannte nationale Stelle, die mit dem Zentralsystem Daten austauscht;
- (g) „Agentur“ die mit der Verordnung (EU) Nr. 1077/2011 errichtete Agentur;
- (h) „Europol“ das mit dem Beschluss 2009/371/JI errichtete Europäische Polizeiamt;
- (i) „EURODAC-Daten“ sämtliche Fingerabdruckdaten, die in der Zentraldatenbank gemäß Artikel 11 und Artikel 16 Absatz 2 gespeichert sind.
- (j) „terroristische Straftaten“ Straftaten nach einzelstaatlichem Recht, die den in den Artikeln 1 bis 4 des Rahmenbeschlusses 2002/475/JI des Rates genannten Straftaten entsprechen oder gleichwertig sind;
- (k) „schwere Straftaten“ Straftaten, die den in Artikel 2 Absatz 2 des Rahmenbeschlusses 2002/584/JI aufgeführten Straftaten entsprechen oder gleichwertig sind, wenn die Straftaten mit einer freiheitsentziehenden Strafe oder Sicherungsmaßnahme für eine Höchstdauer von mindestens drei Jahren nach dem einzelstaatlichen Recht geahndet werden können;
- (l) „Fingerabdruckdaten“ die Fingerabdruckdaten für sämtliche Finger, mindestens aber für die Zeigefinger, oder sollten diese fehlen, für alle anderen Finger einer Person oder eine Fingerabdruckspur.

↓ 2725/2000/EG (angepasst)
⇒ neu

2. ~~Die in Artikel 2 der Richtlinie 95/46/EG definierten Ausdrücke haben in dieser Verordnung die gleiche Bedeutung.~~ Für diese Verordnung gelten die in Artikel 2 der Richtlinie 95/46/EG festgelegten Definitionen, \Rightarrow es sei denn, die Verarbeitung personenbezogener Daten erfolgt zum Zweck der Verhütung, Aufdeckung und Untersuchung terroristischer oder sonstiger schwerer Straftaten durch die benannten Behörden der Mitgliedstaaten \Leftarrow .
3. Sofern nichts anderes angegeben ist, ~~gelten für diese Verordnung haben~~ die in Artikel ~~1~~ 2 ~~des Dubliner Übereinkommens~~ \boxtimes der Dublin-Verordnung \boxtimes festgelegten Definitionen ~~definierten Ausdrücke in dieser Verordnung die gleiche Bedeutung.~~
-

↓ neu

4. Für diese Verordnung gelten die in Artikel 2 des Rahmenbeschlusses 2008/977/JI festgelegten Definitionen, soweit personenbezogene Daten von den benannten Behörden der Mitgliedstaaten zum Zweck der Verhütung, Aufdeckung und Untersuchung terroristischer oder sonstiger schwerer Straftaten nach Maßgabe dieser Verordnung verarbeitet werden.
-

↓ 2725/2000/EG (angepasst)

Artikel 3

~~Zentraleinheit~~ \boxtimes Aufbau des Systems und Grundprinzipien \boxtimes

- ~~1. Bei der Kommission wird eine Zentraleinheit eingerichtet, die dafür zuständig ist, im Namen der Mitgliedstaaten die in Artikel 1 Absatz 2 Buchstabe b) genannte zentrale Datenbank zu betreiben. Die Zentraleinheit wird mit einem computergestützten Fingerabdruckererkennungssystem ausgestattet.~~
-

↓ neu

1. EURODAC umfasst:
- (a) eine automatisierte zentrale Fingerabdruck-Datenbank (Zentralsystem) mit
 - einer Zentraleinheit
 - einem Notfallsystem
 - (b) eine Kommunikationsinfrastruktur zwischen dem Zentralsystem und den Mitgliedstaaten, die ein verschlüsseltes virtuelles Netz für die Übermittlung von EURODAC-Daten zur Verfügung stellt (Kommunikationsinfrastruktur).

2. Jeder Mitgliedstaat benennt eine einzige nationale Zugangsstelle.

↓ 2725/2000/EG (angepasst)

⇒ neu

2.3. ~~Die Zentraleinheit~~ ⇒ Das Zentralsystem ⇐ verarbeitet die Daten von ~~Asylbewerbern sowie von~~ unter Artikel ~~8 oder Artikel 11~~ 9, 14 und 17 fallenden Personen im Auftrag des Herkunftsmitgliedstaats unter den in dieser Verordnung festgelegten Bedingungen ☒ und trennt die Daten mit den geeigneten technischen Mitteln ☒.

↓ 2725/2000/EG Artikel 1 Absatz 2 dritter

Unterabsatz

⇒ neu

4. Die für ~~Eurodac~~EURODAC geltenden Regeln gelten auch für die ~~von den Mitgliedstaaten ausgeführten Vorgänge~~ Operationen der Mitgliedstaaten = von der Übermittlung der Daten an ~~die Zentraleinheit~~ ⇒ das Zentralsystem ⇐ bis zur Verwendung der Ergebnisse des ~~Vergleichs~~Abgleichs.

↓ 2725/2000/EG Artikel 4 Absatz 1 zweiter

Satz

⇒ neu

5. Das Verfahren zur ~~Abnahme von Fingerabdrücken~~Erfassung von Fingerabdruckdaten wird gemäß den innerstaatlichen Gepflogenheiten des betreffenden Mitgliedstaats und unter Beachtung der in ⇒ der Charta der Grundrechte der Europäischen Union, in der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten und ⇐ ~~der Europäischen Menschenrechtskonvention und~~ im Übereinkommen der Vereinten Nationen über die Rechte des Kindes verankerten Schutzklauseln festgelegt ⇒ und angewandt ⇐.

↓ neu

Artikel 4

Betriebsmanagement

1. Für das Betriebsmanagement von EURODAC ist die Agentur zuständig. Diese gewährleistet in Zusammenarbeit mit den Mitgliedstaaten, dass vorbehaltlich einer Kosten-Nutzen-Analyse jederzeit die beste verfügbare Technologie für das Zentralsystem zum Einsatz kommt.
2. Die Agentur ist ferner für folgende Aufgaben im Zusammenhang mit der Kommunikationsinfrastruktur zuständig:

- (a) Überwachung
 - (b) Sicherheit
 - (c) Koordinierung der Beziehungen zwischen den Mitgliedstaaten und dem Betreiber.
3. Die Kommission ist für alle sonstigen Aufgaben im Zusammenhang mit der Kommunikationsinfrastruktur zuständig, insbesondere für:
- (a) Aufgaben im Zusammenhang mit dem Haushaltsvollzug
 - (b) Anschaffung und Erneuerung
 - (c) vertragliche Belange.
4. Bis die Agentur ihre Tätigkeit aufnimmt, ist die Kommission für alle Aufgaben zuständig, die gemäß dieser Verordnung in die Zuständigkeit der Agentur fallen.
5. Das Betriebsmanagement von EURODAC umfasst alle Aufgaben, die erforderlich sind, um EURODAC im Einklang mit dieser Verordnung 24 Stunden am Tag und 7 Tage in der Woche betriebsbereit zu halten; dazu gehören insbesondere die für den einwandfreien Betrieb des Systems erforderlichen Wartungsarbeiten und technischen Anpassungen, um unter anderem die zum Abfragen des Zentralsystems erforderliche Zeit auf einem akzeptablen Niveau zu halten.
6. Unbeschadet des Artikels 17 der Verordnung Nr. 31 (EWG), 11 (EAG)⁴³ wendet die Agentur angemessene Regeln zur Gewährleistung der beruflichen Schweigepflicht oder einer anderen vergleichbaren Geheimhaltungspflicht auf alle Mitarbeiter an, die mit EURODAC-Daten arbeiten. Diese Pflicht besteht auch nach dem Ausscheiden dieser Personen aus dem Amt oder Dienstverhältnis oder nach der Beendigung ihrer Tätigkeit weiter.
-

↓ neu

Artikel 5

Zu Strafverfolgungszwecken zugangsberechtigte Behörden

1. Die Mitgliedstaaten benennen die Behörden, die gemäß dieser Verordnung zum Zugriff auf EURODAC-Daten berechtigt sind. Bei den benannten Behörden handelt es sich um Behörden der Mitgliedstaaten, die für die Verhütung, Aufdeckung oder Untersuchung von terroristischen oder sonstigen schweren Straftaten zuständig sind.
2. Jeder Mitgliedstaat führt eine Liste der benannten Behörden.

⁴³ ABl. 45 vom 14.6.1962, S. 1385.

3. Jeder Mitgliedstaat führt eine Liste der operativen Stellen innerhalb seiner benannten Behörden, die berechtigt sind, den Abgleich mit EURODAC-Daten über die nationale Zugangsstelle zu beantragen.

Artikel 6 Prüfstellen

1. Jeder Mitgliedstaat benennt eine nationale Stelle als Prüfstelle. Die Prüfstellen sind Behörden der Mitgliedstaaten, die für die Verhütung, Aufdeckung oder Untersuchung von terroristischen oder sonstigen schweren Straftaten zuständig sind.
2. Die Prüfstellen tragen dafür Sorge, dass die Bedingungen für die Beantragung eines Abgleichs von Fingerabdruckdaten mit EURODAC-Daten erfüllt sind.

Nur die Prüfstellen sind berechtigt, Anträge auf einen Abgleich von Fingerabdruckdaten an die nationale Zugangsstelle zu übermitteln, die mit dem Zentralsystem Daten austauscht.

Artikel 7 Europol

1. Europol benennt eine mit ordnungsgemäß befugtem Europol-Personal ausgestattete Spezialeinheit, die für Europol als Prüfstelle fungiert, und eine nationale Zugangsstelle in Absprache mit dem betreffenden Mitgliedstaat, die Anträge von Europol auf einen Abgleich von Fingerabdruckdaten an das Zentralsystem übermittelt.
2. Europol benennt eine operative Einheit, die berechtigt ist, über die benannte nationale Zugangsstelle den Abgleich mit EURODAC-Daten zu beantragen.

↓ 2725/2000/EG (angepasst)
⇒ neu

Artikel 8 ~~3~~ ⊗ Statistiken ⊗

~~3=1.~~ Die ~~Zentraleinheit~~ ⊗ Agentur ⊗ erstellt ~~alle drei Monate~~ eine ⇒ monatliche ⊗ Statistik über ~~ihre~~ ⊗ die ⊗ Arbeit ⊗ des Zentralsystems ⊗, aus der ⇒ insbesondere ⊗ Folgendes hervorgeht:

- (a) die Anzahl der ~~über Asylbewerber und über Personen nach Artikel 8 Absatz 1 und Artikel 11 Absatz 1 übermittelten~~ Datensätze, die zu Personen nach Artikel 9 Absatz 1, Artikel 14 Absatz 1 und Artikel 17 Absatz 1 übermittelt wurden;
- (b) die Anzahl der Treffer ~~hinsichtlich der~~ in Bezug auf ~~Asylbewerber~~ ⇒ Antragsteller ⊗, die ~~bereits~~ in einem anderen Mitgliedstaat einen ~~Asylantrag~~ ⇒ Antrag auf internationalen Schutz ⊗ gestellt haben;

- (c) die Anzahl der Treffer ~~hinsichtlich der in Bezug auf die~~ in Artikel ~~8 Absatz 1~~ ~~4~~ ~~Absatz 1~~ ~~bezeichneten~~ ~~genannten~~ Personen, die zu einem späteren Zeitpunkt einen ~~Asylantrag~~ ⇒ Antrag auf internationalen Schutz ⇐ gestellt haben;
- (d) die Anzahl der Treffer ~~hinsichtlich der in Bezug auf die~~ in Artikel ~~11 Absatz 1~~ ~~7~~ ~~Absatz 1~~ ~~bezeichneten~~ ~~genannten~~ Personen, die zu einem früheren Zeitpunkt einen ~~Asylantrag~~ ⇒ Antrag auf internationalen Schutz ⇐ in einem anderen Mitgliedstaat gestellt hatten;
- (e) die Anzahl der Fingerabdruckdaten, ~~welche die die Zentraleinheit~~ ⇒ das ~~Zentralsystem~~ ⇐ ⇒ mehrfach ⇐ ~~erneut~~ vom Herkunftsmitgliedstaat anfordern musste, weil die ursprünglich übermittelten Fingerabdruckdaten für den Abgleich anhand des automatisierten Fingerabdruckidentifizierungssystems unter Verwendung des computergestützten Fingerabdruckerkennungssystems ungeeignet waren;=

↓ neu

- (f) die Zahl der Anträge auf Markierung und Entfernung der Markierung gemäß Artikel 18 Absätze 1 und 2;
- g) die Zahl der Treffer in Bezug auf die in Artikel 18 Absatz 1 genannten Personen, für die Treffer gemäß den Buchstaben b und d dieses Artikels gespeichert wurden.

↓ 2725/2000/EG
⇒ neu

2. Am Ende jeden Jahres wird eine Statistik erstellt, die die ~~seit Beginn der Tätigkeitsaufnahme von Eurodac erstellten dreimonatlichen~~ ⇒ monatlichen ⇐ Statistiken ⇒ des Jahres ⇐ zusammenfasst und ~~dabei~~ die Anzahl der Personen angibt, zu denen ~~Treffer es Treffermeldungen~~ nach den Buchstaben b), c), und d) ~~festgestellt wurden~~ gegeben hat. ⇒ Die Statistik enthält eine Aufgliederung der Daten für jeden einzelnen Mitgliedstaat. ⇐

~~4.~~ Die Zentraleinheit kann gemäß dem Verfahren nach Artikel 23 Absatz 2 beauftragt werden, auf der Grundlage der in der Zentraleinheit verarbeiteten Daten bestimmte andere statistische Aufgaben wahrzunehmen.

↓ 2725/2000/EG (angepasst)
⇒ neu

KAPITEL II

~~ASYLBEWERBER~~ ☒ PERSONEN, DIE INTERNATIONALEN SCHUTZ BEANTRAGEN ☒

Artikel 9 4

Erfassung, Übermittlung und ~~Vergleich~~ Abgleich von ~~Fingerabdrücken~~ Fingerabdruckdaten

1. Jeder Mitgliedstaat nimmt ~~jeden Asylbewerber, der~~ ⇒ jeder Person, die internationalen Schutz beantragt und ⇐ mindestens 14 Jahre alt ist, unverzüglich ~~die Fingerabdrücke aller Finger ab~~ den Abdruck aller Finger ab und übermittelt ~~der Zentraleinheit~~ unverzüglich die Fingerabdruckdaten ☒ zusammen mit den ☒ in Artikel ~~5 Absatz 1~~ 11 Buchstaben ~~(a) (b)~~ (c) (g) dieser Verordnung aufgeführten ~~bezeichneten~~ Daten ⇒ so rasch wie möglich, spätestens aber 72 Stunden nach Antragstellung gemäß Artikel 20 Absatz 2 der Dublin-Verordnung an das Zentralsystem ⇐.

↓ neu

Die Nichteinhaltung der Frist von 72 Stunden entbindet die Mitgliedstaaten nicht von der Verpflichtung, die Fingerabdrücke abzunehmen und an das Zentralsystem zu übermitteln. Können aufgrund des Zustands der Fingerkuppen keine Fingerabdrücke in einer Qualität abgenommen werden, die einen angemessenen Abgleich nach Artikel 25 gewährleistet, nimmt der Herkunftsmitgliedstaat erneut die Fingerabdrücke des Antragstellers ab und übermittelt diese so rasch wie möglich, spätestens aber 48 Stunden nach erfolgreicher Abnahme.

↓ 2725/2000/EG

~~(2) Die Daten nach Artikel 5 Absatz 1 werden durch die Zentraleinheit oder, sofern die technischen Voraussetzungen hierfür erfüllt sind, unmittelbar durch den Herkunftsmitgliedstaat sofort in der zentralen Datenbank gespeichert.~~

↓ neu

2. In Fällen, in denen aufgrund von Maßnahmen zum Schutz der Gesundheit des Antragstellers oder zum Schutz der öffentlichen Gesundheit keine Fingerabdrücke abgenommen werden können, ist es den Mitgliedstaaten gestattet, abweichend von Absatz 1 so rasch wie möglich,

spätestens aber 48 Stunden, nachdem diese Maßnahmen aufgehoben wurden, die Fingerabdrücke abzunehmen und zu übermitteln.

↓ 2725/2000/EG (angepasst)
⇒ neu

3. ~~⊗~~ Mit Ausnahme der gemäß Artikel 10 Buchstabe b übermittelten Daten ~~⊗~~ werden von einem Mitgliedstaat übermittelte Die Fingerabdruckdaten im Sinne von nach Artikel 5(1) 11 Buchstabe (b) a, die von einem Mitgliedstaat übermittelt wurden, ⇒ automatisch ⇐ ~~werden von der Zentraleinheit mit den von anderen Mitgliedstaaten übermittelten und in der zentralen Datenbank bereits gespeicherten Fingerabdruckdaten verglichen~~ Fingerabdruckdaten abgeglichen, die andere Mitgliedstaaten übermittelt haben und die bereits ~~in der Zentraldatenbank~~ ⇒ im Zentralsystem ⇐ gespeichert sind.
4. ~~Die Zentraleinheit~~ ⇒ Das Zentralsystem ⇐ ~~veranlasst trägt~~ auf Antrag eines Mitgliedstaates ~~dafür Sorge,~~ dass ~~sich der Vergleich beim Abgleich nach Absatz 3 neben den außer auf die Daten anderer Mitgliedstaaten auch auf die von diesem Mitgliedstaat früher zu einem früheren Zeitpunkt übermittelten Fingerabdruckdaten erstreckt~~ abgeglichen werden.
5. ~~Die Zentraleinheit~~ ⇒ Das Zentralsystem ⇐ übermittelt ~~unverzüglich~~ den Treffer oder das negative Ergebnis des ~~Abgleichs Vergleichs~~ ⇒ automatisch ⇐ an den Herkunftsmitgliedstaat. Liegt ein Treffer vor, übermittelt ~~sie es~~ zu allen mit dem Treffer in Zusammenhang stehenden Datensätzen die Daten ~~gemäß nach Artikel 5 Absatz 18 Buchstaben a bis (⇒ g ⇐), die Daten gemäß Artikel 5 Absatz 1 Buchstabe b) werden jedoch nur übermittelt, soweit sie Grundlage für den Treffer waren~~ ⇒ , gegebenenfalls zusammen mit den markierten Daten nach Artikel 18 Absatz 1 ⇐.

~~Eine direkte Übermittlung des Ergebnisses des Vergleichs an den Herkunftsmitgliedstaat ist zulässig, wenn die technischen Voraussetzungen dafür erfüllt sind.~~

- ~~7. Die Durchführungsbestimmungen über die zur Anwendung der Absätze 1 bis 6 erforderlichen Verfahren werden gemäß dem Verfahren nach Artikel 22 Absatz 1 festgelegt.~~

↓ neu

Artikel 10

Informationen zur Rechtsstellung der betroffenen Person

Die nachstehenden Informationen werden an das Zentralsystem übermittelt und dort im Einklang mit Artikel 9 zum Zwecke der Übermittlung gemäß Artikel 9 Absatz 5 gespeichert:

- (a) Wenn eine Person, die internationalen Schutz beantragt hat, oder eine andere Person nach Artikel 18 Absatz 1 Buchstabe d der Dublin-Verordnung im Zuge einer Überstellung nach Annahme eines Wiederaufnahmegesuchs gemäß Artikel 24 der Dublin-Verordnung in dem Mitgliedstaat ankommt, der für die Prüfung des Antrags auf internationalen Schutz zuständig

ist, aktualisiert dieser seinen gemäß Artikel 8 gespeicherten Datensatz zu der betreffenden Person durch Hinzufügung des Zeitpunkts ihrer Ankunft.

- (b) Wenn eine Person, die internationalen Schutz beantragt hat, im Zuge einer Überstellung nach Annahme eines Aufnahmegesuchs gemäß Artikel 22 der Dublin-Verordnung in dem Mitgliedstaat ankommt, der für die Prüfung des Antrags auf internationalen Schutz zuständig ist, übermittelt dieser seinen gemäß Artikel 11 gespeicherten Datensatz zu der betreffenden Person, dem er den Zeitpunkt ihrer Ankunft hinzugefügt hat.
- (c) Sobald der Herkunftsmitgliedstaat nachweisen kann, dass die betreffende Person, deren Daten gemäß Artikel 11 in EURODAC gespeichert sind, das Hoheitsgebiet der Mitgliedstaaten verlassen hat, aktualisiert er seinen gemäß Artikel 11 gespeicherten Datensatz zu der betreffenden Person durch Hinzufügung des Zeitpunkts, zu dem die Person das Hoheitsgebiet verlassen hat, um die Anwendung des Artikels 19 Absatz 2 und des Artikels 20 Absatz 5 der Dublin-Verordnung zu erleichtern.
- (d) Sobald der Herkunftsmitgliedstaat gewährleistet, dass die betreffende Person, deren Daten gemäß Artikel 11 in EURODAC gespeichert sind, das Hoheitsgebiet der Mitgliedstaaten aufgrund eines Rückführungsbeschlusses oder einer Abschiebungsanordnung verlassen hat, denen eine Rücknahme oder Ablehnung des Antrags gemäß Artikel 19 Absatz 3 der Dublin-Verordnung vorangegangen ist, aktualisiert er seinen gemäß Artikel 11 gespeicherten Datensatz zu der betreffenden Person durch Hinzufügung des Zeitpunkts, zu dem die Person abgeschoben wurde oder das Hoheitsgebiet verlassen hat.
- (e) Der Mitgliedstaat, der gemäß Artikel 17 Absatz 1 der Dublin-Verordnung die Verantwortung für die Prüfung des Antrags übernimmt, aktualisiert seinen gemäß Artikel 11 gespeicherten Datensatz zu der betreffenden Person durch Hinzufügung des Zeitpunkts, zu dem die Entscheidung, den Antrag zu prüfen, getroffen wurde.

↓ 2725/2000/EG
⇒ neu

Artikel ~~11~~ Datenspeicherung

~~In der zentralen Datenbank~~ ⇒ Im Zentralsystem ⇐ werden ausschließlich folgende Daten gespeichert:

(~~a~~) Fingerabdruckdaten;

(~~b~~) Herkunftsmitgliedstaat, Ort und Zeitpunkt ~~der Stellung des Asylantrags~~ ⇒ , zu dem der Antrag auf internationalen Schutz gestellt wurde; ⇐ ⇒ in den Fällen nach Artikel 10 Buchstabe b ist unter Zeitpunkt der Antragstellung das Datum anzugeben, das der Mitgliedstaat, der den Antragsteller überstellt hat, eingegeben hat. ⇐

(c) Geschlecht;

- (d) vom Herkunftsmitgliedstaat verwendete Kennnummer;
- (e) Zeitpunkt der Abnahme der Fingerabdrücke;
- (f) Zeitpunkt der Übermittlung der Daten an ~~die Zentraleinheit~~; ⇒ das Zentralsystem ⇐
- ~~(g) Zeitpunkt der Eingabe der Daten in die zentrale Datenbank;~~

↓ neu

(g) Benutzerkennwort

↓ 2725/2000/EC
⇒ neu

~~(h) Angaben zu dem/den Empfänger(n), an den/die die Daten übermittelt wurden, sowie Zeitpunkt(e) der Übermittlung(en).~~

(h) gegebenenfalls gemäß Artikel 10 Buchstabe a oder Buchstabe b der Zeitpunkt der Ankunft der betreffenden Person nach einer erfolgreichen Überstellung

(i) gegebenenfalls gemäß Artikel 10 Buchstabe c der Zeitpunkt, zu dem die betreffende Person das Hoheitsgebiet der Mitgliedstaaten verlassen hat

(j) gegebenenfalls gemäß Artikel 10 Buchstabe d der Zeitpunkt, zu dem die betreffende Person das Hoheitsgebiet der Mitgliedstaaten verlassen hat oder abgeschoben wurde

(k) gegebenenfalls gemäß Artikel 10 Buchstabe e der Zeitpunkt, zu dem die Prüfung des Antrags beschlossen wurde

~~2. Die Zentraleinheit vernichtet nach der Speicherung der Daten in der zentralen Datenbank die zur Datenübermittlung verwendeten Datenträger, sofern der Herkunftsmitgliedstaat nicht deren Rückgabe verlangt hat.~~

Artikel 12 ~~6~~ **Aufbewahrung der Daten**

Jeder Datensatz nach Artikel ~~5 Absatz 1~~ 11 wird ~~für zehn Jahre~~ ab dem Zeitpunkt der Abnahme der Fingerabdrücke zehn Jahre ~~in der zentralen Datenbank~~ ⇒ im Zentralsystem ⇐ aufbewahrt.

Nach Ablauf dieses Zeitraums ~~löscht die Zentraleinheit automatisch die Daten in der zentralen Datenbank~~ werden die Daten im ~~Zentraleinheit~~ ⇒ Zentralsystem ⇐ automatisch gelöscht.

Artikel 13 ~~7~~

Vorzeitige Löschung der Daten

1. Daten über Personen, die vor Ablauf des in Artikel 12 genannten Zeitraums die Staatsbürgerschaft ~~Staatsangehörigkeit~~ eines Mitgliedstaats erworben haben, ~~bevor der in Artikel 6 genannte Zeitraum abgelaufen ist,~~ werden, ~~sobald der Herkunftsmitgliedstaat davon Kenntnis erhält, dass die betreffende Person die Staatsangehörigkeit eines Mitgliedstaats erworben hat,~~ gemäß Artikel ~~15 Absatz 3~~ 27 Absatz 4 in der zentralen Datenbank ⇨ im Zentralsystem ⇩ gelöscht, sobald der Herkunftsmitgliedstaat Kenntnis davon erhält, dass die betreffende Person die Staatsbürgerschaft eines Mitgliedstaats erworben hat.

↓ neu

2. Das Zentralsystem informiert alle Herkunftsmitgliedstaaten über die Löschung von Daten aus dem in Absatz 1 genannten Grund durch einen anderen Herkunftsmitgliedstaat, nachdem dieser mit Daten, die sie zu Personen nach Artikel 9 Absatz 1 oder nach Artikel 14 Absatz 1 übermittelt hatten, einen Treffer erzielt hat.

↓ 2725/2000/EG (angepasst)

⇨ neu

KAPITEL III

AUSLÄNDER ~~⊗~~ DRITTSTAATSANGEHÖRIGE ODER STAATENLOSE ~~⊗~~ , DIE IN VERBINDUNG MIT DEM ILLEGALEN ÜBERSCHREITEN EINER AUSSENGRENZEN BEIM RECHTSWIDRIGEN ÜBERSCHREITEN EINER AUSSENGRENZE AUFGEGRIFFEN WERDEN

Artikel 14 ~~8~~

Erfassung und Übermittlung von Fingerabdruckdaten

1. Jeder Mitgliedstaat nimmt unter Beachtung der in der Europäischen Menschenrechtskonvention und im Übereinkommen der Vereinten Nationen über die Rechte des Kindes verankerten Schutzklauseln jedem mindestens 14 Jahre alten Ausländer ~~⊗~~ Drittstaatsangehörigen oder Staatenlosen ~~⊗~~, der mindestens vierzehn Jahre alt ist und der in Verbindung mit dem illegalen Überschreiten – aus einem Drittstaat kommend – beim rechtswidrigen Überschreiten der Grenze dieses Mitgliedstaats auf dem Land-, See- oder Luftwege aus einem Drittstaat kommend von den zuständigen Kontrollbehörden aufgegriffen und nicht zurückgewiesen wird ⇨ oder der sich weiterhin im Hoheitsgebiet der Mitgliedstaaten aufhält und während des Zeitraums zwischen dem Aufgreifen und der Abschiebung auf der Grundlage eines Rückführungsbeschlusses nicht in Haft oder

Gewahrsam genommen oder dessen Bewegungsfreiheit nicht in anderer Weise räumlich beschränkt wurde \Leftarrow , unverzüglich ~~die Fingerabdrücke~~ den Abdruck aller Finger ab.

2. Der betreffende Mitgliedstaat übermittelt ~~der Zentraleinheit~~ unverzüglich ~~die folgenden Daten im Zusammenhang mit jedem~~ \Rightarrow so rasch wie möglich, spätestens aber 72 Stunden, nachdem \Leftarrow ~~Ausländer~~ \boxtimes der Drittstaatsangehörige oder Staatenlose \boxtimes ~~nach~~ gemäß Absatz 1, der nicht zurückgewiesen wird, \Rightarrow aufgegriffen wurde, \Leftarrow die folgenden Daten zu dieser Person \Rightarrow an das Zentralsystem \Leftarrow :

(~~a~~) Fingerabdruckdaten $\frac{2}{3}$

(~~b~~) Herkunftsmitgliedstaat, Ort und Zeitpunkt ~~des Aufgreifens~~, zu dem die Person aufgegriffen wurde

(c) Geschlecht $\frac{2}{3}$

(d) vom Herkunftsmitgliedstaat verwendete Kennnummer $\frac{2}{3}$

(e) Zeitpunkt der Abnahme der Fingerabdrücke $\frac{2}{3}$

(f) Zeitpunkt der Übermittlung der Daten an ~~die Zentraleinheit~~, \Rightarrow das Zentralsystem \Leftarrow

\Downarrow neu

(g) Benutzerkennwort

3. In Fällen, in denen Personen, die in der in Absatz 1 beschriebenen Weise aufgegriffen wurden und sich weiterhin im Hoheitsgebiet der Mitgliedstaaten aufhalten, aber, nachdem sie aufgegriffen wurden, für einen Zeitraum von mehr als 72 Stunden in Haft oder Gewahrsam genommen wurden oder deren Bewegungsfreiheit in anderer Weise räumlich beschränkt wurde, werden die in Absatz 2 genannten Daten zu diesen Personen abweichend von Absatz 2 vor ihrer Entlassung aus der Haft oder dem Gewahrsam oder vor Aufhebung der räumlichen Beschränkung ihrer Bewegungsfreiheit übermittelt.
4. Die Nichteinhaltung der Frist von 72 Stunden entbindet die Mitgliedstaaten nicht von der Verpflichtung, die Fingerabdrücke abzunehmen und an das Zentralsystem zu übermitteln. Können aufgrund des Zustands der Fingerkuppen keine Fingerabdrücke in einer Qualität abgenommen werden, die einen angemessenen Abgleich nach Artikel 25 gewährleistet, nimmt der Herkunftsmitgliedstaat erneut die Fingerabdrücke der betreffenden Person ab und übermittelt diese so rasch wie möglich, spätestens aber 48 Stunden nach erfolgreicher Abnahme.
5. In Fällen, in denen aufgrund von Maßnahmen zum Schutz der Gesundheit des Antragstellers oder zum Schutz der öffentlichen Gesundheit keine Fingerabdrücke abgenommen werden können, ist es den Mitgliedstaaten gestattet, abweichend von Absatz 1 innerhalb der in Absatz 2 festgelegten Frist, nachdem diese Maßnahmen aufgehoben wurden, die Fingerabdrücke abzunehmen und zu übermitteln.

Artikel ~~15~~ 9

Datenspeicherung

1. Die ~~in Artikel 5 Absatz 1 Buchstabe g) und in Artikel 8 Absatz 2 14 Absatz 2 genannten~~ aufgeführten Daten werden ~~in der zentralen Datenbank~~ ⇒ im Zentralsystem ⇐ gespeichert.

Unbeschadet des Artikels ~~3 Absatz 3~~ 8 werden Daten, die ~~der Zentraleinheit~~ ⇒ dem Zentralsystem ⇐ gemäß Artikel ~~8~~ 14 Absatz 2 übermittelt werden, ~~in der zentralen Datenbank~~ ausschließlich zum Zwecke des ~~Vergleichs~~ Abgleichs mit in der Folge an die ~~Zentraleinheit~~ ⇒ das Zentralsystem ⇐ übermittelten Daten ~~über Asylbewerber~~ ⇒ zu Personen, die internationalen Schutz beantragen, ⇐ gespeichert.

~~Die Zentraleinheit~~ ⇒ Das Zentralsystem ⇐ darf ~~ihre~~ gemäß Artikel ~~8~~ 14 Absatz 2 übermittelte Daten weder mit zuvor ~~in der zentralen Datenbank~~ ⇒ im Zentralsystem ⇐ gespeicherten Daten noch mit Daten ~~vergleichen~~ abgleichen, die ~~der Zentraleinheit~~ ⇒ dem Zentralsystem ⇐ in der Folge gemäß Artikel ~~8~~ 14 Absatz 2 übermittelt werden.

2. ~~Die in Artikel 4 Absatz 1 zweiter Satz, Artikel 4 Absatz 2 und Artikel 5 Absatz 2 vorgesehenen Verfahren sowie die aufgrund von Artikel 4 Absatz 7 erlassenen Bestimmungen finden Anwendung. Was den Vergleich Für den Abgleich~~ von in der Folge an die ~~Zentraleinheit~~ ⇒ das Zentralsystem ⇐ übermittelten Daten ~~über Asylbewerber~~ ⇒ zu Personen, die internationalen Schutz beantragen, ⇐ mit den in Absatz 1 genannten Daten ~~anbelangt, so~~ gelten die in Artikel ~~4 Absätze 3, 5 und 6~~ 9 Absätze 3 und 5 sowie in Artikel 25 Absatz 4 vorgesehenen Verfahren.

Artikel ~~16~~ 10

Aufbewahrung der Daten

1. Jeder Datensatz ~~betreffend einen zu einem Ausländer~~ ⊗ Drittstaatsangehörigen oder Staatenlosen ⊗ nach Artikel ~~8 Absatz 1~~ 14 Absatz 1 wird für ⇒ ein Jahr ⇐ ~~zwei Jahre~~ ab dem Zeitpunkt der Abnahme der Fingerabdrücke des ~~Ausländers~~ ⊗ Drittstaatsangehörigen oder Staatenlosen ⊗ ~~in der zentralen Datenbank~~ ⇒ im Zentralsystem ⇐ aufbewahrt. Nach Ablauf dieses Zeitraums ~~löscht die Zentraleinheit automatisch die Daten in der zentralen Datenbank~~ werden die Daten ~~in der Zentraleinheit~~ ⇒ im Zentralsystem ⇐ automatisch gelöscht.

2. Daten ~~über einen Ausländer~~ ⊗ zu Drittstaatsangehörigen oder Staatenlosen ⊗ nach Artikel ~~8 Absatz 1~~ 14 Absatz 1 werden unverzüglich gemäß Artikel ~~15 Absatz 3~~ 28 Absatz 3 ~~in der zentralen Datenbank~~ ⇒ aus dem Zentralsystem ⇐ gelöscht, ~~wenn~~ ⊗ sobald ⊗ dem Herkunftsmitgliedstaat vor Ablauf des ~~Zweijahreszeitraums~~ ⇒ Einjahreszeitraums ⇐ nach Absatz 1 einer der folgenden Umstände bekannt wird:

- (a) dem ~~Ausländer~~ ⊗ Drittstaatsangehörigen oder Staatenlosen ⊗ wurde eine Aufenthaltsgenehmigung ⊗ ein Aufenthaltstitel ⊗ erteilt;

- (b) der ~~Ausländer~~ ☒ Drittstaatsangehörige oder Staatenlose ☒ hat das Hoheitsgebiet der Mitgliedstaaten verlassen;
- (c) der ~~Ausländer~~ ☒ Drittstaatsangehörige oder Staatenlose ☒ hat die Staatsbürgerschaft ~~Staatsangehörigkeit~~ eines Mitgliedstaats erworben ~~angenommen~~.

↓ neu

3. Das Zentralsystem informiert alle Herkunftsmitgliedstaaten über die Löschung von Daten aus einem in Absatz 2 Buchstabe a oder b genannten Grund durch einen anderen Herkunftsmitgliedstaat, nachdem dieser mit Daten, die die Herkunftsmitgliedstaaten zu Personen nach Artikel 14 Absatz 1 übermittelt hatten, einen Treffer erzielt hat.
4. Das Zentralsystem informiert alle Herkunftsmitgliedstaaten über die Löschung von Daten aus einem in Absatz 2 Buchstabe c genannten Grund durch einen anderen Herkunftsmitgliedstaat, nachdem dieser mit Daten, die die Herkunftsmitgliedstaaten zu Personen nach Artikel 9 Absatz 1 oder Artikel 14 Absatz 1 übermittelt hatten, einen Treffer erzielt hat.

↓ 2725/2000/EG (angepasst)

⇒ neu

KAPITEL IV

~~AUSLÄNDER~~ ☒ DRITTSTAATSANGEHÖRIGE ODER STAATENLOSE ☒ , DIE SICH ILLEGAL IN EINEM MITGLIEDSTAAT AUFHALTEN

Artikel 17 ~~II~~

Vergleich der Abgleich von Fingerabdruckdaten

1. Um zu überprüfen, ob ein ~~Ausländer~~ ☒ Drittstaatsangehöriger oder Staatenloser ☒, der sich illegal im Hoheitsgebiet eines Mitgliedstaats aufhält, zu einem früheren Zeitpunkt einen ~~Asylantrag~~ ⇒ Antrag auf internationalen Schutz ⇐ in einem anderen Mitgliedstaat gestellt hat, kann ~~der jeder~~ Mitgliedstaat ~~der Zentraleinheit~~ ⇒ dem Zentralsystem ⇐ die ~~Daten betreffend Fingerabdrücke~~ Fingerabdruckdaten, die er ~~gegebenenfalls von~~ einem solchen mindestens 14 Jahre alten ~~Ausländer~~ ☒ Drittstaatsangehörigen oder Staatenlosen ☒ ~~gegebenenfalls~~ abgenommen hat, zusammen mit der von diesem Mitgliedstaat verwendeten Kennnummer übermitteln.

Eine Überprüfung, ob der ~~Ausländer~~ ☒ Drittstaatsangehörige oder Staatenlose ☒ zu einem früheren Zeitpunkt bereits einen ~~Asylantrag~~ ⇒ Antrag auf internationalen Schutz ⇐ in einem anderen Mitgliedstaat gestellt hat, ist in der Regel begründet, wenn:

- (a) der ~~Ausländer~~ Drittstaatsangehörige oder Staatenlose erklärt, dass er einen ~~Asylantrag~~ Antrag auf internationalen Schutz gestellt habe, jedoch den Mitgliedstaat der Antragstellung nicht angibt;
- (b) der ~~Ausländer~~ Drittstaatsangehörige oder Staatenlose ~~kein Asyl beantragt~~ keinen Antrag auf internationalen Schutz stellt , die Rückführung in sein Herkunftsland jedoch mit der Begründung ablehnt, ~~dass er dort in Gefahr wäre~~, er sei dort in Gefahr, oder
- (c) der ~~Ausländer~~ Drittstaatsangehörige oder Staatenlose seine Abschiebung anderweitig zu verhindern versucht, indem er es ablehnt, bei der Feststellung seiner Identität mitzuwirken, vor allem indem er keine oder gefälschte Ausweispapiere vorlegt.
2. Soweit die Mitgliedstaaten an dem in Absatz 1 bezeichneten Verfahren teilnehmen, übermitteln sie ~~der Zentraleinheit~~ dem Zentralsystem ~~die Abdruckdaten~~ den Abdruck aller Finger oder zumindest der Zeigefinger der ~~Ausländer~~ Drittstaatsangehörigen oder Staatenlosen gemäß Absatz 1; wenn letztere fehlen, übermitteln sie ~~die Abdrücke~~ den Abdruck aller sonstigen Finger.
3. Die Fingerabdruckdaten von ~~Ausländern~~ Drittstaatsangehörigen oder Staatenlosen nach Absatz 1 werden ~~der Zentraleinheit~~ dem Zentralsystem ausschließlich zum Zwecke des ~~Vergleichs~~ Abgleichs mit den von anderen Mitgliedstaaten übermittelten und im Zentralsystem bereits gespeicherten Fingerabdruckdaten von Asylbewerbern Personen, die internationalen Schutz beantragen, übermittelt, die von anderen Mitgliedstaaten übermittelt wurden und bereits in der zentralen Datenbank gespeichert worden sind sind.
- Die Fingerabdruckdaten ~~soleher~~ ~~Ausländer~~ dieser Drittstaatsangehörigen oder Staatenlosen werden nicht weder in der zentralen Datenbank im Zentralsystem gespeichert und auch nicht noch mit den ~~der Zentraleinheit~~ dem Zentralsystem gemäß Artikel ~~8 Absatz 2~~ 14 Absatz 2 übermittelten Daten vergleichen abgeglichen.
4. ~~Was den Vergleich~~ Für den Abgleich von nach diesem Artikel übermittelten Fingerabdruckdaten mit den von anderen Mitgliedstaaten übermittelten und bereits in der Zentraleinheit im Zentralsystem gespeicherten Fingerabdruckdaten von Asylbewerbern Personen, die internationalen Schutz beantragen , anbelangt, so finden gelten die in Artikel ~~4 Absätze 3, 5 und 6~~ 9 Absätze 3 und 5 vorgesehenen Verfahren sowie die gemäß Artikel 4 Absatz 7 erlassenen Bestimmungen Anwendung.
- ~~5. Sobald die Ergebnisse des Vergleichs dem Herkunftsmitgliedstaat übermittelt worden sind,~~
- a) ~~löscht die Zentraleinheit unverzüglich die Fingerabdruckdaten und andere ihr nach Absatz 1 übermittelte Daten und~~
- b) ~~vernichtet unverzüglich die vom Herkunftsmitgliedstaat für die Übermittlung der Daten an die Zentraleinheit verwendeten Datenträger, sofern der Herkunftsmitgliedstaat nicht deren Rückgabe verlangt hat.~~

KAPITEL V

~~ANERKANNTE FLÜCHTLINGE~~ ☒ PERSONEN, DENEN INTERNATIONALER SCHUTZ GEWÄHRT WIRD ☒

~~Artikel 12~~

~~Sperrung von Daten~~

~~1. Daten über einen Asylbewerber, die gemäß Artikel 4 Absatz 2 gespeichert worden sind, werden in der zentralen Datenbank gesperrt, wenn die betreffende Person in einem Mitgliedstaat als Flüchtling anerkannt und zugelassen worden ist. Eine solche Sperrung wird von der Zentraleinheit auf Anweisung des Herkunftsmitgliedstaats vorgenommen.~~

~~Solange noch keine Entscheidung gemäß Absatz 2 getroffen worden ist, werden Treffer bezüglich Personen, die in einem Mitgliedstaat als Flüchtling anerkannt und zugelassen wurden, nicht übermittelt. Die Zentraleinheit teilt dem anfragenden Mitgliedstaat ein negatives Ergebnis mit.~~

~~2. Fünf Jahre nach Aufnahme der Tätigkeit von Eurodac wird anhand von der Zentraleinheit erstellter verlässlicher Statistiken über die Personen, die in einem Mitgliedstaat einen Asylantrag gestellt haben, nachdem sie in einem anderen Mitgliedstaat als Flüchtling anerkannt und zugelassen worden sind, gemäß den einschlägigen Bestimmungen des Vertrags darüber entschieden, ob die Daten über Personen, die in einem Mitgliedstaat als Flüchtling anerkannt und zugelassen worden sind,~~

~~(a) entweder gemäß Artikel 6 zum Zwecke des Vergleichs nach Artikel 4 Absatz 3 gespeichert werden sollten oder~~

~~(b) vorzeitig gelöscht werden sollten, sobald eine Person als Flüchtling anerkannt und zugelassen worden ist.~~

~~3. In dem in Absatz 2 Buchstabe a) angeführten Fall werden die gemäß Absatz 1 gesperrten Daten freigegeben, und das in Absatz 1 genannte Verfahren wird nicht länger angewandt.~~

~~4. In dem in Absatz 2 Buchstabe b) angeführten Fall werden~~

~~(a) Daten, die gemäß Absatz 1 gesperrt worden sind, von der Zentraleinheit unverzüglich gelöscht und~~

~~(b) Daten über Personen, die in der Folge als Flüchtling anerkannt und zugelassen werden, entsprechend Artikel 15 Absatz 3 gelöscht, sobald der Herkunftsmitgliedstaat davon Kenntnis erhält, dass die betreffende Person in einem Mitgliedstaat als Flüchtling anerkannt und zugelassen worden ist.~~

~~5. Die Durchführungsbestimmungen für die Sperrung von Daten nach Absatz 1 und die Erstellung der Statistiken nach Absatz 2 werden nach dem in Artikel 22 Absatz 1 vorgesehenen Verfahren angenommen.~~

↓ neu

Artikel 18

Datenmarkierung

1. Der Herkunftsmitgliedstaat, der einer Person, die internationalen Schutz beantragt hat und deren Daten gemäß Artikel 11 zuvor im Zentralsystem gespeichert wurden, internationalen Schutz gewährt hat, markiert die relevanten Daten im Einklang mit den von der Agentur festgelegten Bestimmungen für elektronische Kommunikation mit dem Zentralsystem. Diese Markierung wird gemäß Artikel 12 für Datenübermittlungszwecke nach Artikel 9 Absatz 5 im Zentralsystem gespeichert.
 2. Der Herkunftsmitgliedstaat entfernt die Markierung von Daten zu Drittstaatsangehörigen oder Staatenlosen, deren Daten zuvor gemäß Absatz 1 markiert worden waren, wenn der ihnen gewährte Schutzstatus nach Artikel 14 oder 19 der Richtlinie 2004/83/EG aberkannt, beendet oder eine Verlängerung abgelehnt wird.
-

↓ neu

KAPITEL VI

VERFAHREN FÜR DEN ABGLEICH UND DIE ÜBERTRAGUNG VON DATEN FÜR STRAFVERFOLGUNGSZWECKE

Artikel 19

Verfahren für den Abgleich von Fingerabdruckdaten mit EURODAC-Daten

1. Die in Artikel 5 Absatz 1 genannten Behörden und Europol können in elektronischer Form einen begründeten Antrag an die Prüfstelle richten und ersuchen diese damit um die Übermittlung von Fingerabdruckdaten an das EURODAC-Zentralsystem über die nationale Zugangsstelle zwecks Datenabgleichs. Erhält die Prüfstelle einen solchen Antrag, prüft sie, ob die Bedingungen des Artikels 20 oder 21 für die Beantragung des Abgleichs erfüllt sind.
2. Sind sämtliche Bedingungen für die Beantragung des Abgleichs erfüllt, übermittelt die Prüfstelle den Antrag auf Abgleich der nationalen Zugangsstelle, die diesen zwecks Abgleichs mit den EURODAC-Daten in die EURODAC-Zentraldatenbank eingibt.

3. In dringenden Ausnahmefällen kann die Prüfstelle bei Erhalt eines Antrags einer benannten Behörde die Fingerabdruckdaten unverzüglich der nationalen Zugangsstelle übermitteln und nachträglich überprüfen, ob alle Bedingungen des Artikels 20 oder 21 erfüllt sind; überprüft wird auch, ob tatsächlich ein dringender Ausnahmefall gegeben war. Die nachträgliche Überprüfung ist unverzüglich nach der Bearbeitung des Antrags durchzuführen.
4. Wird bei der nachträglichen Überprüfung festgestellt, dass der Zugang nicht berechtigt war, löschen die Behörden, die Zugang zu den aus EURODAC erhaltenen Informationen hatten, diese Informationen und melden die Löschung der Prüfstelle.

Artikel 20

Bedingungen für den Zugang benannter Behörden zu EURODAC-Daten

1. Die benannten Behörden können im Rahmen ihrer Zuständigkeiten nur dann den Abgleich von Fingerabdruckdaten mit den Daten in der EURODAC-Zentraldatenbank beantragen, wenn der Abgleich mit den Daten der nationalen Fingerabdruck-Datenbanken des Mitgliedstaats und der automatisierten daktyloskopischen Identifizierungssysteme der anderen Mitgliedstaaten nach dem Beschluss 2008/615/JI ergebnislos war und
 - (a) für die Verhütung, Aufdeckung oder Untersuchung terroristischer oder sonstiger schwerer Straftaten erforderlich ist;
 - (b) im Einzelfall erforderlich ist, wobei kein systematischer Abgleich stattfindet, und
 - (c) berechtigte Gründe für die Annahme vorliegen, dass der Abgleich mit EURODAC-Daten zur Verhütung, Aufdeckung oder Untersuchung der fraglichen Straftaten beitragen wird.
2. Anträge auf Abgleich mit EURODAC-Daten sind auf Abfragen anhand von Fingerabdruckdaten beschränkt.

Artikel 21

Bedingungen für den Zugang von Europol zu EURODAC-Daten

1. Europol kann im Rahmen seines Mandats für spezifische Analysezwecke sowie für allgemeine und strategische Analysen Anträge auf Abgleich mit EURODAC-Daten stellen, wenn dies zur Erfüllung seiner Aufgaben gemäß dem Europol-Beschluss notwendig ist.
2. Anträge auf Abgleich mit EURODAC-Daten sind auf die Fingerabdruckdaten beschränkt.
3. Die Verarbeitung der von Europol durch den Abgleich mit EURODAC-Daten erlangten Informationen unterliegt der Zustimmung des Mitgliedstaats, der die betreffenden Daten in das System eingegeben hat. Die Zugangsberechtigung ist über die nationale Europol-Zentralstelle des betreffenden Mitgliedstaats einzuholen.

Kommunikation zwischen den Prüfstellen und den nationalen Zugangsstellen

1. Für die Übermittlung von Daten zwischen den Prüfstellen der Mitgliedstaaten und Europol und den nationalen Zugangsstellen wird die EURODAC-Kommunikationsinfrastruktur verwendet. Die Kommunikation erfolgt ausschließlich auf elektronischem Weg.
2. Die Fingerabdrücke werden von den Mitgliedstaaten digitalisiert und im Datenformat nach Anhang I übermittelt, um sicherzustellen, dass der Abgleich mit einem automatisierten Fingerabdruckidentifizierungssystem vorgenommen werden kann.

↓ 2725/2000/EG (angepasst)
⇒ neu

KAPITEL ~~VI~~ VII

DATENVERARBEITUNG~~VERWENDUNG DER DATEN,~~ DATENSCHUTZ~~, SICHERHEIT~~ UND HAFTUNG

Artikel ~~23~~ 13

Verantwortung für die Verwendung der Datenverarbeitung

1. Der Herkunftsmitgliedstaat ist verantwortlich für
 - (a) die Rechtmäßigkeit der Abnahme der Fingerabdrücke;
 - (b) die Rechtmäßigkeit der Übermittlung der Fingerabdruckdaten sowie ~~der übrigen sonstiger~~ Daten nach Artikel ~~5 Absatz 1~~ 11, Artikel ~~8 Absatz 1~~ 14 Absatz 2 und Artikel ~~11 Absatz 2~~ 17 Absatz 2 an ~~die Zentraleinheit~~ ⇒ das Zentralsystem ⇐;
 - (c) die Richtigkeit und die Aktualität der Daten bei deren Übermittlung an ~~die Zentraleinheit~~ ⇒ das Zentralsystem ⇐;
 - (d) die Rechtmäßigkeit der Speicherung, Aufbewahrung, Berichtigung und Löschung der Daten ~~in der zentralen Datenbank~~ ⇒ im Zentralsystem ⇐ unbeschadet der Verantwortung der ~~Kommission~~ ⇒ Agentur ⇐;
 - (e) die Rechtmäßigkeit der ~~Verwendung~~ Verarbeitung der ~~von der Zentraleinheit~~ ⇒ vom Zentralsystem ⇐ übermittelten Ergebnisse des ~~Vergleichs~~ Abgleichs der Fingerabdruckdaten.
2. Gemäß Artikel ~~14~~ 34 trägt der Herkunftsmitgliedstaat für die Sicherheit der Daten nach Absatz 1 vor und bei der Übermittlung an ~~die Zentraleinheit~~ ⇒ das Zentralsystem ⇐ sowie für die Sicherheit der Daten, die er ~~von der Zentraleinheit~~ ⇒ vom Zentralsystem ⇐ empfängt, Sorge.

3. Der Herkunftsmitgliedstaat ist für die endgültige Identifizierung der Daten gemäß Artikel ~~4 Absatz 6~~ 25 Absatz 4 verantwortlich.
4. Die ~~Kommission~~ Agentur trägt dafür Sorge, dass ~~die Zentraleinheit~~ das Zentralsystem gemäß den Bestimmungen der Verordnung ~~und ihren Durchführungsbestimmungen~~ betrieben wird. Insbesondere gewährleistet die Agentur Folgendes:
- (a) ~~sie trifft sie~~ Maßnahmen, um ~~dafür zu sorgen~~ zu gewährleisten, dass ~~in der Zentraleinheit tätige~~ mit dem Zentralsystem arbeitende Personen die darin ~~in der zentralen Datenbank~~ gespeicherten Daten nur in einer ~~dem in Artikel 1 Absatz 1 genannten Zweck von Eurodac entsprechenden~~ Weise ~~verwenden~~ verarbeiten, die dem mit EURODAC verfolgten Zweck nach Artikel 1 Absatz 1 entspricht;
- ~~(b) stellt sie sicher, dass die in der Zentraleinheit tätigen Personen allen Aufforderungen nachkommen, die seitens der Mitgliedstaaten im Einklang mit der Verordnung in Bezug auf die Speicherung, den Vergleich, die Berichtigung und die Löschung von Daten, für die sie zuständig sind, ergehen;~~
- ~~(b)~~ (e) sie trifft sie die notwendigen Maßnahmen, um die Sicherheit ~~der Zentraleinheit~~ des Zentralsystems gemäß Artikel ~~14~~ 34 zu gewährleisten;
- ~~(c)~~ (d) sie stellt sie sicher, dass unbeschadet ~~des Artikels 20 und der Befugnisse der unabhängigen Kontrollinstanz, die gemäß Artikel 286 Absatz 2 des Vertrags eingerichtet wird,~~ der Befugnisse des Europäischen Datenschutzbeauftragten nur die zu einer Tätigkeit in der Zentraleinheit befugten Personen Zugang zu dem System ~~den in der zentralen Datenbank gespeicherten Daten~~ erhalten, die befugt sind, in der Zentraleinheit mit dem Zentralsystem zu arbeiten.

Die ~~Kommission~~ Agentur unterrichtet das Europäische Parlament, ~~und~~ den Rat sowie den Europäischen Datenschutzbeauftragten über die Maßnahmen, die sie gemäß Unterabsatz 1 ergreift.

↓ 407/2002/EG Artikel 2 (angepasst)
⇒ neu

Artikel 24 **Übermittlung**

1. Die Digitalisierung der ~~Fingerabdrücke~~ Fingerabdruckdaten und deren Übermittlung erfolgen in dem in Anhang I bezeichneten Datenformat. Die ~~Zentraleinheit~~ Agentur legt die technischen Anforderungen für die Übermittlung der Datenformate zwischen den Mitgliedstaaten und ~~der Zentraleinheit~~ dem Zentralsystem ~~und umgekehrt~~ fest, sofern dies für den effizienten Betrieb ~~der Zentraleinheit~~ des Zentralsystems erforderlich ist. Die ~~Zentraleinheit~~ Agentur stellt sicher, dass die von den Mitgliedstaaten übermittelten Fingerabdruckdaten im computergestützten Fingerabdruckerkennungssystem automatisierten Fingerabdruckidentifizierungssystem abgeglichen werden können.

2. Die Mitgliedstaaten ~~sollten~~ \boxtimes übermitteln \boxtimes die Daten nach Artikel ~~5 Absatz 1~~ 11 Absatz 1, Artikel 14 Absatz 2 und Artikel 17 Absatz 2 ~~der Eurodac-Verordnung~~ auf elektronischem Weg ~~übermitteln~~. \Rightarrow Die in Artikel 11 Absatz 1 und Artikel 14 Absatz 2 aufgeführten Daten werden automatisch im Zentralsystem gespeichert. \Leftarrow Die ~~Zentraleinheit~~ \boxtimes Agentur \boxtimes legt die technischen Voraussetzungen fest, ~~mit~~ unter denen eine ordnungsgemäße elektronische Übermittlung der Daten zwischen den Mitgliedstaaten und ~~der Zentraleinheit~~ \Rightarrow dem Zentralsystem \Leftarrow ~~und umgekehrt~~ gewährleistet werden kann, sofern dies für den effizienten Betrieb ~~der Zentraleinheit~~ \Rightarrow des Zentralsystems \Leftarrow erforderlich ist. ~~Die Übermittlung der Daten in Papierform anhand des Formblatts gemäß Anhang II oder auf sonstigen Datenträgern (Disketten, CD-ROM oder sonstigen in der Zukunft entwickelten und allgemein verwendeten Datenträger) sollte auf Fälle anhaltender technischer Störungen begrenzt bleiben.~~
3. Die Kennnummer nach Artikel ~~5 Absatz 1 Buchstabe d)~~ 11 Buchstabe d, Artikel 14 Absatz 2 Buchstabe d und Artikel 17 Absatz 1 ~~der Eurodac-Verordnung~~ muss die eindeutige Zuordnung der Daten zu einer bestimmten Person und zu dem ~~die Daten übermittelnden~~ Mitgliedstaat, ~~der die Daten übermittelt hat~~, ermöglichen. Weiterhin muss ~~sie die Aussage ermöglichen, sich anhand der Kennnummer feststellen lassen, ob sich diese die Daten sich auf einen Asylbewerber oder eine Person nach Artikel 8 oder Artikel 11 der Eurodac-Verordnung,~~ Artikel 14 oder Artikel 17 beziehen.
4. Die Kennnummer beginnt mit dem oder den Kennbuchstaben, mit dem oder denen gemäß der in Anhang I genannten Norm die ~~die Daten übermittelnden~~ Mitgliedstaaten bezeichnet werden, ~~die die Daten übermitteln~~. Dem oder den Kennbuchstaben folgt die Kennung für die Personenkategorien. Dabei werden Daten von ~~Asylbewerbern~~ \boxtimes Personen nach Artikel 9 Absatz 1 \boxtimes mit „1“, von Personen nach Artikel ~~8~~ 14 Absatz 1 ~~der Eurodac-Verordnung~~ mit „2“ und von Personen nach Artikel ~~11~~ 17 ~~der Eurodac-Verordnung~~ mit „3“ gekennzeichnet.
5. Die ~~Zentraleinheit~~ \boxtimes Agentur \boxtimes legt die ~~von den Mitgliedstaaten anzuwendenden~~ technischen Verfahren fest, ~~die die Mitgliedstaaten bei der Übermittlung der Daten an das mit denen gewährleistet werden kann, dass bei der Zentraleinheit~~ \Rightarrow Zentralsystem \Leftarrow ~~eindeutige Daten eingehen~~ anzuwenden haben, um die Eindeutigkeit der Daten zu gewährleisten.
64. ~~Die Zentraleinheit~~ \Rightarrow Das Zentralsystem \Leftarrow bestätigt den Empfang der übermittelten Daten unverzüglich. Zu diesem Zweck legt die ~~Zentraleinheit~~ \boxtimes Agentur \boxtimes die technischen ~~Anforderungen~~ Voraussetzungen fest, ~~mit~~ unter denen gewährleistet werden kann, dass die Mitgliedstaaten auf Anfrage eine Empfangsbestätigung erhalten.

Artikel 25 ~~3~~

Durchführung des Abgleichs Datenabgleich und Übermittlung der Ergebnisse

1. Die Mitgliedstaaten gewährleisten die Übermittlung der Fingerabdruckdaten in einer für einen Abgleich durch das ~~computergestützte Fingerabdruckererkennungssystem~~ geeigneten automatisierten Fingerabdruckidentifizierungssystem angemessenen Qualität. ~~Erforderlichenfalls definiert die Zentraleinheit die geeignete Qualität der übermittelten Fingerabdruckdaten, um zu gewährleisten, dass die von ihr vorgenommenen Abgleiche zu möglichst genauen Ergebnissen führen.~~ In dem Maße, in dem gewährleistet werden muss, dass ~~die~~ \Rightarrow vom Zentralsystem \Leftarrow erstellten Abgleichsergebnisse einen sehr hohen Grad an Präzision erreichen, ~~legt die~~ \Rightarrow Agentur \Leftarrow Kriterien für eine angemessene Qualität der zu übermittelnden Fingerabdruckdaten fest. ~~Die Zentraleinheit~~ \Rightarrow Das Zentralsystem \Leftarrow überprüft

unverzüglich die Qualität der übermittelten Fingerabdruckdaten. ~~Falls Sind die Fingerabdruckdaten für Abgleiche durch das computergestützte Fingerabdruckererkennungssystem automatisierte Fingerabdruckidentifizierungssystem ungeeignet sind, ersucht die Zentraleinheit den~~ \Rightarrow teilt es dies \Leftarrow dem betreffenden Mitgliedstaat ~~unverzüglich um Übermittlung qualitativ geeigneter Fingerabdruckdaten~~ \Rightarrow mit \Leftarrow . \Rightarrow Der Mitgliedstaat übermittelt \Leftarrow qualitativ geeignete Fingerabdruckdaten \Rightarrow , für die er die gleiche Kennnummer wie beim vorherigen Fingerabdruckdatenset verwendet \Leftarrow .

2. ~~Die Zentraleinheit~~ \Rightarrow Das Zentralsystem \Leftarrow führt die Abgleiche in der Reihenfolge des Eingangs der Anfragen durch. Jede Anfrage muss innerhalb von 24 Stunden bearbeitet ~~sein~~ werden. Ein Mitgliedstaat kann bei Anfragen nach Abgleichen, ~~die auf elektronischem Wege übermittelt wurden,~~ aus Gründen des innerstaatlichen Rechts verlangen, dass besonders eilbedürftige Abgleiche innerhalb einer Stunde durchgeführt werden. Können diese Bearbeitungszeiten aus Gründen, die die ~~Zentraleinheit~~ \Rightarrow Agentur \Leftarrow nicht zu vertreten hat, nicht eingehalten werden, bearbeitet ~~die Zentraleinheit~~ \Rightarrow das Zentralsystem \Leftarrow die Anfrage ~~nach Wegfall dieser Gründe~~ prioritär, sobald sich die Umstände geändert haben. In ~~diesen~~ ~~derartigen~~ Fällen legt die ~~Zentraleinheit~~ \Rightarrow Agentur \Leftarrow die Kriterien für die prioritäre Behandlung von Anfragen fest, sofern dies für den effizienten Betrieb ~~der Zentraleinheit~~ \Rightarrow des Zentralsystems \Leftarrow erforderlich ist.
3. Die ~~Zentraleinheit~~ \Rightarrow Agentur \Leftarrow legt die operativen Verfahren für die Verarbeitung der ~~empfangenen~~ eingegangenen Daten und für die Übermittlung ~~der Ergebnisse der Abgleiche~~ des Ergebnisses des Datenabgleichs fest, sofern dies für den effizienten Betrieb ~~der Zentraleinheit~~ \Rightarrow des Zentralsystems \Leftarrow erforderlich ist.

↓ 2725/2000/EG Artikel 4 Absatz 6
(angepasst)
 \Rightarrow neu

4. Die Ergebnisse des Vergleichs Abgleichs werden ~~in dem~~ im Herkunftsmitgliedstaat \Rightarrow von einem Fachmann für Daktyloskopie \Leftarrow sofort geprüft. Die endgültige Identifizierung wird von dem Herkunftsmitgliedstaat gemeinsam mit dem betroffenen Mitgliedstaat gemäß Artikel ~~1532~~ des Dubliner Übereinkommens \boxtimes der Dublin-Verordnung \boxtimes in Zusammenarbeit mit den betroffenen Mitgliedstaaten vorgenommen.

~~Von der Zentraleinheit~~ \Rightarrow Vom Zentralsystem \Leftarrow erhaltene Informationen über sonstige Daten, die sich als unzuverlässig herausgestellt haben, werden gelöscht ~~oder vernichtet~~, sobald festgestellt ist, dass die Daten unzuverlässig sind.

↓ neu

5. Ergibt die endgültige Identifizierung gemäß Absatz 4, dass das vom Zentralsystem übermittelte Abgleichergebnis fehlerhaft ist, teilen die Mitgliedstaaten dies der Kommission und der Agentur mit.

Artikel 26 4

Mitteilungen Kommunikation zwischen ~~den~~ Mitgliedstaaten und ~~der Zentraleinheit~~ ⇒ dem Zentralsystem ⇐

Die Übermittlung von Daten ~~zwischen den~~ durch die Mitgliedstaaten ~~und der Zentraleinheit~~ ⇒ an das Zentralsystem ⇐ ~~und umgekehrt erfolgt unter Verwendung der IDA-Basisdienste, die in der Entscheidung Nr. 1719/1999/EG des Europäischen Parlaments und des Rates vom 12. Juli 1999 über Leitlinien einschließlich der Festlegung von Projekten von gemeinsamem Interesse für transeuropäische Netze zum elektronischen Datenaustausch zwischen Verwaltungen (IDA)(2) vorgesehen sind.~~ ⇒ über die EURODAC Kommunikationsinfrastruktur ⇐. Die ~~Zentraleinheit~~ ⊗ Agentur ⊗ legt die technischen Verfahren für die ~~Verwendung~~ Nutzung der ~~IDA-Basisdienste~~ ⇒ Kommunikationsinfrastruktur ⇐ fest, sofern dies für den effizienten Betrieb ~~der Zentraleinheit~~ ⇒ des Zentralsystems ⇐ erforderlich ist.

Artikel 14

Sicherheit

1. ~~Der Herkunftsmitgliedstaat trifft die notwendigen Maßnahmen, um~~

- ~~(a) zu verhindern, dass Unbefugte Zugang zu den nationalen Anlagen erhalten, in denen die Vorgänge ausgeführt werden, die entsprechend dem Zweck von Eurodac dem Mitgliedstaat obliegen (Kontrollen am Eingang der Anlagen);~~
- ~~(b) zu verhindern, dass Eurodac-Daten und Datenträger von Unbefugten gelesen, kopiert, verändert oder gelöscht werden (Kontrolle der Datenträger);~~
- ~~(c) zu gewährleisten, dass nachträglich nachgeprüft und festgestellt werden kann, welche Daten wann und von wem in Eurodac gespeichert worden sind (Kontrolle der Datenspeicherung);~~
- ~~(d) die unbefugte Eingabe von Daten in Eurodac und jede unbefugte Veränderung oder Löschung von in Eurodac gespeicherten Daten zu verhindern (Kontrolle der Dateneingabe);~~
- ~~(e) zu gewährleisten, dass die zur Benutzung von Eurodac Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (Zugriffskontrolle);~~
- ~~(f) zu gewährleisten, dass nachgeprüft und festgestellt werden kann, welchen Behörden Eurodac-Daten mit Hilfe von Datenübertragungseinrichtungen übermittelt werden können (Kontrolle der Übermittlung);~~

~~(g) zu verhindern, dass bei der direkten Übermittlung der Daten an die zentrale Datenbank und umgekehrt bzw. beim Transport von Datenträgern von den Mitgliedstaaten zur Zentraleinheit und umgekehrt die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Kontrolle des Transports).~~

~~2. In Bezug auf den Betrieb der Zentraleinheit ist die Kommission für die Anwendung der Maßnahmen nach Absatz 1 verantwortlich.~~

↓ 2725/2000/EG
⇒ neu

Artikel 27 ~~15~~

Zugriff auf die in ~~Eurodac~~ **EURODAC** gespeicherten Daten und Berichtigung oder Löschung dieser Daten

1. Der Herkunftsmitgliedstaat hat Zugriff auf die von ihm übermittelten Daten, die er übermittelt hat und die gemäß dieser Verordnung in der zentralen Datenbank ⇒ im Zentralsystem ⇐ gespeichert sind.

Kein Mitgliedstaat darf von anderen Mitgliedstaaten übermittelte Daten abfragen oder solche Daten übermittelt bekommen, erhalten, mit Ausnahme der Daten, die das Ergebnis des Vergleichs Abgleichs nach Artikel 4 Absatz 5 9 Absatz 5 sind.

↓ 2725/2000/EG (angepasst)
⇒ neu

2. Zugriff nach Absatz 1 auf die in der zentralen Datenbank ⇒ im Zentralsystem ⇐ gespeicherten Daten haben diejenigen nationalen Behörden der Mitgliedstaaten, die von den Mitgliedstaaten letzteren ⇒ für die Zwecke des Artikels 1 Absatz 1 ⇐ benannt worden sind. ⇒ Die Benennung weist die für die Wahrnehmung von Aufgaben im Zusammenhang mit der Anwendung dieser Verordnung zuständige Dienststelle aus. ⇐ Jeder Mitgliedstaat übermittelt der Kommission ⇒ und der Agentur unverzüglich ⇐ ein Verzeichnis dieser Behörden ⇒ und aller daran vorgenommenen Änderungen ⇐ . ⇒ Die Agentur veröffentlicht die konsolidierte Fassung der Liste im Amtsblatt der Europäischen Union. Im Falle von Änderungen veröffentlicht die Agentur jedes Jahr eine aktualisierte und konsolidierte Fassung der Liste. ⇐
3. Unbeschadet der Löschung von Daten nach Artikel 6, Artikel 10 Absatz 1 oder Artikel 12 Absatz 4 Buchstabe a) 12 oder Artikel 16 Absatz 1 ist lediglich der Herkunftsmitgliedstaat berechtigt, die Daten, die er an die Zentraleinheit ⇒ das Zentralsystem ⇐ übermittelt hat, durch Berichtigung oder Ergänzung zu verändern oder sie zu löschen.

~~Werden die Daten unmittelbar von dem Herkunftsmitgliedstaat in der zentralen Datenbank gespeichert, so kann dieser die Daten unmittelbar ändern oder löschen.~~

~~Werden die Daten nicht unmittelbar von dem Herkunftsmitgliedstaat in der zentralen Datenbank gespeichert, so nimmt die Zentraleinheit auf Ersuchen dieses Mitgliedstaats Änderungen oder Löschungen vor.~~

4. Hat ein Mitgliedstaat oder die Zentraleinheit ⇒ Agentur ⇐ Grund zu der Annahme, dass ~~in der zentralen Datenbank~~ ⇒ im Zentralsystem ⇐ gespeicherte Daten sachlich falsch sind, so benachrichtigt er/sie so rasch wie möglich den Herkunftsmitgliedstaat.

Hat ein Mitgliedstaat Grund zu der Annahme, dass die Speicherung von Daten ~~in der zentralen Datenbank~~ ⇒ im Zentralsystem ⇐ im Widerspruch zu dieser Verordnung steht, so benachrichtigt er so rasch wie möglich ebenfalls ⇒ die Agentur, die Kommission und ⇐ den Herkunftsmitgliedstaat so rasch wie möglich. Dieser Letzterer überprüft die betreffenden Daten und ändert oder löscht sie nötigenfalls unverzüglich.

5. ⇒ Die Agentur ⇐ ~~leitet Den Behörden eines Drittlands werden~~ in der zentralen Datenbank ⇒ im Zentralsystem ⇐ gespeicherte Daten von der Zentraleinheit weder übermittelt noch zur Verfügung gestellt, nicht an die Behörden eines Drittstaats weiter noch stellt sie sie ihnen zur Verfügung – es sei denn, dass die Zentraleinheit sie hierzu im Rahmen eines Gemeinschaftsübereinkommens über die Kriterien und Verfahren Mechanismen zur Bestimmung des für die Prüfung eines Asylantrags ⇒ Antrags auf internationalen Schutz ⇐ zuständigen Mitgliedstaats ausdrücklich ermächtigt wird.

Artikel 22

Durchführungsbestimmungen

1. ~~Der Rat nimmt die zu folgenden Zwecken erforderlichen Durchführungsbestimmungen mit der in Artikel 205 Absatz 2 des Vertrags festgelegten Mehrheit an:~~

~~Festlegung des Verfahrens nach Artikel 4 Absatz 7,~~

~~Festlegung des Verfahrens für die Sperrung der Daten nach Artikel 12 Absatz 1,~~

~~Erstellung der Statistiken nach Artikel 12 Absatz 2.~~

~~In Fällen, in denen diese Durchführungsbestimmungen Auswirkungen auf die von den Mitgliedstaaten zu tragenden Betriebskosten haben, beschließt der Rat einstimmig.~~

2. ~~Die Maßnahmen, auf die in Artikel 3 Absatz 4 verwiesen wird, werden nach dem in Artikel 23 Absatz 2 genannten Verfahren beschlossen.~~

Artikel 28 16

Aufzeichnung der Daten Verarbeitungsvorgänge durch die Zentraleinheit

1. Die Zentraleinheit ⇒ Agentur ⇐ ~~fertigt Aufzeichnungen~~ führt über alle Datenverarbeitungsvorgänge in der Zentraleinheit ⇒ im Zentralsystem ⇐ Buch an. Diese Aus diesen Aufzeichnungen geben Aufschluss über den gehen der Zweck des Zugriffs, der den Tag und die Uhrzeit, die übermittelten Daten, die für eine Abfrage verwendeten Daten und die

~~Bezeichnung der eingebenden oder abfragenden Stelle sowie der Namen der Stellen und verantwortlichen Personen hervor, die Daten eingegeben oder abgefragt haben.~~

- Die Aufzeichnungen dürfen nur für die datenschutzrechtliche Kontrolle der Zulässigkeit der Datenverarbeitung sowie zur Gewährleistung der Datensicherheit gemäß Artikel ~~14~~ 34 verwendet werden. Sie werden durch geeignete Maßnahmen gegen unberechtigten Zugriff gesichert und nach einer Frist von einem Jahr ⇒ nach Ablauf der Aufbewahrungsfrist nach Artikel 12 und Artikel 16 Absatz 1 ⇐ gelöscht, wenn sie nicht für ein bereits eingeleitetes Kontrollverfahren benötigt werden.

↓ neu

- Jeder Mitgliedstaat ergreift die erforderlichen Maßnahmen, um die in den Absätzen 1 und 2 genannten Ziele in Bezug auf sein nationales System umzusetzen. Darüber hinaus führt jeder Mitgliedstaat Buch über die zur Dateneingabe und -abfrage ordnungsgemäß befugten Personen.

↓ 2725/2000/EG (angepasst)
⇒ neu

~~Artikel 23~~

~~Ausschuss~~

~~1. Die Kommission wird von einem Ausschuss unterstützt.~~

~~2. Wird auf das Verfahren dieses Absatzes Bezug genommen, so gelten die Artikel 5 und 7 des Beschlusses 1999/468/EG.~~

~~Der Zeitraum nach Artikel 5 Absatz 6 des Beschlusses 1999/486/EG wird auf drei Monate festgesetzt.~~

~~3. Der Ausschuss gibt sich eine Geschäftsordnung.~~

~~Artikel 29~~ 18

Rechte der von der Datenverarbeitung betroffenen Personen

- Der Herkunftsmitgliedstaat unterrichtet die unter diese Verordnung fallenden Personen, ~~die unter diese Verordnung fallen~~, ⇒ schriftlich, gegebenenfalls auch mündlich, in einer Sprache, die sie verstehen oder bei der vernünftigerweise davon ausgegangen werden kann, dass sie sie verstehen, ⇐ über:

(a) die Identität des für die Datenverarbeitung Verantwortlichen und gegebenenfalls seines Vertreters;

- (b) ~~die Zwecke den mit~~ der Verarbeitung ~~der~~ ☒ ihrer ☒ Daten ~~in im Rahmen von~~ ~~Eurodac~~EURODAC verfolgten Zweck, ⇒ einschließlich einer Beschreibung der Ziele der Dublin-Verordnung im Einklang mit Artikel 4 der Dublin-Verordnung ⇐;
- (c) die Empfänger der Daten;
- (d) in die Verpflichtung zur Fingerabdrucknahme bei Personen im Sinne ~~des Artikels der~~ ~~Artikel~~ 4 9 oder 8 14;
- (e) ~~die Auskunfts- und Berichtigungsrechte bezüglich~~ ihr Recht, Auskunft über ☒ sie betreffende ☒ ~~sie betreffender~~ Daten zu erhalten ☒ und zu beantragen, dass sie betreffende unrichtige Daten korrigiert werden ☒ ⇒ oder sie betreffende unrechtmäßig gespeicherte Daten gelöscht werden, sowie das Recht, Informationen über die Verfahren zur Ausübung dieser Rechte, einschließlich der Kontaktdaten des für die Datenverarbeitung Verantwortlichen und der nationalen Kontrollbehörden nach Artikel 31 Absatz 1 zu erhalten. ⇐

Die in Unterabsatz 1 genannten Informationen werden Personen im Sinne ~~des Artikels der~~ ~~Artikel~~ 4 9 oder ~~Artikels~~ 8 14 zum Zeitpunkt der Fingerabdruckabnahme erteilt.

Die in Unterabsatz 1 genannten Informationen werden Personen im Sinne des Artikels ~~11~~ 17 spätestens zum Zeitpunkt der Übermittlung der sie betreffenden Daten ~~an die Zentraleinheit~~ ⇒ an das Zentralsystem ⇐ erteilt. Diese Informationspflicht besteht nicht, wenn die Erteilung dieser Informationen sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde.

↓ neu

Nach dem Verfahren des Artikels 40 Absatz 2 der Dublin-Verordnung wird ein gemeinsames Merkblatt erstellt, das mindestens die Angaben gemäß Absatz 1 dieses Artikels und gemäß Artikel 4 Absatz 1 der Dublin-Verordnung enthält. Das Merkblatt sollte klar und einfach in einer Sprache abgefasst sein, die die Person versteht oder bei der vernünftigerweise davon ausgegangen werden kann, dass sie sie versteht.

Ist die Person, die unter diese Verordnung fällt, minderjährig, unterrichten die Mitgliedstaaten die Person in einer ihrem Alter angemessenen Weise.

↓ 2725/2000/EG
⇒ neu

2. In allen Mitgliedstaaten kann jede von einer Datenverarbeitung betroffene Person nach Maßgabe der Rechts- und Verwaltungsvorschriften und der Verfahren des jeweiligen Mitgliedstaats die in Artikel 12 der Richtlinie 95/46/EG genannten Rechte wahrnehmen.

Unbeschadet der Verpflichtung zur Bereitstellung anderweitiger Informationen gemäß Artikel 12 Buchstabe a) der Richtlinie 95/46/EG hat die betroffene Person das Recht, darüber unterrichtet zu werden, welche sie betreffenden Daten ~~in der zentralen Datenbank~~ ⇒ im

Zentralsystem \Leftrightarrow gespeichert sind und welcher Mitgliedstaat die Daten an ~~die Zentraleinheit~~ \Rightarrow das Zentralsystem \Leftrightarrow übermittelt hat. Der Zugang zu den Daten kann nur von den Mitgliedstaaten gewährt werden.

3. In ~~jedem Mitgliedstaat~~ allen Mitgliedstaaten kann jede Person verlangen, dass sachlich falsche Daten berichtigt oder unrechtmäßig gespeicherte Daten gelöscht werden. Die Berichtigung und die Löschung werden ohne ungebührliche Verzögerung durch den Mitgliedstaat, der die Daten übermittelt hat, nach seinen Rechts- und Verwaltungsvorschriften und Verfahren vorgenommen.
4. Werden die Ansprüche auf Berichtigung und Löschung in einem anderen Mitgliedstaat als dem Mitgliedstaat oder den Mitgliedstaaten, der/die die Daten übermittelt hat/haben, geltend gemacht, so setzen sich die Behörden dieses Mitgliedstaats mit den Behörden des betreffenden Mitgliedstaats oder der betreffenden Mitgliedstaaten in Verbindung, damit diese die Richtigkeit der Daten sowie die Rechtmäßigkeit ihrer Übermittlung und ihrer Speicherung ~~in der zentralen Datenbank~~ \Rightarrow im Zentralsystem \Leftrightarrow überprüfen können.
5. Zeigt sich, dass die ~~in der zentralen Datenbank~~ \Rightarrow im Zentralsystem \Leftrightarrow gespeicherten Daten sachlich falsch sind oder unrechtmäßig gespeichert wurden, so werden sie von dem Mitgliedstaat, der sie übermittelt hat, gemäß Artikel ~~15 Absatz 3~~ 27 Absatz 3 berichtigt oder gelöscht. Der betreffende Mitgliedstaat bestätigt der betroffenen Person schriftlich ohne ungebührliche Verzögerung, dass er Maßnahmen zur Berichtigung oder Löschung der sie betreffenden Daten ergriffen hat.
6. Ist der Mitgliedstaat, der die Daten übermittelt hat, nicht der Ansicht, dass die ~~in der zentralen Datenbank~~ \Rightarrow im Zentralsystem \Leftrightarrow gespeicherten Daten sachlich falsch sind oder unrechtmäßig gespeichert wurden, so teilt er der betroffenen Person ohne ungebührliche Verzögerung in einer schriftlichen Begründung mit, warum er nicht bereit ist, die Daten zu berichtigen oder zu löschen.

Der Mitgliedstaat teilt der betroffenen Person ebenfalls mit, welche Schritte sie ergreifen kann, wenn sie mit der Begründung nicht einverstanden ist. Hierzu gehören Angaben darüber, auf welche Weise bei einem Gericht oder den zuständigen Behörden des betreffenden Mitgliedstaats Klage zu erheben oder gegebenenfalls Beschwerde einzulegen ist, sowie Angaben über jede finanzielle oder sonstige Unterstützung, die gemäß den Rechts- und Verwaltungsvorschriften sowie den Verfahren des betreffenden Mitgliedstaats zur Verfügung steht.

7. Jeder Antrag nach den Absätzen 2 und 3 enthält die zur Identifizierung der betroffenen Person erforderlichen Angaben einschließlich der Fingerabdrücke Fingerabdruckdaten. Diese Daten werden ausschließlich für die Wahrnehmung der in den Absätzen 2 und 3 genannten Rechte verwendet und anschließend unverzüglich vernichtet.
8. Die zuständigen Behörden der Mitgliedstaaten arbeiten aktiv zusammen, damit die Ansprüche im Sinne der Absätze 3, 4 und 5 unverzüglich erfüllt werden.

↓ neu

9. Fordert eine Person sie betreffende Daten gemäß Absatz 2 an, wird dies von der zuständigen Behörde in einem Schriftstück, in dem die Anforderung festgehalten wird, aufgezeichnet; dieses Schriftstück stellt sie den nationalen Kontrollbehörden auf deren Anfrage unverzüglich zur Verfügung.

↓ 2725/2000/EG (angepasst)

⇒ neu

- ~~9.~~ 10. In jedem Mitgliedstaat ~~leistet~~ unterstützt die nationale ~~Kontrollstelle~~ Kontrollbehörde ~~gemäß Artikel 28 Absatz 4 der Richtlinie 95/46/EG der betroffenen~~ die betroffene Person ~~⇒ auf deren Antrag~~ ⇐ bei der Wahrnehmung ihrer Rechte Unterstützung gemäß Artikel 28 Absatz 4 der Richtlinie 95/46/EG.

- ~~10.~~ 11. Die nationale ~~Kontrollstelle~~ Kontrollbehörde des Mitgliedstaats, der die Daten übermittelt hat, und die nationale ~~Kontrollstelle~~ Kontrollbehörde des Mitgliedstaats, in dem sich die betroffene Person aufhält, unterstützen und - wenn sie darum ersucht werden - beraten diese bei der Wahrnehmung ihres Rechts auf Berichtigung oder Löschung von Daten. Beide nationalen ~~Kontrollstellen~~ Kontrollbehörden arbeiten zu diesem Zweck zusammen. Ersuchen um Unterstützung können an die nationale ~~Kontrollstelle~~ Kontrollbehörde des Aufenthaltsmitgliedstaats gerichtet werden, der die Ersuchen an die Stelle des Mitgliedstaats weiterleitet, der die Daten übermittelt hat. ~~Alternativ hierzu kann die betroffene Person unmittelbar die gemeinsame Kontrollstelle nach Artikel 20 um Unterstützung ersuchen.~~

- ~~11.~~ 12. In allen Mitgliedstaaten kann jede Person nach Maßgabe der Rechts- und Verwaltungsvorschriften und Verfahren des betreffenden Mitgliedstaats bei einem Gericht oder den zuständigen Behörden dieses Staates Klage erheben oder gegebenenfalls Beschwerde einlegen, wenn ihr das in Absatz 2 vorgesehene Auskunftsrecht verweigert wird.

- ~~12.~~ 13. Jede Person kann nach Maßgabe der Rechts- und Verwaltungsvorschriften und der Verfahren des Mitgliedstaats, der die Daten übermittelt hat, hinsichtlich der sie betreffenden, ~~in der zentralen Datenbank~~ ⇒ im Zentralsystem ⇐ gespeicherten Daten bei einem Gericht oder den zuständigen Behörden dieses Staates Klage erheben oder gegebenenfalls Beschwerde einlegen, um ihre Rechte nach Absatz 3 geltend zu machen. Die Verpflichtung der nationalen ~~Kontrollstellen~~ Kontrollbehörden zur Unterstützung und – sofern beantragt – zur Beratung der betroffenen Person gemäß Absatz ~~10~~ 13 bleibt während des ganzen Verfahrens bestehen.

Artikel 30 ~~19~~

⊗ Überwachung durch die ⊗ Nationale Kontrollstelle Kontrollbehörde

1. Jeder Mitgliedstaat sieht vor, dass die gemäß Artikel 28 Absatz 1 der Richtlinie 95/46/EG benannte(n) nationale(n) ~~Kontrollstelle(n)~~ Kontrollbehörde(n) nach Maßgabe des jeweiligen nationalen Rechts die Rechtmäßigkeit der Verarbeitung personenbezogener Daten gemäß dieser Verordnung durch den betreffenden Mitgliedstaat einschließlich der Übermittlung

dieser Daten an ~~die Zentraleinheit~~ ⇒ das Zentralsystem ⇐ unabhängig überwacht/überwachen.

2. Jeder Mitgliedstaat trägt dafür Sorge, dass seine nationale ~~Kontrollstelle~~ Kontrollbehörde die Möglichkeit hat, sich von Personen mit ausreichender Kenntnis im Bereich der Personenidentifizierung mittels der Fingerabdrücke (Daktyloskopie) beraten zu lassen.

↓ neu

Artikel 31

Überwachung durch den Europäischen Datenschutzbeauftragten

1. Der Europäische Datenschutzbeauftragte stellt sicher, dass die Verarbeitung personenbezogener Daten in EURODAC, insbesondere durch die Agentur, im Einklang mit der Verordnung (EG) Nr. 45/2001 und dieser Verordnung erfolgt.
2. Der Europäische Datenschutzbeauftragte trägt dafür Sorge, dass mindestens alle vier Jahre die Verarbeitung personenbezogener Daten durch die Agentur nach den internationalen Prüfungsgrundsätzen überprüft wird. Der Prüfbericht wird dem Europäischen Parlament, dem Rat, der Agentur, der Kommission und den nationalen Kontrollbehörden übermittelt. Die Agentur erhält Gelegenheit, vor der Annahme des Berichts Bemerkungen abzugeben.

Artikel 32

Zusammenarbeit zwischen den nationalen Kontrollbehörden und dem Europäischen Datenschutzbeauftragten

1. Die nationalen Kontrollbehörden und der Europäische Datenschutzbeauftragte arbeiten im Rahmen ihrer jeweiligen Zuständigkeiten aktiv zusammen und sorgen für eine koordinierte Überwachung von EURODAC.
2. Im Rahmen ihrer jeweiligen Zuständigkeiten tauschen sie einschlägige Informationen aus, unterstützen sich gegenseitig bei Überprüfungen und Inspektionen, prüfen Schwierigkeiten bei der Auslegung oder Anwendung dieser Verordnung, gehen Problemen bei der Wahrnehmung der unabhängigen Überwachung oder der Ausübung der Rechte betroffener Personen nach, arbeiten harmonisierte Vorschläge im Hinblick auf gemeinsame Lösungen für etwaige Probleme aus und fördern erforderlichenfalls die Sensibilisierung für die Datenschutzrechte.
3. Die nationalen Kontrollbehörden und der Europäische Datenschutzbeauftragte kommen zu diesem Zweck mindestens zweimal pro Jahr zusammen. Die Kosten und die Ausrichtung dieser Sitzungen übernimmt der Europäische Datenschutzbeauftragte. In der ersten Sitzung wird eine Geschäftsordnung angenommen. Weitere Arbeitsverfahren werden je nach Bedarf gemeinsam festgelegt. Ein gemeinsamer Tätigkeitsbericht wird dem Europäischen Parlament, dem Rat, der Kommission und der Agentur alle zwei Jahre übermittelt.

Artikel 33

Schutz der für die Zwecke der Verhütung, Aufdeckung und Untersuchung terroristischer oder sonstiger schwerer Straftaten verarbeiteten personenbezogenen Daten

1. Für die Verarbeitung personenbezogener Daten zu Strafverfolgungszwecken auf der Grundlage dieser Verordnung gilt der Rahmenbeschluss 2008/977/JI.
2. Die Verarbeitung personenbezogener Daten durch Europol nach Maßgabe dieser Verordnung erfolgt in Übereinstimmung mit dem Beschluss 2009/371/JI.
3. Die nach Maßgabe dieser Verordnung von EURODAC erhaltenen personenbezogenen Daten dürfen nur für die Zwecke der Verhütung, Aufdeckung und Untersuchung terroristischer oder sonstiger schwerer Straftaten verarbeitet werden.
4. 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.
5. Die Rechtmäßigkeit der Verarbeitung personenbezogener Daten auf der Grundlage dieser Verordnung durch die Mitgliedstaaten, einschließlich der Übermittlung dieser Daten an und von EURODAC, wird von den gemäß dem Rahmenbeschluss 2008/977/JI benannten nationalen Behörden überwacht.

Artikel 34

Datensicherheit

1. Der Herkunftsmitgliedstaat gewährleistet die Datensicherheit vor und während der Übermittlung an das Zentralssystem.
2. Jeder Mitgliedstaat trifft für sein innerstaatliches System die erforderlichen Maßnahmen, einschließlich der Aufstellung eines Sicherheitsplans, um
 - a) die Daten physisch zu schützen, auch durch die Aufstellung von Notfallplänen für den Schutz kritischer Infrastrukturen;
 - b) zu verhindern, dass Unbefugte Zugang zu den innerstaatlichen Anlagen erhalten, in denen der Mitgliedstaat Tätigkeiten ausführt, die dem Zweck von EURODAC dienen (Zugangskontrolle);
 - c) das unbefugte Lesen, Kopieren, Verändern oder Entfernen von Datenträgern zu verhindern (Datenträgerkontrolle);
 - d) die unbefugte Eingabe von Daten sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten zu verhindern (Speicherkontrolle);

- e) die unbefugte Verarbeitung von EURODAC-Daten und die unbefugte Änderung oder Löschung von Daten, die in EURODAC verarbeitet wurden, zu verhindern (Kontrolle der Dateneingabe);
 - f) sicherzustellen, dass die zur Benutzung von EURODAC befugten Personen über Benutzerkennworte und einen personalisierten Zugangsmodus ausschließlich Zugriff auf die ihrer Zugriffsberechtigung unterliegenden Daten haben (Kontrolle des Datenzugriffs);
 - g) sicherzustellen, dass die zum Zugriff auf EURODAC-Daten berechtigten Behörden Profile mit einer Beschreibung der Aufgaben und Befugnisse der Personen erstellen, die zum Zugriff auf die Daten sowie zu ihrer Eingabe, Aktualisierung, Löschung und Abfrage berechtigt sind, und dass diese Profile den nationalen Kontrollbehörden nach Artikel 25 des Rahmenbeschlusses 2008/799/JI auf deren Anfrage unverzüglich zur Verfügung gestellt werden (Profile der zugriffsberechtigten Personen);
 - h) zu gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Datenübertragungseinrichtungen übermittelt werden können (Übermittlungskontrolle);
 - i) sicherzustellen, dass nachgeprüft und festgestellt werden kann, welche Daten wann, von wem und zu welchem Zweck in EURODAC verarbeitet worden sind (Datenerfassungskontrolle);
 - j) insbesondere durch geeignete Verschlüsselungstechniken zu verhindern, dass bei der Übermittlung personenbezogener Daten an EURODAC und von EURODAC oder während des Transports von Datenträgern die Daten von Unbefugten gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle);
 - k) die Effizienz der in diesem Absatz genannten Sicherheitsmaßnahmen zu überwachen und die notwendigen organisatorischen Maßnahmen im Zusammenhang mit der internen Überwachung zu treffen, die die Einhaltung der Bestimmungen dieser Verordnung sicherstellen (Eigenkontrolle).
3. Die Agentur ergreift die Maßnahmen, die erforderlich sind, um die in Absatz 2 genannten Ziele in Bezug auf den Betrieb von EURODAC, einschließlich der Annahme eines Sicherheitsplans, zu verwirklichen.

Artikel 35

Verbot der Übermittlung von Daten an Drittstaaten, internationale Organisationen oder private Stellen

Personenbezogene Daten, die ein Mitgliedstaat oder Europol nach dieser Verordnung aus der EURODAC-Zentraldatenbank erhalten hat, dürfen nicht an einen Drittstaat, eine internationale Organisation oder eine private Stelle innerhalb oder außerhalb der Europäischen Union übermittelt oder ihnen zur Verfügung gestellt werden. Dieses Verbot schränkt das Recht der Mitgliedstaaten auf die Übermittlung solcher Daten an Drittstaaten, auf die die Dublin-Verordnung anwendbar ist, nicht ein.

Protokollierung und Dokumentierung

1. Die Mitgliedstaaten und Europol gewährleisten, dass alle Datenverarbeitungsvorgänge, die aus Anträgen auf Abgleich mit EURODAC-Daten nach dieser Verordnung resultieren, zum Zwecke der Prüfung der Zulässigkeit des Antrags, der Überwachung der Rechtmäßigkeit der Datenverarbeitung sowie zur Gewährleistung der Datenintegrität und -sicherheit und zur Eigenkontrolle aufgezeichnet werden.
2. Das Protokoll beziehungsweise die Unterlagen enthalten folgende Angaben:
 - a) den genauen Zweck des Antrags auf Abgleich, einschließlich Angaben zur Art der terroristischen und sonstigen schweren Straftat, und im Falle Europol den genauen Zweck des Antrags auf Abgleich;
 - b) das betreffende nationale Aktenzeichen;
 - c) das Datum und den genauen Zeitpunkt des Antrags der nationalen Zugangsstelle auf Abgleich mit den Daten des EURODAC-Zentralsystems;
 - d) die Bezeichnung der Behörde, die den Zugriff zwecks Datenabgleichs beantragt hat, sowie die zuständige Person, die den Antrag gestellt und die Daten verarbeitet hat;
 - e) gegebenenfalls die Anwendung des Dringlichkeitsverfahrens nach Artikel 19 Absatz 3 und das Ergebnis der nachträglichen Überprüfung;
 - f) die für den Abgleich verwendeten Daten;
 - g) nach Maßgabe der innerstaatlichen Rechtsvorschriften oder der Bestimmungen des Europol-Beschlusses die Kennung des Beamten, der die Abfrage vorgenommen hat, und des Beamten, der die Abfrage oder Übermittlung angeordnet hat.
3. Die Protokolle oder Unterlagen dürfen nur zu Datenschutzzwecken zur Überwachung der Rechtmäßigkeit der Datenverarbeitung sowie zur Gewährleistung der Datensicherheit verwendet werden. Für die Überwachung und Bewertung gemäß Artikel 38 dürfen nur Protokolle verwendet werden, die keine personenbezogenen Daten enthalten. Die für die Prüfung der Zulässigkeit des Antrags und die Überwachung der Rechtmäßigkeit der Datenverarbeitung sowie die Gewährleistung der Datenintegrität und -sicherheit zuständigen nationalen Kontrollbehörden haben auf Antrag zur Erfüllung ihrer Aufgaben Zugang zu diesen Protokollen.

Artikel 37 ~~17~~
Haftung

1. Jede Person oder jeder Mitgliedstaat, der ~~bzw. oder~~ dem durch eine rechtswidrige Verarbeitung oder durch eine andere Handlung, die den Bestimmungen dieser Verordnung zuwiderläuft, ein Schaden entstanden ist, hat das Recht, von dem für den erlittenen Schaden verantwortlichen Mitgliedstaat Schadenersatz zu verlangen. Dieser Mitgliedstaat wird teilweise oder vollständig von seiner Haftung befreit, wenn er nachweist, dass er für den Umstand, durch den der Schaden eingetreten ist, nicht verantwortlich ist.
2. Für Schäden ~~an der zentralen Datenbank~~ ⇒ am Zentralsystem ⇐, die darauf zurückzuführen sind, dass ein Mitgliedstaat seinen Verpflichtungen aufgrund dieser Verordnung nicht nachgekommen ist, ist dieser Mitgliedstaat haftbar, es sei denn, die ~~Kommission~~ ⇒ Agentur oder ein anderer Mitgliedstaat ⇐ hat keine angemessenen Schritte unternommen, um den Schaden abzuwenden oder zu mindern.
3. Die Durchsetzung von Schadenersatzansprüchen nach den Absätzen 1 und 2 gegen einen Mitgliedstaat unterliegt den innerstaatlichen Rechtsvorschriften des beklagten Mitgliedstaats.

KAPITEL VIII

ÄNDERUNGEN AN DER VERORDNUNG (EU) NR. 1077/2011

Artikel 38

Bestimmungen zur Änderung der Verordnung (EU) Nr. 1077/2011

1. Artikel 5 erhält folgende Fassung:

„Artikel 5

Aufgaben im Zusammenhang mit EURODAC

In Bezug auf EURODAC nimmt die Agentur die folgenden Aufgaben wahr:

- a) die Aufgaben, die der Agentur durch die Verordnung (EU) Nr. .../... [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. {.../...}] übertragen wurden.

b) Aufgaben im Zusammenhang mit Schulungen zur technischen Nutzung von EURODAC.“

2. Artikel 12 Absatz 1 wird wie folgt geändert:

a) Die Buchstaben t, u und v erhalten folgende Fassung:

„t) die Berichte über die technische Funktionsweise des SIS II gemäß Artikel 50 Absatz 4 der Verordnung (EG) Nr. 1987/2006 und Artikel 66 Absatz 4 des Beschlusses 2007/533/JI, über die technische Funktionsweise des VIS gemäß Artikel 50 Absatz 3 der Verordnung (EG) Nr. 767/2008 und Artikel 17 Absatz 3 des Beschlusses 2008/633/JI und über die technische Funktionsweise von EURODAC gemäß Artikel 40 Absatz 4 der Verordnung (EU) Nr. .../... [des Europäischen Parlaments und des Rates über die Einrichtung von „EURODAC“ für den Abgleich von Fingerabdruckdaten zum Zweck der effektiven Anwendung der Verordnung (EU) Nr. {.../...} zur 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 mit EURODAC-Daten] anzunehmen;

u) den Jahresbericht über die Tätigkeit des Zentralsystems von EURODAC gemäß Artikel 40 Absatz 1 der Verordnung (EU) Nr. .../... [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. .../...] anzunehmen;

v) zu den Berichten des Europäischen Datenschutzbeauftragten über die Überprüfungen gemäß Artikel 45 der Verordnung (EG) Nr. 1987/2006, Artikel 42 Absatz 2 der Verordnung (EG) Nr. 767/2008 und Artikel 31 Absatz 2 der Verordnung (EU) Nr. .../... [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. .../...] Stellung zu nehmen und für angemessene Folgemaßnahmen zu den Überprüfungen Sorge zu tragen;“

b) Buchstabe x erhält folgende Fassung:

„x) Statistiken über die Arbeit des Zentralsystems von EURODAC gemäß Artikel 8 Absatz 2 der Verordnung (EU) Nr. .../... [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. .../...] zu erstellen;“

c) Buchstabe z erhält folgende Fassung:

„z) dafür zu sorgen, dass die Liste der gemäß Artikel 27 Absatz 2 der Verordnung (EU) Nr. .../... [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. .../...] benannten Behörden jährlich veröffentlicht wird;“

3. Artikel 15 Absatz 4 erhält folgende Fassung:

„4. Europol und Eurojust können an Sitzungen des Verwaltungsrats als Beobachter teilnehmen, wenn auf der Tagesordnung das SIS II betreffende Angelegenheiten im Zusammenhang mit der Anwendung des Beschlusses 2007/533/JI stehen. Europol kann auch an Sitzungen des Verwaltungsrats als Beobachter teilnehmen, wenn auf der Tagesordnung das VIS betreffende Angelegenheiten im Zusammenhang mit der Anwendung des Beschlusses 2008/633/JI oder EURODAC betreffende Angelegenheiten im Zusammenhang mit der Anwendung der Verordnung (EU) Nr. .../... [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. .../...] stehen.“

4. Artikel 17 wird wie folgt geändert:

a) Absatz 5 Buchstabe g erhält folgende Fassung:

„g) unbeschadet des Artikels 17 des Statuts Geheimhaltungsvorschriften festzulegen, um Artikel 17 der Verordnung (EG) Nr. 1987/2006, Artikel 17 des Beschlusses 2007/533/JI, Artikel 26 Absatz 9 der Verordnung (EG) Nr. 767/2008 oder Artikel 4 Absatz 6 der Verordnung (EU) Nr. .../... [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. .../...] nachzukommen;“

b) Absatz 6 Buchstabe i erhält folgende Fassung:

„i) die Entwürfe der Berichte über die technische Funktionsweise jedes der in Artikel 12 Absatz 1 Buchstabe t genannten IT-Großsysteme und den Entwurf des Jahresberichts über die Tätigkeit des Zentralsystems von EURODAC gemäß Artikel 12 Absatz 1 Buchstabe u auf der Grundlage der Kontroll- und Bewertungsergebnisse;“

5. Artikel 19 Absatz 3 erhält folgende Fassung:

„(3) Europol und Eurojust können jeweils einen Vertreter in die SIS II-Beratergruppe entsenden. Europol kann auch einen Vertreter in die VIS-Beratergruppe und die EURODAC-Beratergruppe entsenden.“

KAPITEL ~~VII~~ IX

SCHLUSSBESTIMMUNGEN

Artikel ~~39~~ 24

Kosten

1. Die Kosten im Zusammenhang mit der Einrichtung und dem Betrieb ~~der Zentraleinheit~~ ⇒ des Zentralsystems und der Kommunikationsinfrastruktur ⇐ gehen zu Lasten des Gesamthaushaltsplans der Europäischen Union.
2. Die Kosten für die nationalen Einheiten ⇒ Zugangsstellen ⇐ und die Kosten für deren Anbindung an ~~die zentrale Datenbank~~ ⇒ das Zentralsystem ⇐ werden von den Mitgliedstaaten getragen.
3. Die Mitgliedstaaten und Europol errichten und unterhalten auf eigene Kosten die zur Anwendung dieser Verordnung notwendige technische Infrastruktur und kommen für die Kosten auf, die ihnen durch Anträge auf Abgleich mit EURODAC-Daten für die Zwecke der Verhütung, Aufdeckung und Untersuchung von in dieser Verordnung erfassten Straftaten entstehen.
- ~~3. Die Kosten für die Übermittlung der Daten aus dem Herkunftsmitgliedstaat sowie die Übermittlung der Ergebnisse des Vergleichs an diesen Mitgliedstaat werden von diesem getragen~~

Artikel ~~40~~ 24

Jahresbericht: Überwachung und Bewertung

1. Die ~~Kommission~~ ⇒ Agentur ⇐ unterbreitet dem Europäischen Parlament und dem Rat jährlich einen Bericht über die Tätigkeit ~~der Zentraleinheit~~ ⇒ des Zentralsystems ⇐. Der jährliche Bericht gibt unter anderem Aufschluss über Verwaltung und Leistung von ~~„Eurodac“~~ EURODAC gemessen an Mengenindikatoren, die für die in Absatz 2 genannten Ziele vorgegeben werden.
2. Die ~~Kommission~~ ⇒ Agentur ⇐ trägt dafür Sorge, dass ☒ Verfahren ☒ Systeme zur Verfügung stehen, ~~um die Funktionsweise mit denen der Betrieb der Zentraleinheit~~ ⇒ des Zentralsystems ⇐ ~~gemessen an den Zielen hinsichtlich~~ anhand von Leistungs-, Kostenwirksamkeits- und ~~Qualität der Dienstleistung~~ zu überwachen Dienstleistungsqualitätszielen überwacht werden kann.

~~3. Die Kommission unterzieht die Arbeitsweise der Zentraleinheit regelmäßig einer Bewertung, um festzustellen, ob diese ihre Ziele kostenwirksam erreicht hat, und um Leitlinien zur Verbesserung der Effizienz künftiger Vorgänge zu erarbeiten.~~

~~4. Ein Jahr, nachdem Eurodac seine Tätigkeit aufgenommen hat, legt die Kommission einen Bewertungsbericht über die Zentraleinheit vor, in dem sie im Wesentlichen das Verhältnis zwischen erwarteter und tatsächlicher Nachfrage prüft, auf operative und administrative Fragen im Lichte der Erfahrungen eingeht und Möglichkeiten für kurzfristige Verbesserungen der operativen Praxis aufzeigt.~~

↓ neu

3. Zum Zwecke der Wartung des Systems sowie zur Erstellung von Berichten und Statistiken hat die Agentur Zugang zu den erforderlichen Informationen über die Verarbeitungsvorgänge im Zentralsystem.

4. Alle zwei Jahre legt die Agentur dem Europäischen Parlament, dem Rat, der Kommission und dem Europäischen Datenschutzbeauftragten einen Bericht über den technischen Betrieb des Zentralsystems, einschließlich der Sicherheitsaspekte, vor.

↓ 2725/2000/EG
⇒ neu

5. ~~Drei Jahre, nachdem Eurodac seine Tätigkeit aufgenommen hat,~~ ⇒ nach dem Inkrafttreten dieser Verordnung gemäß Artikel 46 Absatz 2 ⇐ und sodann alle ~~sechs~~ ⇒ vier ⇐ Jahre, legt die Kommission eine umfassende Bewertung von ~~Eurodac~~EURODAC vor, in der sie die Ergebnisse an den Zielen misst, ~~ein Urteil darüber abgibt und prüft,~~ ob die grundlegenden Prinzipien weiterhin gültig sind; dazu gehören auch alle gebotenen Schlussfolgerungen für künftige Tätigkeiten ~~zieht~~ ⇒ und gegebenenfalls erforderliche Empfehlungen ⇐. ⇒ Die Kommission legt die Bewertung dem Europäischen Parlament und dem Rat vor. ⇐

↓ neu

6. Die Mitgliedstaaten stellen der Agentur und der Kommission die Informationen zur Verfügung, die zum Abfassen der in den Absätzen 4 und 5 genannten Berichte erforderlich sind.

7. Die Agentur stellt der Kommission die Informationen zur Verfügung, die zur Durchführung der in Absatz 5 genannten Bewertung erforderlich sind.

8. Die Mitgliedstaaten und Europol erstellen Jahresberichte über die Wirksamkeit des Abgleichs von Fingerabdruckdaten mit EURODAC-Daten für Strafverfolgungszwecke; diese Berichte enthalten auch Angaben und Statistiken über den genauen Zweck des Abgleichs, einschließlich über die Art der terroristischen oder sonstigen schweren Straftat, die Anzahl der Anträge auf Abgleich, die Anzahl und die Art von Fällen, in denen die Identität einer Person

festgestellt werden konnte, die Notwendigkeit und die Nutzung des Ausnahmeverfahrens in dringenden Fällen sowie über Fälle, in denen bei der nachträglichen Überprüfung durch die Prüfstelle festgestellt wurde, dass das Dringlichkeitsverfahren nicht gerechtfertigt war. Die Berichte werden der Kommission vorgelegt.

9. Die Agentur, die Mitgliedstaaten und Europol stellen der Kommission die für die Bewertungsberichte nach Absatz 5 erforderlichen Informationen zur Verfügung. Diese Informationen dürfen nicht zu einer Störung von Arbeitsverfahren führen oder Angaben enthalten, die Rückschlüsse auf Quellen, Bedienstete oder Ermittlungen der benannten Behörden gestatten.

↓ 2725/2000/EG (angepasst)
⇒ neu

Artikel 41 ~~25~~ **Sanktionen**

Die Mitgliedstaaten ~~sorgen dafür~~, ☒ treffen die erforderlichen Maßnahmen, um sicherzustellen ☒, dass ~~bei einer dem in Artikel 1 Absatz 1 genannten Zweck~~ ☒ jede ☒ Verarbeitung von ⇒ im Zentralsystem ⇐ ~~gespeicherten Daten, die dem in Artikel 1 Absatz 1 genannten Zweck von Eurodac/EURODAC zuwiderläuft, zuwiderlaufenden Verwendung von Daten, die in der zentralen Datenbank gespeichert sind, entsprechende Sanktionen verhängt werden~~ ☒ mit wirksamen, verhältnismäßigen und abschreckenden Sanktionen, einschließlich verwaltungs- und/oder strafrechtlicher Sanktionen im Einklang mit dem nationalen Recht, geahndet wird. ☒

Artikel 42 ~~26~~ **Territorialer Anwendungsbereich**

Die Bestimmungen dieser Verordnung sind nicht anwendbar auf Gebiete, für die ~~das Dubliner Übereinkommen~~ ☒ die Dublin-Verordnung ☒ nicht gilt.

↓ neu

Artikel 43 **Meldung der benannten Behörden und Prüfstellen**

1. Jeder Mitgliedstaat teilt [spätestens drei Monate nach dem Inkrafttreten dieser Verordnung] der Kommission seine benannten Behörden mit und meldet unverzüglich jede Änderung.
2. Jeder Mitgliedstaat teilt [spätestens drei Monate nach dem Inkrafttreten dieser Verordnung] der Kommission seine Prüfstelle mit und meldet unverzüglich jede Änderung.

3. Europol teilt [spätestens drei Monate nach dem Inkrafttreten dieser Verordnung] der Kommission seine Prüfstelle sowie die benannte nationale Zugangsstelle mit und meldet unverzüglich jede Änderung.
4. Die Kommission veröffentlicht die in den Absätzen 1, 2 und 3 genannten Informationen einmal im Jahr im *Amtsblatt der Europäischen Union*.

↓ neu

Artikel 44

Übergangsbestimmungen

Daten, die gemäß Artikel 12 der Verordnung (EG) Nr. 2725/2000 des Rates im Zentralsystem blockiert wurden, werden freigegeben und gemäß Artikel 18 Absatz 1 dieser Verordnung zu dem in Artikel 46 vorgesehenen Zeitpunkt markiert.

Artikel 45

Aufhebung

Die Verordnung (EG) Nr. 2725/2000 des Rates vom 11. Dezember 2000 und die Verordnung (EG) Nr. 407/2002 des Rates werden mit Wirkung ab dem in Artikel 46 Absatz 2 genannten Zeitpunkt aufgehoben.

Bezugnahmen auf die aufgehobenen Verordnungen sind nach Maßgabe der Entsprechungstabelle in Anhang III zu lesen.

↓ 2725/2000/EG Artikel 27 (angepasst)

⇒ neu

Artikel ~~46~~ 27

Inkrafttreten und Anwendbarkeit

1. Diese Verordnung tritt am zwanzigsten Tage nach ihrer Veröffentlichung im *Amtsblatt der Europäischen ~~Gemeinschaften~~ Union* in Kraft.
2. ~~Der Tag, ab dem diese~~ Diese Verordnung wird zwei Jahre nach ihrem Inkrafttreten anwendbar. gilt und Eurodac seine Tätigkeit aufnimmt, wird in einer im *Amtsblatt der Europäischen Gemeinschaften* veröffentlichten Mitteilung der Kommission bekannt gegeben, wenn folgende Bedingungen erfüllt sind:
 - a) ~~jeder Mitgliedstaaten hat der Kommission mitgeteilt, dass er die technischen Vorkehrungen getroffen hat, die für die Übermittlung der Daten an die Zentraleinheit entsprechend den Durchführungsbestimmungen nach Artikel 4 Absatz 7 und für die Erfüllung der Durchführungsbestimmungen nach Artikel 12 Absatz 5 erforderlich sind, und~~

~~b) die Kommission hat die technischen Vorkehrungen getroffen, die erforderlich sind, damit die Zentraleinheit ihre Tätigkeit entsprechend den Durchführungsbestimmungen nach Artikel 4 Absatz 7 und Artikel 12 Absatz 5 aufnehmen kann.~~

↓ neu

3. Die Mitgliedstaaten benachrichtigen die Kommission und die Agentur, sobald sie die technischen Vorkehrungen für die Datenübermittlung an das Zentralsystem getroffen haben, in jedem Fall aber nicht später als zwei Jahre nach dem Inkrafttreten dieser Verordnung.

4. Diese Verordnung ist in allen ihren Teilen verbindlich und gilt gemäß den Verträgen unmittelbar in den Mitgliedstaaten.

↓ 2725/2000/EG

Geschehen zu Brüssel am [...]

Im Namen des Europäischen Parlaments
Der Präsident

Im Namen des Rates
Der Präsident

↓407/2002/EG ⇒ neu

Anhang I

Datenformat für den Austausch von Fingerabdruckdaten

Folgendes Format für den Austausch von Fingerabdruckdaten wird ~~festgelegt~~ vorgeschrieben:

~~ANSI/NIST-CSL 1-1993~~ ⇒ ANSI/NIST-ITL 1a-1997, Ver.3, Juni 2001 (INT-1) ⇐ und alle zukünftigen Fortentwicklungen dieses Standards.

Norm für die Kennbuchstaben der Mitgliedstaaten

Es gilt folgende ISO-Norm: ISO 3166 – 2 – Buchstaben-Code.

EURODAC – Fingerabdruckblatt

1.	Kennnummer			
2.	Ort der Antragstellung oder des Aufgriffs			
3.	Zeitpunkt der Antragstellung oder des Aufgriffs			
4.	Geschlecht			
5.	Zeitpunkt der Abnahme der Fingerabdrücke			
6.	Zeitpunkt der Übermittlung der Daten an das Zentralsystem			

105 mm vom oberen Rand des Formblatts

155 mm vom oberen Rand des Formblatts

205 mm vom oberen Rand des Formblatts

ABGEROLLTE FINGERABDRÜCKE

1. Daumen rechts	2. Zeigefinger rechts	3. Mittelfinger rechts	4. Ringfinger rechts	5. Kleiner Finger rechts
50 mm	40 mm	40 mm	40 mm	40 mm
6. Daumen links	7. Zeigefinger links	8. Mittelfinger links	9. Ringfinger links	10. Kleiner Finger links
40 mm				

KONTROLL-FINGERABDRÜCKE

LINKE HAND Gleichzeitiger Abdruck der vier Finger 75 mm 65 mm	BEIDE DAUMEN Gleichzeitiger Abdruck der Finger		RECHTE HAND Gleichzeitiger Abdruck der vier Finger 75 mm
	LINKS	RECHTS	
	30 mm	30 mm	



ANHANG II
Aufgehobene Verordnungen
(Bezugnahme in Artikel 45)

Verordnung (EG) Nr. 2725/2000 des Rates (ABl. L 316 vom 15.12.2000, S. 1)

Verordnung (EG) Nr. 407/2002 des Rates (ABl. L 62 vom 5.3.2002, S. 1)

ANHANG III
Entsprechungstabelle

Verordnung (EG) Nr. 2725/2000	Diese Verordnung
Artikel 1 Absatz 1	Artikel 1 Absatz 1
Artikel 1 Absatz 2 Unterabsatz 1	Artikel 3 Absatz 1
Artikel 1 Absatz 2 Unterabsatz 2	gestrichen
Artikel 1 Absatz 2 Unterabsatz 3	Artikel 3 Absatz 4
Artikel 1 Absatz 3	Artikel 1 Absatz 3
Artikel 2	Artikel 2
Artikel 3 Absatz 1	gestrichen
Artikel 3 Absatz 2	Artikel 3 Absatz 3
Artikel 3 Absatz 3	Artikel 8
Artikel 3 Absatz 4	gestrichen
Artikel 4 Absatz 1	Artikel 9 Absatz 1 und Artikel 3 Absatz 5
Artikel 4 Absatz 2	gestrichen
Artikel 4 Absatz 3	Artikel 9 Absatz 3
Artikel 4 Absatz 4	Artikel 9 Absatz 4
Artikel 4 Absatz 5	Artikel 9 Absatz 5
Artikel 4 Absatz 6	Artikel 25 Absatz 4
Artikel 5	Artikel 11
Artikel 6	Artikel 12
Artikel 7	Artikel 13
Artikel 8	Artikel 14

Artikel 9	Artikel 15
Artikel 10	Artikel 16
Artikel 11 Absätze 1 bis 4	Artikel 17 Absätze 1 bis 4
Artikel 11 Absatz 5	gestrichen
Artikel 12	Artikel 18
Artikel 13	Artikel 23
Artikel 14	gestrichen
Artikel 15	Artikel 27
Artikel 16	Artikel 28
Artikel 17	Artikel 37
Artikel 18	Artikel 29
Artikel 19	Artikel 30
Artikel 20	gestrichen
Artikel 21	Artikel 39
Artikel 22	gestrichen
Artikel 23	gestrichen
Artikel 24	Artikel 40
Artikel 25	Artikel 24
Artikel 26	Artikel 42
Artikel 27	Artikel 46

**Verordnung (EG)
Nr. 407/2002**

Diese Verordnung

Artikel 2

Artikel 24

Artikel 3

Artikel 25

Artikel 4

Artikel 26

Artikel 5 Absatz 1

Artikel 3 Absatz 3

Anhang I

Anhang I

Anhang II

gestrichen

FINANZBOGEN ZU RECHTSAKTEN

1. RAHMEN DES VORSCHLAGS/DER INITIATIVE

- 1.1. Bezeichnung des Vorschlags/der Initiative
- 1.2. Politikbereiche in der ABM/ABB-Struktur
- 1.3. Art des Vorschlags/der Initiative
- 1.4. Ziel(e)
- 1.5. Begründung des Vorschlags/der Initiative
- 1.6. Dauer der Maßnahme und ihrer finanziellen Auswirkungen
- 1.7. Vorgeschlagene Methode(n) der Mittelverwaltung

2. VERWALTUNGSMASSNAHMEN

- 2.1. Monitoring und Berichterstattung
- 2.2. Verwaltungs- und Kontrollsystem
- 2.3. Prävention von Betrug und Unregelmäßigkeiten

3. ERWARTETE FINANZIELLE AUSWIRKUNGEN DES VORSCHLAGS/DER INITIATIVE

- 3.1. Betroffene Rubrik(en) des mehrjährigen Finanzrahmens und Ausgabenlinie(n)
- 3.2. Erwartete Auswirkungen auf die Ausgaben
 - 3.2.1. *Übersicht*
 - 3.2.2. *Erwartete Auswirkungen auf die Mittel [der Einrichtung]*
 - 3.2.3. *Erwartete Auswirkungen auf die Humanressourcen [der Einrichtung]*
 - 3.2.4. *Vereinbarkeit mit dem mehrjährigen Finanzrahmen*
 - 3.2.5. *Finanzierungsbeteiligung Dritter*
- 3.3. Auswirkungen auf die Einnahmen

FINANZBOGEN ZU RECHTSAKTEN

11. RAHMEN DES VORSCHLAGS/DER INITIATIVE

11.1. Bezeichnung des Vorschlags/der Initiative

Geänderter Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Einrichtung von „EURODAC“ für den Abgleich von Fingerabdruckdaten zum Zweck der effektiven Anwendung der Verordnung (EU) Nr. [.../...] [zur 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 mit 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

11.2. Politikbereiche in der ABM/ABB-Struktur⁴⁴

Politikbereich: Inneres (Titel 18)

Tätigkeit: Agentur für das Betriebsmanagement von IT-Großsystemen im Bereich Freiheit, Sicherheit und Recht (Artikel 18 02 11)

11.3. Art des Vorschlags/der Initiative

Der Vorschlag/die Initiative betrifft eine **neue Maßnahme**.

Der Vorschlag/die Initiative betrifft eine **neue Maßnahme im Anschluss an ein Pilotprojekt/eine vorbereitende Maßnahme**⁴⁵.

Der Vorschlag/die Initiative betrifft die **Verlängerung einer bestehenden Maßnahme**.

Der Vorschlag/die Initiative betrifft eine **neu ausgerichtete Maßnahme**.

11.4. Ziele

11.4.1 *Mit dem Vorschlag/der Initiative verfolgte mehrjährige strategische Ziele der Kommission*

Entfällt

11.4.2 *Einzelziele und ABM/ABB-Tätigkeiten*

Einzelziel Nr. 1

⁴⁴ ABM: Activity Based Management: maßnahmenbezogenes Management – ABB: Activity Based Budgeting: maßnahmenbezogene Budgetierung.

⁴⁵ Im Sinne von Artikel 49 Absatz 6 Buchstabe a oder b der Haushaltsordnung.

Beitrag zum Gemeinsamen Europäischen Asylsystem durch strengere gemeinsame Schutzstandards, Unterstützung der Zusammenarbeit in der Praxis und Stärkung der Solidarität innerhalb der EU und zwischen EU-Staaten und Drittstaaten mit Unterstützung des Europäischen Flüchtlingsfonds

Einzelziel Nr. 2

Beitrag zur Verhütung, Aufdeckung und Untersuchung terroristischer und sonstiger schwerer Straftaten

ABM/ABB-Tätigkeiten

18 02– Solidarität – Außengrenzen, Rückkehr, Visapolitik und Freizügigkeit von Personen

11.4.3. Erwartete Ergebnisse und Auswirkungen

Bitte geben Sie an, wie sich der Vorschlag/die Initiative auf die Empfänger/Zielgruppe auswirken dürfte.

Der vorliegende Vorschlag übernimmt die Verbesserungen der Regelungen vom vorhergehenden Vorschlag [KOM(2010) 555 endg.], also die neuen Funktionen für Asylangelegenheiten, und zusätzlich die Abfragefunktion zu Strafverfolgungszwecken, die ursprünglich in KOM(2009) 342 endg. und KOM(2009) 344 endg. vorgeschlagen worden war.

Die Daten der von der Verarbeitung Betroffenen werden besser verwaltet und geschützt werden können. Gleichzeitig werden die Mitgliedstaaten leichter feststellen können, welcher Mitgliedstaat für die Prüfung eines Asylantrags zuständig ist. Um die Verhütung, Aufdeckung und Untersuchung terroristischer und sonstiger schwerer Straftaten zu erleichtern, wird die Datenabfrage in EURODAC zu Strafverfolgungszwecken erlaubt.

11.4.4. Leistungs- und Erfolgsindikatoren

Bitte geben Sie an, anhand welcher Indikatoren sich die Realisierung des Vorschlags/der Initiative verfolgen lässt.

Was die Verbesserung des Datenschutzes und der Leistungsfähigkeit von EURODAC betrifft, kommen als Indikatoren die jährlichen Statistiken über die Anwendung von EURODAC, d. h. die Statistiken über verpasste Treffer, falsche Treffer, Übermittlungsverzögerungen usw., sowie die alle vier Jahre stattfindende Evaluierung von EURODAC in Betracht. Die geplante Änderung, Daten zu „markieren“ statt – wie in der ursprünglichen Verordnung – zu „blockieren“, soll von der IT-Agentur binnen zwei Jahren nach Veröffentlichung der Verordnung umgesetzt werden. Als Erfolgsindikatoren gelten der jährliche EURODAC-Bericht, der Aufschluss darüber geben wird, in wie vielen Fällen Daten markiert wurden, und die Antworten der Mitgliedstaaten in der alle vier Jahre stattfindenden Evaluierung, die Auskunft darüber geben werden, ob diese Informationen eine Rücküberstellung in das Land ermöglicht haben, das die betroffene Person von Anfang an hätte aufnehmen sollen. Mit der Änderung der Bestimmungen über die Löschung der Daten soll sichergestellt werden, dass in EURODAC keine Daten von EU-Bürgern gespeichert werden. Dies lässt sich beim EU-Beitritt neuer Mitgliedstaaten (z. B. Kroatien) überprüfen: Alle Daten, die kroatische Staatsbürger betreffen, müssten dann automatisch gelöscht werden. Ob diese Änderung erfolgreich umgesetzt wurde, wird die vierjährige Evaluierung zeigen.

Was die Indikatoren für eine bessere Verhütung, Aufdeckung und Untersuchung terroristischer und anderer schwerer Straftaten anbelangt, so wären hierzu die Statistiken über die Anzahl solcher Straftaten heranzuziehen, die nach einer EURODAC-Abfrage zu Strafverfolgungszwecken verhütet, aufgedeckt oder untersucht werden konnten. Die IT-Modifikationen, die einen Abgleich mit Fingerabdruckspuren ermöglichen, sollen von der IT-Agentur innerhalb von zwei Jahren nach Veröffentlichung der Verordnung vorgenommen werden. Es lässt sich nicht vorhersagen, wie viele Anträge zu Strafverfolgungszwecken gestellt werden, aber auch wenn im Laufe mehrerer Jahre nur einige wenige schwere Straftaten aufgeklärt oder verhindert werden, hat sich die Investition gelohnt. Der Vorschlag enthält erhebliche Schutzvorkehrungen, um eine exzessive Abfrage zu Strafverfolgungszwecken zu verhindern (es muss sich um eine schwere Straftat im Sinne des Europäischen Haftbefehls handeln und die Prüm-Kriterien müssen gegeben sein). Ein

Erfolgsindikator ist deshalb auch die Feststellung, ob nur solche Anträge gestellt werden, die diesen strengen Kriterien genügen.

Artikel 40 des Vorschlags enthält statistische Vorgaben.

11.5. Begründung des Vorschlags/der Initiative

11.5.1. Kurz- oder langfristig zu deckender Bedarf

Näheres zu den folgenden Ausführungen findet sich in den Abschnitten 1, 3, 5 und 7 der Begründung des Vorschlags:

Damit sich die Mitgliedstaaten über den Status derjenigen Antragsteller informieren können, denen in einem Mitgliedstaat bereits internationaler Schutz gewährt wurde, *sollten die Daten über Flüchtlinge freigegeben werden* (d. h. abrufbar gemacht werden).

Um die Anwendung der Dublin-Verordnung zu erleichtern, müssen die Mitgliedstaaten *die Fälle in EURODAC angeben, in denen sie die Souveränitäts- oder die humanitäre Klausel der Verordnung anwenden*, d. h. in denen sie die Verantwortung für die Prüfung des Antrags einer Person übernehmen, für die sie normalerweise nach den Kriterien der Dublin-Verordnung nicht zuständig wären.

Um die *Kohärenz des Asyl-Besitzstands* zu gewährleisten, wird vorgeschlagen, den Anwendungsbereich der Verordnung auf den subsidiären Schutz auszudehnen.

Des Weiteren wird zur Gewährleistung der *Kohärenz des Asyl-Besitzstands* vorgeschlagen, die Aufbewahrungszeit für Daten von Drittstaatsangehörigen oder Staatenlosen, deren Fingerabdrücke nach illegalem Überschreiten einer Außengrenze abgenommen wurden, dem Zeitraum anzugleichen, für den Artikel 10 Absatz 1 der Dublin-Verordnung die Zuständigkeit auf der Grundlage dieser Information zuweist (d. h. ein Jahr).

Infolge des Ergebnisses der Verhandlungen im Rat wurde ein neuer Artikel eingeführt, damit die Mitgliedstaaten über Informationen zur Rechtsstellung der betroffenen Person (Asylsucher oder illegaler Einwanderer) verfügen. Der neue Artikel sieht vor, dass die Mitgliedstaaten auch zu informieren sind, wenn eine bestimmte Person, deren Daten in der Datenbank gespeichert sind, nach einem Dublin-Aufnahmeverfahren überstellt wurde oder freiwillig oder aufgrund eines Rückführungsbeschlusses oder einer Abschiebungsanordnung das Hoheitsgebiet der Mitgliedstaaten verlassen hat.

Um die Verhütung, Aufdeckung und Untersuchung terroristischer und anderer schwerer Straftaten zu erleichtern, wird der Zugang zu EURODAC für Datenabfragen zu Strafverfolgungszwecken erlaubt.

11.5.2. Mehrwert durch die Intervention der EU

Laut Europol stellt die zunehmende grenzüberschreitende Kriminalität eine der größten Bedrohungen für unsere Gesellschaft dar. Ohne eine adäquate, effiziente Zusammenarbeit der Strafverfolgungsbehörden der Mitgliedstaaten, zu der auch der Zugang zu relevanten Informationen in anderen Mitgliedstaaten gehört, wird es für diese Behörden sehr schwierig, wenn nicht gar unmöglich sein, ihre Aufgaben im Zusammenhang mit der Verhütung,

Aufdeckung und Untersuchung terroristischer und anderer schwerer Straftaten zu erfüllen, d. h. die grenzüberschreitende Kriminalität wirksam zu bekämpfen. Aufgrund der Beschaffenheit dieser Straftaten bedarf es eines Instrumentariums auf EU-Ebene, das als Grundlage für die länderübergreifende Zusammenarbeit bei der Kriminalitätsbekämpfung dienen kann.

Maßnahmen auf EU-Ebene haben außerdem den Vorteil, dass gleiche Vorschriften für den Datenschutz gelten. Würden die Mitgliedstaaten ihre eigenen Vorschriften erlassen, wäre die Harmonisierung derartiger Schutzvorschriften sehr viel schwieriger. Blicke die EU untätig, wäre dies dem Datenschutz abträglich, da die Strafverfolgungsbehörden gezwungen wären, weit mehr Daten zu verarbeiten als nötig wäre, wenn sie Zugang zu einem Zentralregister der verfügbaren Daten hätten. Da die Schutzvorschriften nicht EU-weit angeglichen wären, wäre zudem beim Schutz personenbezogener Daten unter Umständen ein sehr starkes Gefälle zwischen den Mitgliedstaaten zu beobachten. Die Behörden könnten die Daten nicht gezielt bei dem Mitgliedstaat abfragen, der sie gespeichert hat, sondern müssten ihre Anfragen an alle Mitgliedstaaten richten. All diese Anfragen hätten letztlich zur Folge, dass weit mehr Daten verarbeitet würden, was an sich schon für den Datenschutz von Nachteil ist.

EURODAC ist eine Fingerabdruck-Datenbank, die zurzeit noch von der Europäischen Kommission, in Zukunft aber von der IT-Agentur betrieben wird, so dass nur die Union die notwendige Aktualisierung des EURODAC-Systems vornehmen kann, wie sie in der letzten Bewertung von EURODAC beschrieben wurde. Die Zentraleinheit muss die Änderungen im Hinblick auf die Datenmarkierung (statt wie bisher Datenblockierung) vollziehen. Die Mitgliedstaaten, die zu Strafverfolgungszwecken auf EURODAC zugreifen wollen, können dies nur über das hier vorgeschlagene zentral koordinierte System tun. Die Union muss deshalb die Grundlage dafür schaffen, dass Fingerabdruckspuren von einem Tatort mit Fingerabdrücken, die bei der Stellung eines Asylantrags abgenommen wurden, verglichen werden können. Ein solcher Datenabgleich wäre ohne Intervention der Union nicht möglich.

11.5.3. Erkenntnisse aus früheren ähnlichen Maßnahmen

Die EURODAC-Datenbank, die Fingerabdrücke aller Asylbewerber in der EU enthält, wird seit dem 15. Januar mit Erfolg betrieben. Ihre ursprüngliche Auslegung war für den intendierten Zweck größtenteils gut geeignet, aber wie die Bewertung des Dublin-Systems 2007, zu dem auch die EURODAC-Verordnung gehört, gezeigt hat,⁴⁶ sind gewisse Anpassungen notwendig, damit die Datenbank besser genutzt werden kann. Die hier vorgeschlagenen Änderungen beruhen somit überwiegend auf den aus den früheren Bewertungen gewonnenen Erkenntnissen. Mit dem Einsatz von EURODAC für Strafverfolgungszwecke ist überdies ein weiterer Effizienzgewinn verbunden, da bereits vorhandene Daten mit einer nur geringen Investition von EU-Mitteln besser genutzt werden können.

⁴⁶ KOM(2007) 299 endg.

11.5.4. *Kohärenz mit anderen Finanzierungsinstrumenten sowie mögliche Synergieeffekte*

Der vorliegende Vorschlag steht mit dem Vorschlag zur Neufassung der Dublin-Verordnung⁴⁷ in Einklang.

⁴⁷ Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur 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, (KOM(2008) 820).

11.6. Dauer der Maßnahme und ihrer finanziellen Auswirkungen

Vorschlag/Initiative mit **befristeter Geltungsdauer**

– Geltungsdauer: [TT/MM]JJJJ bis [TT/MM]JJJJ

– Finanzielle Auswirkungen: JJJJ bis JJJJ

Vorschlag/Initiative mit **unbefristeter Geltungsdauer**

– Umsetzung mit einer Anlaufphase von [Jahr] bis [Jahr],

– Vollbetrieb wird angeschlossen.

11.7. Vorgeschlagene Methoden der Mittelverwaltung⁴⁸

Indirekte zentrale Verwaltung durch Übertragung von Haushaltsvollzugsaufgaben an:

– Exekutivagenturen

– von der Europäischen Union geschaffene Einrichtungen⁴⁹

– nationale öffentliche Einrichtungen bzw. privatrechtliche Einrichtungen, die im öffentlichen Auftrag tätig werden

– Personen, die mit der Durchführung bestimmter Maßnahmen im Rahmen des Titels V des Vertrags über die Europäische Union betraut und in dem maßgeblichen Basisrechtsakt nach Artikel 49 der Haushaltsordnung bezeichnet sind

Gemeinsame Verwaltung mit internationalen Organisationen (*bitte auflisten*)

Falls mehrere Methoden der Mittelverwaltung zum Einsatz kommen, ist dies unter „Bemerkungen“ näher zu erläutern.

Bemerkungen

EURODAC wird der Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts („IT-Agentur“) unterstellt. Die IT-Agentur wird die weiteren im EURODAC-Vorschlag erläuterten Funktionen entwickeln.

⁴⁸ Erläuterungen zu den Methoden der Mittelverwaltung und Verweise auf die Haushaltsordnung enthält die Website BudgWeb (in französischer und englischer Sprache): http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

⁴⁹ Einrichtungen im Sinne des Artikels 185 der Haushaltsordnung.

12. VERWALTUNGSMASSNAHMEN

12.1. Monitoring und Berichterstattung

Bitte geben Sie an, wie oft und unter welchen Bedingungen diese Tätigkeiten erfolgen.

Die Wirksamkeit der mit diesem Vorschlag eingeführten Änderungen wird im Rahmen von Jahresberichten über die Tätigkeit des EURODAC-Zentralsystems kontrolliert. Für die Überwachung des Datenschutzes ist der Europäische Datenschutzbeauftragte zuständig.

Nationale Stellen, die für die Beaufsichtigung der Verarbeitung personenbezogener Daten zuständig sind, sollten die Rechtmäßigkeit der Verarbeitung personenbezogener Daten durch die Mitgliedstaaten überwachen, während die mit dem Europol-Beschluss eingerichtete gemeinsame Kontrollinstanz die Rechtmäßigkeit der Datenverarbeitung durch Europol überwachen sollte.

Die Bewertung von EURODAC war in der ursprünglichen Verordnung in Artikel 24 geregelt. In diesem Vorschlag ist die Überwachung und Bewertung der Datenbank in Artikel 40 geregelt.

12.2. Verwaltungs- und Kontrollsystem

12.2.1. Ermittelte Risiken

Wird die Verordnung in ihrer derzeitigen Fassung nicht erheblich geändert, sind die Wirksamkeit von EURODAC sowie der Zweck des Systems, nämlich die Unterstützung der Anwendung der Dublin-Verordnung, in Frage gestellt. Wenn die Verordnung nicht an die Veränderungen des Asyl- und des Datenschutzrechts angepasst wird, könnten sich hieraus große Probleme ergeben.

12.2.2. Vorgesehene Kontrollen

Indikatoren sind die Statistiken über die Anwendung von EURODAC, d. h. die Statistiken über verpasste Treffer, falsche Treffer, Übermittlungsverzögerungen usw.

12.3. Prävention von Betrug und Unregelmäßigkeiten

Bitte geben Sie an, welche Präventions- und Schutzmaßnahmen bestehen oder vorgesehen sind.

Zur Bekämpfung von Betrug, Korruption und sonstigen rechtswidrigen Handlungen finden die Vorschriften der Verordnung (EG) Nr. 1037/1999 auf die für das Betriebsmanagement von EURODAC zuständige Agentur uneingeschränkt Anwendung.

Die Agentur tritt der Interinstitutionellen Vereinbarung über die internen Untersuchungen des Europäischen Amtes für Betrugsbekämpfung (OLAF) bei und erlässt unverzüglich die für alle Beschäftigten der Agentur geltenden einschlägigen Vorschriften.

Die Finanzierungsbeschlüsse sowie die sich daraus ergebenden Durchführungsvereinbarungen und -instrumente sehen ausdrücklich vor, dass der Rechnungshof und OLAF

erforderlichenfalls eine Vor-Ort-Kontrolle bei den Empfängern der Mittel der Agentur sowie bei den verteilenden Stellen durchführen können.

13. ERWARTETE FINANZIELLE AUSWIRKUNGEN DES VORSCHLAGS/DER INITIATIVE

13.1. Betroffene Rubrik(en) des mehrjährigen Finanzrahmens und Ausgabenlinie(n)

1. Bestehende Haushaltslinien

In der Reihenfolge der Rubriken des mehrjährigen Finanzrahmens und der Haushaltslinien.

Rubrik des mehrjährigen Finanzrahmens	Haushaltslinie	Art der Ausgaben	Finanzierungsbeiträge			
	Nummer [Bezeichnung.....]	GM/NGM ⁽⁵⁰⁾	von EFTA-Ländern ⁵¹	von Bewerberländern ⁵²	von Drittländern	nach Artikel 18 Absatz 1 Buchstabe aa der Haushaltsordnung
3A	18.02.11.01 Agentur für das Betriebsmanagement von IT-Großsystemen im Bereich Freiheit, Sicherheit und Recht — Beitrag zu den Titeln 1 und 2	GM	NEIN	NEIN	JA	NEIN
	18.02.11.02 Agentur für das Betriebsmanagement von IT-Großsystemen im Bereich Freiheit, Sicherheit und Recht — Beitrag zu Titel 3					

2. Neu zu schaffende Haushaltslinien

In der Reihenfolge der Rubriken des mehrjährigen Finanzrahmens und der Haushaltslinien.

Rubrik des mehrjährigen Finanzrahmens	Haushaltslinie	Art der Ausgaben	Finanzierungsbeiträge			
	Nummer [Bezeichnung.....]	GM/NGM	von EFTA-Ländern	von Bewerberländern	von Drittländern	nach Artikel 18 Absatz 1 Buchstabe aa der Haushaltsordnung
	[XX.YY.YY.YY]		JA/NEIN	JA/NEIN	JA/NEIN	JA/NEIN

⁵⁰ GM=Getrennte Mittel / NGM=Nicht getrennte Mittel.

⁵¹ EFTA: Europäische Freihandelsassoziation.

⁵² Bewerberländer und gegebenenfalls potenzielle Bewerberländer des Westbalkans.

13.2. Erwartete Auswirkungen auf die Ausgaben

13.2.1. Übersicht

in Mio. EUR (3 Dezimalstellen)

Rubrik des mehrjährigen Finanzrahmens	Nummer	[Rubrik 3A]
--	---------------	-------------

GD <Inneres>			Jahr N ⁵³ (2013)	Jahr N+1	Jahr N+2		Bei längerer Dauer (Ziff. 1.6.) bitte weitere Spalten einfügen			INSGESAMT
Titel 1 (Personalausgaben) ⁵⁴	Verpflichtungen	(1)	0,128	0,064	0,064					0,256
	Zahlungen	(2)	0,128	0,064	0,064					0,256
Titel 2 (Sonstige Verwaltungsausgaben) ⁵⁵	Verpflichtungen	(1a)	0,100	0	0					0,100
	Zahlungen	(2a)	0,100	0	0					0,100
Titel 3 (Operative Ausgaben)	Verpflichtungen	(3a)	2,415	0	0					2,415
	Zahlungen	(3b)	1,690	0,725	0					2,415
Mittel INSGESAMT für GD <Inneres>	Verpflichtungen	=1+1a +3	2,643	0,064	0,064					2,771
	Zahlungen	=2+2a +3b	1,918	0,789	0,064					2,771

⁵³ Das Jahr N ist das Jahr, in dem mit der Umsetzung des Vorschlags/der Initiative begonnen wird.

⁵⁴ Zur Erläuterung der Personalausgaben siehe 13.2.3.1.

⁵⁵ Konferenzen, Sitzungen, sonstige Verwaltungsausgaben.

Rubrik des mehrjährigen Finanzrahmens	5	Verwaltungsausgaben
--	----------	---------------------

in Mio. EUR (3 Dezimalstellen)

		Jahr N	Jahr N+1	Jahr N+2	Jahr N+3	Bei längerer Dauer (Ziff. 1.6.) bitte weitere Spalten einfügen			INSGESAMT
GD <Inneres>									
• Personalausgaben		0	0	0					
• Sonstige Verwaltungsausgaben		0	0	0					
GD <Inneres> INSGESAMT	Mittel	0	0	0					

Mittel INSGESAMT unter RUBRIK 5 des mehrjährigen Finanzrahmens	(Verpflichtungen insges. = Zahlungen insges.)	0	0	0					
---	--	---	---	---	--	--	--	--	--

in Mio. EUR (3 Dezimalstellen)

		Jahr N ⁵⁶	Jahr N+1	Jahr N+2	Jahr N+3	Bei längerer Dauer (Ziff. 1.6.) bitte weitere Spalten einfügen			INSGESAMT
Mittel INSGESAMT unter RUBRIKEN 1 bis 5 des mehrjährigen Finanzrahmens	Verpflichtungen	2,643	0,064	0,064					2,771
	Zahlungen	1,918	0,789	0,064					2,771

⁵⁶ Das Jahr N ist das Jahr, in dem mit der Umsetzung des Vorschlags/der Initiative begonnen wird.

13.2.2. Erwartete Auswirkungen auf die Mittel [der Einrichtung]

- Für den Vorschlag/die Initiative werden keine operativen Mittel benötigt.
- Für den Vorschlag/die Initiative werden die folgenden operativen Mittel benötigt:

Mittel für Verpflichtungen, in Mio. EUR (3 Dezimalstellen)

Ziele und Outputs			Jahr	Jahr	Jahr	Jahr	Bei längerer Dauer (Ziff. 1.6.) bitte weitere Spalten einfügen					INSGESAMT				
			N	N+1	N+2	N+3										
↓													OUTPUTS			
	Art ⁵⁷	Durchschnittskosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Gesamtzahl	Gesamtkosten

EINZELZIEL Nr. 1:⁵⁸ Asylrechtliche Anforderungen nach der EURODAC-Verordnung

Andere Änderungen als für Strafverfolgungszwecke	Realisierung		1	0,100	0	0	0	0	0	0	0	0	0	0		0,100
Zwischensumme für Einzelziel Nr. 1			1	0,100	0	0	0	0	0	0	0	0	0	0		0,100

EINZELZIEL Nr. 2: Beitrag zur Verhütung, Aufdeckung und Untersuchung terroristischer und sonstiger schwerer Straftaten

Änderungen für Strafverfolgungszwecke	Realisierung		1	2,543	1	0,064	1	0,064								2,671
Zwischensumme für Einzelziel Nr. 2			1	2,543	1	0,064	1	0,064								2,671

⁵⁷ Outputs sind Produkte, die geliefert, und Dienstleistungen, die erbracht werden (z. B.: Austausch von Studenten, gebaute Straßenkilometer...)

⁵⁸ Wie in Ziffer 1.4.2. „Einzelziele ...“.

GESAMTKOSTEN

2 2,643 1 0,064 1 0,064

2,771

13.2.3. Erwartete Auswirkungen auf die Humanressourcen der IT-Agentur

13.2.3.1. Zusammenfassung

- Für den Vorschlag/die Initiative werden keine Verwaltungsmittel benötigt.
- Für den Vorschlag/die Initiative werden die folgenden Verwaltungsmittel benötigt:

in Mio. EUR (3 Dezimalstellen)

	Jahr N ⁵⁹	Jahr N+1	Jahr N+2	Jahr N+3	Bei längerer Dauer (Ziff. 1.6.) bitte weitere Spalten einfügen	INSGES AMT
--	-------------------------	-------------	-------------	-------------	---	---------------

Beamte der Funktionsgruppe AD							
Beamte der Funktionsgruppe AST							
Vertragsbedienstete	0,128	0,064	0,064				0,256
Zeitbedienstete							
Abgeordnete nationale Sachverständige							

INSGESAMT	0,128	0,064	0,064				0,256
------------------	--------------	--------------	--------------	--	--	--	--------------

Personalbedarf pro Jahr	N	N+1	N+2
Personalbedarf insgesamt	2	1	1

Das vorhandene Personal der IT-Agentur kann für die Umrüstung von EURODAC nicht eingesetzt werden, weil es nicht auf Systementwicklung spezialisiert ist und für den Betrieb der bestehenden EURODAC-Funktionen benötigt wird. Die in diesem Vorschlag eingeführte Möglichkeit, Fingerabdruckspuren von einem Tatort mit abgenommenen Fingerabdrücken zu vergleichen, erfordert Sachkenntnisse, über die die IT-Agentur und die Kommission derzeit nicht verfügen. Daher müssen Vertragsbedienstete wie folgt eingestellt werden:

⁵⁹ Das Jahr N ist das Jahr, in dem mit der Umsetzung des Vorschlags/der Initiative begonnen wird.

Jahr N: Zwei Vertragsbedienstete für technische Aufgaben (Arbeit an den technischen Spezifikationen, technische Unterstützung für administrative Aufgaben, Koordinierung der internen Dienststellen) und für die Betreuung von Vergabeverfahren (Vorbereitung und Veröffentlichung von Ausschreibungen, Mitwirkung in den Ausschüssen für die Öffnung und Bewertung der Angebote, Erstellung des Bewertungsberichts, Zuschlagserteilung, Vertragsunterzeichnung).

In den Jahren N+1 und N+2 wird ein Mitarbeiter benötigt für technische Aufgaben (Projektmanagement, Follow-up der Vertragsleistungen, qualitative Prüfung und Annahme der Vertragsleistungen, Koordinierung der internen Dienststellen, Dienstleistungsaufträge, Änderungswünsche).

Im Jahr N+3 werden, sobald die Entwicklungsphase abgeschlossen ist, neue Funktionen verfügbar sein. Zusätzliches Personal dürfte dann nicht mehr erforderlich sein.

13.2.3.2. Erwarteter Personalbedarf bei der übergeordneten GD

- Für den Vorschlag/die Initiative wird kein Personal benötigt.
- Für den Vorschlag/die Initiative wird das folgende Personal benötigt:

Schätzung in ganzzahligen Werten (oder mit höchstens einer Dezimalstelle)

	Jahr N	Jahr N+1	Jahr N+2	Jahr N+3	Bei längerer Dauer (Ziff. 1.6.) bitte weitere Spalten einfügen		
• Im Stellenplan vorgesehene Planstellen (Beamte und Bedienstete auf Zeit)							
XX 01 01 01 (am Sitz und in den Vertretungen der Kommission)							
XX 01 01 02 (in den Delegationen)							
XX 01 05 01 (indirekte Forschung)							
10 01 05 01 (direkte Forschung)							
• Externes Personal (in Vollzeitäquivalenten = FTE)⁶⁰							
XX 01 02 01 (AC, INT, ANS der Globaldotation)							
XX 01 02 02 (AC, INT, JED, AL und ANS in den Delegationen)							
XX 01 04 <i>yy⁶¹</i>	- am Sitz ⁶²						
	- in den Delegationen						
XX 01 05 02 (AC, INT, ANS der indirekten Forschung)							
10 01 05 02 (AC, INT, ANS der direkten Forschung)							
Sonstige Haushaltslinien (bitte angeben)							
INSGESAMT							

XX steht für den jeweiligen Haushaltstitel bzw. Politikbereich

⁶⁰ AC= Vertragsbediensteter, INT= Leiharbeitskraft („*Intérimaire*“), JED = Junger Sachverständiger in Delegationen, AL = örtlich Bediensteter, ANS = Abgeordneter Nationaler Sachverständiger.

⁶¹ Teilobergrenze für aus den operativen Mitteln finanziertes externes Personal (vormalige BA-Linien).

⁶² Insbesondere Strukturfonds, Europäischer Landwirtschaftsfonds für die Entwicklung des ländlichen Raums (ELER) und Europäischer Fischereifonds (EFF).

Der Personalbedarf wird durch der Verwaltung der Maßnahme zugeordnetes Personal der GD oder GD-interne Personalumsetzung gedeckt. Hinzu kommen etwaige zusätzliche Mittel für Personal, die der für die Verwaltung der Maßnahme zuständigen GD nach Maßgabe der verfügbaren Mittel im Rahmen der jährlichen Mittelzuweisung zugeteilt werden.

Beschreibung der auszuführenden Aufgaben:

Beamte und Zeitbedienstete	
Externes Personal	

Einzelheiten der Kostenberechnung für die VZE sind im Anhang zum Abschnitt 3 anzugeben.

13.2.4. Vereinbarkeit mit dem mehrjährigen Finanzrahmen

- Der Vorschlag/die Initiative ist sowohl mit dem mehrjährigen Finanzrahmen für 2007-13 als auch mit dem für 2014-20 vereinbar.
- Der Vorschlag/die Initiative erfordert eine Anpassung der betreffenden Rubrik des mehrjährigen Finanzrahmens.

Bitte erläutern Sie die erforderliche Anpassung unter Angabe der einschlägigen Haushaltslinien und der entsprechenden Beträge.

- Der Vorschlag/die Initiative erfordert eine Inanspruchnahme des Flexibilitätsinstruments oder eine Änderung des mehrjährigen Finanzrahmens⁶³.

Bitte erläutern Sie den Bedarf unter Angabe der einschlägigen Rubriken und Haushaltslinien sowie der entsprechenden Beträge.

13.2.5. Finanzierungsbeteiligung Dritter

- Der Vorschlag/die Initiative sieht keine Kofinanzierung durch Dritte vor.
- Der Vorschlag/die Initiative sieht folgende Kofinanzierung vor:

Mittel in Mio. EUR (3 Dezimalstellen)

	Jahr N	Jahr N+1	Jahr N+2	Jahr N+3	Bei längerer Dauer (Ziff. 1.6.) bitte weitere Spalten einfügen			Insgesamt
Geldgeber/kofinanzierende Organisation								
Kofinanzierung INSGESAMT								

⁶³ Siehe Nummern 19 und 24 der Interinstitutionellen Vereinbarung.

13.3. Auswirkungen auf die Einnahmen

- Der Vorschlag/die Initiative wirkt sich nicht auf die Einnahmen aus.
- Der Vorschlag/die Initiative wirkt sich auf die Einnahmen aus, und zwar
 - auf die Eigenmittel
 - (1) auf die sonstigen Einnahmen

in Mio. EUR (3 Dezimalstellen)

Einnahmenlinie:	Für das laufende Haushaltsjahr zur Verfügung stehende Mittel	Auswirkungen des Vorschlags/der Initiative ⁶⁴					Bei längerer Dauer (Ziff. 1.6.) bitte weitere Spalten einfügen		
		Jahr N	Jahr N+1	Jahr N+2	Jahr N+3				

Bitte geben Sie für die sonstigen zweckgebundenen Einnahmen die einschlägigen Ausgabenlinien an.

Einnahmenlinie 6312

Bitte geben Sie an, wie die Auswirkungen auf die Einnahmen berechnet werden.

[NO, IS und CH zahlen einen Beitrag in Höhe von 12,452 % der Zahlungen im jeweiligen Jahr]

⁶⁴ Bei den traditionellen Eigenmitteln (Zölle, Zuckerabgaben) sind die Beträge netto, d. h. abzüglich 25 % für Erhebungskosten, anzugeben.

Anlage 2



**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 12 October 2012

**5086/7/12
REV 7**

**JAI 5
DAPIX 3
ENFOPOL 5
CRIMORG 3**

NOTE

from: Presidency
to: Working Group on Information Exchange and Data Protection (DAPIX)

No. prev. doc.: 6077/10/11 REV 10 JAI 72 DAPIX 5 ENFOPOL 19 CRIMORG 6

Subject: Implementation of the provisions on information exchange of the "Prüm Decisions"
- overview of documents and procedures
- overview of declarations
- state of play of implementation of automated data exchange

1. Introduction and content of the document

The provisions of the "Prüm Decisions"¹ relating to information exchange concern:

- supply of information relating to major events and in order to prevent terrorist offences;
- automated searching of DNA profiles, dactyloscopic data and vehicle registration data (VRD);
- data protection.

¹ Council Decision 2008/615/JHA and 2008/616/JHA, published in OJ L 210 of 6.8.2008, p. 1 and 12.

Member States had to comply with the first and last categories of provisions by 26 August 2009 and with the automated searching provisions by 26 August 2011 at the latest. Member States have to fulfill a number of formal requirements, next to the technical implementation.

The current document aims to provide:

- a brief overview of the formalities to be complied with, the related documents and procedures;
- an overview of the declarations made by Member States pursuant to the relevant provisions of the Prüm Decisions;
- the state of play of implementation of the automated data exchange of DNA, fingerprint and vehicle registration data (VRD).

2. Documents and procedures

2.1 Declarations / notifications

Delegations have to provide a number of declarations and notifications to the General Secretariat of the Council.

Contact points:

- for the automated searching of DNA profiles (Article 6(1) of Council Decision 2008/615/JHA)
- for the automated searching of dactyloscopic data (Article 11(1) of Council Decision 2008/615/JHA)
- for the automated searching of VRD (Article 12(2) of Council Decision 2008/615/JHA)
- for exchange of information on major events (Article 15 of Council Decision 2008/615/JHA)
- for exchange of information to prevent terrorist offences (Article 16(3) of Council Decision 2008/615/JHA)
- of data protection authorities (Article 19 of Council Decision 2008/616/JHA)

This information should be provided to the General Secretariat of the Council by mail to prum@consilium.europa.eu. Annex 1 indicates which Member States have already provided this information.

List of national DNA analysis files

Pursuant to Article 2(3) of Council Decision 2008/615/JHA, each Member State must inform the General Secretariat of the Council of the national DNA analysis files to which Articles 2 and 6 apply and the conditions for automated searching as referred to in Article 3(1).

The information must be sent to the General Secretariat of the Council by an official letter of the Permanent Representation.

Annex 1 indicates which Member States have submitted this declaration and in which official Council documents these are issued. As they are public documents, they can be obtained from the Council website.

Maximum search capacities for dactyloscopic data

Pursuant to Article 13 of Council Decision 2008/616/JHA, each Member State must inform the General Secretariat of the Council by mail (prum@consilium.europa.eu) of the maximum search capacities per day for dactyloscopic data of identified persons and for dactyloscopic data of persons not yet identified.

Document 5860/5/10 REV 5 JAI 92 CRIMORG 16 ENFOPOL 29 compiles this information and is the basis on which Member States' experts decide on the mutually agreed capacities. As it is a public document, it can be obtained from the Council website.

Readiness to apply

According to Article 36(2) of Council Decision 2008/615/JHA, Member States shall notify to the General Secretariat of the Council and the Commission the legal implementation of the Prüm Decisions and to apply the Decision immediately in its relations with Member States which have given the same notification.

This notification must be sent to the General Secretariat of the Council by an official letter of the Permanent Representation.

Annex 1 indicates which Member States have submitted this declaration and in which official Council documents these are issued. As they are public documents, they can be obtained from the Council website.

Data protection requirements

Prior to any processing of personal data and to evaluating the implementation of chapter 2 provisions, Member States have to guarantee the level of data protection and comply with all standards and procedures required by Chapter 6 of Council Decision 2008/615/JHA.

To this end, they have to fill in the questionnaire set out in document 6661/1/09 REV 1 ADD 1 REV 1 CRIMORG 25 ENFOPOL 39 and send it to prum@consilium.europa.eu.

Annex 2 indicates which Member States have replied to the data protection questionnaire and in which official Council documents these are issued.

2.2 Implementation of the automated data exchanges

Member States should regularly report on the national state of play of the implementation (legal and technical) of the automated data exchanges.

To that end, they should update the tables set out in annex 3 regarding DNA, annex 4 regarding fingerprints and annex 5 regarding VRD by sending a mail to prum@consilium.europa.eu.

Member States shall make sure that they implement the technical specifications as set out in Council Decision 2008/616/JHA (OJ L OJ L 210 of 6.8.2008, p. 12), notably by

- ensuring that the relevant national databases are made available
- using TESTA II as the network for the data exchange
- for the VRD exchange, using a version of the Eucaris software.

Member States that are already operational should act as “supporting partners” to Member States that are not yet operational with a view to:

- organising the technical support,
- helping the respective MS to meet the technical requirements,
- carrying out the pilot run,
- providing at least one expert to lead and/or participate in evaluation visits.

The choice of a supporting partner is done on the basis of bilateral contacts. Member States requiring the contact details from relevant experts in the other Member States can consult the contact lists issued by the General Secretariat of the Council.

Advice can also be sought from the respective lead experts:

- DNA: Dr. C.P. van der Beek MBA, k.v.d.beek@nfi.minvenj.nl
- Fingerprints: it05@bka.bund.de
- VRD: dsoops@skynet.be

For VRD, in case of technical problems, IT management, etc., contact with Eucaris can be made via secretariat@eucaris.net.

2.3 Evaluation procedure

Before a Member State can start the operational automated searching of any of the categories, it should pass an evaluation procedure², the details of which are set out in document 6661/2/09 REV 2 CRIMORG 25 ENFOPOL 39³ as amended by doc. 10149/10 JAI 463 CRIMORG 103 ENFOPOL 145 ENFOCUSTOM 43.

Detailed descriptions of the evaluation procedures are set out for

- DNA data in doc. 11899/2/10 REV 2 DAPIX 8 CRIMORG 141 ENFOPOL 203 + COR1
- dactyloscopic data in doc. 11898/2/10 REV 2 DAPIX 7 CRIMORG 140 ENFOPOL 202 + COR 1
- VRD in document 6661/1/09 REV 1 ADD 5 REV 2.

In summary, the procedure consists of a questionnaire, a pilot run and an evaluation visit.

The data protection questionnaire should be filled in before any evaluation procedure starts (cf. annex 2).

² Article 20 of Council Decision 2008/616/JHA

³ This evaluation procedure applies as from 13 October 2009 to any Member State wishing to start a data exchange pursuant to the Prüm Decisions (cf. doc. 13919/1/09 REV 1 CRIMORG 136 ENFOPOL 233) without prejudice to Article 25(3) of Council Decision 2008/615/JHA. Until then, Member States implemented the Prüm exchange of DNA, dactyloscopic and VRD pursuant to the Prüm Treaty. The latest decision in this regard ("7th Decision of the Committee of Ministers") is of 9 October 2009.

The evaluation procedure is started when the Member State fills in the **questionnaire** related to the data category for which it wishes to start the implementation and sends this to the General Secretariat of the Council (prum@consilium.europa.eu).

The questionnaires are set out in the following documents:

- DNA: 6661/1/09 REV 1 ADD 2
- dactyloscopic data: 6661/09 ADD 3
- VRD: 6661/1/09 REV 1 ADD 4 REV 1

Annexes 3 to 5 will reflect which Member States have replied to which questionnaires and in which official Council documents these replies are issued.

By this time, all the relevant declarations and notifications must also have been sent (cf. point 2.1 and annex 1 of current document).

The **pilot run** and **evaluation visit** must be organised in close cooperation with the supporting Member State and the lead expert. Information thereon must be sent regularly to the General Secretariat of the Council (prum@consilium.europa.eu) with a view to updating annexes 3 to 5 to the current document so that a general planning and overview can be kept.

Once the pilot run and evaluation visit have been done, the **evaluation report** shall be submitted to the Council so that the **Council** can take a **decision** that the Member State can start the operational data exchange. This will be indicated in the annexes 3 to 5, including the reference of the relevant Council document(s).

3. Obligations for operational Member States

As soon as Member States become operational, they should participate in the work as supporting partner for non-operational Member States. In this context, they should send the name of (an) expert(s) who can participate in the evaluation visits to the General Secretariat of the Council (prum@consilium.europa.eu).

Member States shall compile statistics on the results of the automated data exchange in accordance with the agreed models for DNA (doc. 14103/1/11 REV 1 JAI 619 DAPIX 114 CRIMORG 145 ENFOPOL 300 and 14383/12 DAPIX 118 for DNA match statistics 2011), dactyloscopic data (doc. 16891/11 JAI 830 DAPIX 147 CRIMORG 202 ENFOPOL 400) and VRD (doc. 13837/10 JAI 755 DAPIX 18 CRIMORG 159 ENFOPOL 251 ENFOCUSTOM 77). Member States shall forward the statistics and further information on the administrative, technical and financial implementation (prum@consilium.europa.eu).

Declarations and notifications by Member States

MS	Art. 6(1) (DNA)	Art. 11(1) Fingerprints	Art. 12(2) VRD	Art. 15 Major events	Art. 16 CT	Art. 19/616 DPA	Art. 2(3) DNA files ST DOC	Art. 36(2) implementation ST DOC
	nep DS 1037/12	nep DS 1039/12	nep DS 1009/12	nep DS 1148/12	nep DS 1010/12	DS 1111/12		
BE	X	X	X	X	X	X	7655/12	
BG	X	X	X	X	X	X	6643/12	
CZ	X	X		X	X	X	13903/11	
DK	X	X	X	X	X	X		
DE	X	X	X	X	X	X	10271/11	10271/11
EE	X	X	X	X	X	X	8745/12	
IE	X	X	X			X		
EL	X	X		X	X			
ES	X	X	X	X	X	X	6946/10	5537/11
FR	X	X	X	X	X	X	18714/11	
IT	X	X	X	X	X			
CY	X	X	X	X	X	X	16029/11	
LV	X	X	X	X	X	X	10849/11	
LT	X	X	X	X	X	X	13246/11	
LU	X	X	X	X	X	X	13449/10	13449/10
HU	X	X	X	X	X	X	11355/12	
MT	X	X	X	X	X	X		
NL	X	X	X	X	X	X		

AT	X	X	X	X	X	X	5864/10 ADD 1	5864/10
PL	X	X	X	X	X	X	11184/12	
PT	X	X	X	X	X	X	8095/11	
RO	X	X	X	X	X	X	7043/12	
SI	X	X	X	X	X	X	8511/11	8511/11
SK	X	X	X	X	X	X	14459/10	
FI	X	X	X	X	X	X	6753/12	
SE	X	X	X	X	X	X		
UK	X	X	X	X	X	X		

Replies to the data protection questionnaire (doc. 6661/1/09 REV 1 ADD 1 REV 1)

MS	Document	date
BE	5078/12	9 January 2012
BG	9021/10	10 May 2010
CZ	8670/11	14 April 2011
DK		
DE	not applicable (cf. 2008/615/JHA, Art. 25(3))	
EE	13822/11	13 September
EL		
ES	not applicable (cf. 2008/615/JHA, Art. 25(3))	
FR	7997/11	22 March 2011
IE		
IT		
CY	7263/10	26 March 2010
LV	6406/10	17 February 2010
LT	12458/11	6 July 2011
LU	not applicable (cf. 2008/615/JHA, Art. 25(3))	
HU	11288/1/11 REV 1	8 May 2012
MT	13649/12	13 September 2012
NL	12992/11 + COR1	2 August 2011
AT	not applicable (cf. 2008/615/JHA, Art. 25(3))	
PL	6675/2/10 REV 2	24 January 2012
PT	7940/11	21 March 2011
RO	11714/10 + REV 1 + ADD 1	06 July 2010
SI	11712/1/10 REV 1	11 May 2011
SK	7549/10	31 March 2010
FI	6671/10	26 February 2010
SE	16489/11	16 November 2011
UK	<i>reply to provisional version in 2010</i>	

STATE OF PLAY: DNA -

Operational Member States are indicated in italic.

Regular updates of the table should be sent to prum@consilium.europa.eu

MS	Implementation			Evaluation						Observation
	legal	technical	supporting MS	Questionnaire	Pilot run	Visit	Evaluation report	Team ⁴	Council Decision	
BE	Corresponding Royal Decree still pending	Test runs with NL, AT and LU technically almost operational CODIS 7.0 installed		7664/1/12 REV 1				NL LU ...		Evaluation visit planned for after the Royal Decree being published
<i>BG</i>		<i>Operational with SI, AT, NL, FR</i>								<i>Prüm Treaty</i>
<i>CZ</i>		<i>CODIS 7.0 installed</i>	<i>SK</i>	<i>13795/11</i>	<i>x</i>	<i>x</i>	<i>16487/11</i>	<i>SK</i>	<i>2012/58/EU OJ L 30/12</i>	<i>Approval of Binding instructions still pending, start of data exchange foreseen for end 2012</i>
DK	Legislation passed in June 2008	Preparations ongoing CODIS 7.0 installed tests with DE, FI						DE ...		Operational end of 2012
<i>DE</i>	<i>completed in June 2009 on federal level</i>	<i>Operational with AT, SI, LU, ES, NL, FR, LV, SK, RO</i>								<i>Prüm Treaty</i>

⁴ Lead MS in bold

MS	Implementation			Evaluation						Observation
	legal	technical	supporting MS	Questionnaire	Pilot run	Visit	Evaluation report	Team ⁴	Council Decision	
EE		CODIS 7.0 installed	NL FI	5079/12	X	X	7671/12		2012/299/EU OJ L 151/31	Operational January 2013
EL	completed	CODIS 7 installed								
ES		Operational with DE, AT, LU, SI, FR, NL, SK, LV, RO / CODIS 7.0 installed								Prüm Treaty
FR		Operational with DE, ES, NL, AT, LU, SI, SK, BG, RO								Prüm Treaty
IE	Legislation underpinning the establishment of the DNA database has been drafted and is awaiting parliamentary review. Separate legislation governing data protection aspects is currently being drafted. Legislation is expected to be in place by end 2011.	Ireland does not yet have a fully operational DNA database, preparations for its introduction are being made including - <ul style="list-style-type: none"> the procurement of a new Laboratory Information Management System upgrading of data analysis software procurement and testing of instrumentation for automated sample handling and signing of letter of agreement with FBI for version 7.0 of CODIS 								Technical implementation advancing well
IT	Accomplished	Upgrade of software ongoing								Operational in 2013
CY	Legislation was adopted by Ministerial Council on 6 June 2012	Technical implementation ready in April 2011, tests successful with AT, evaluation visit successful in November 2011	AT	15036/11	X	X	17652/11	AT		Awaiting Council Decision after completion of legal implementation

MS	Implementation			Evaluation						Observation
	legal	technical	supporting MS	Questionnaire	Pilot run	Visit	Evaluation report	Team ⁴	Council Decision	
<i>LV</i>		<i>Operational with AT, NL, DE, LT, FI, SK, RO, testing with ES</i>	<i>DE</i>	<i>8066/11</i>	<i>X</i>	<i>X</i>	<i>13860/11</i>	<i>DE</i>	<i>2011/715/EU OJ L 285/24</i>	
<i>LT</i>		<i>Operational with AT, LV, FI, N., RO, testing with EE, DE</i>		<i>12995/11</i>	<i>X</i>	<i>X</i>	<i>13838/11</i>	<i>AT</i>	<i>2011/887/EU OJ L 344/36</i>	
<i>LU</i>		<i>Operational with AT, DE, ES, NL, SI, FR, SK; testing with BE</i>								<i>Prüm Treaty</i>
<i>HU</i>		<i>Operational with AT</i>	<i>AT</i>	<i>15627/11</i>	<i>X</i>	<i>X</i>	<i>11353/12</i>	<i>AT</i>	<i>2012/445/EU OJ L 202/22</i>	
<i>MT</i>	completed	<i>CODIS 7.0 installed, testing ongoing with several countries</i>		<i>13650/12</i>						
<i>NL</i>		<i>Operational with AT, DE, SI, LU, FI, FR, ES, BG, SK, RO, LT, LV;</i>								<i>Prüm Treaty</i>
<i>AT</i>		<i>Operational with DE, ES, LU, SI, NL, FR, RO, BG, FI, SK, LT, LV, HU, testing with EE, CY</i>								<i>Prüm Treaty</i>

MS	Implementation			Evaluation						Observation
	legal	technical	supporting MS	Questionnaire	Pilot run	Visit	Evaluation report	Team ⁴	Council Decision	
PL	Legislation passed Parliament on 16 September 2011	Connected to sTESTA CODIS 7.0 installed	SK	11185/12						evaluation October 2012
PT		CODIS 7.0 installed	DE	7655/11 +ADD 1	X	X	11377/11	DE	2011/472/EU OJ L 195/71	Waiting for political decision to start
RO		<i>Operational with AT, NL, SI, FR, SK, LV, LT, DE, ES; Testing with CY, EE; CODIS 7.0 installed</i>								<i>Prüm Treaty</i>
SI		<i>Operational with BG, DE, AT, NL, ES, LU, SK, FR, RO</i>								<i>Prüm Treaty</i>
SK		<i>Operational with AT, ES, NL, SI, LU, LV, DE, RO; FR, PT, CZ testing finished, 2 CODIS 7.0 installed</i>	AT	9023/10	X	X	13487/1/10	AT NL	2010/689/EU OJ L 294/14	
FI		<i>Operational with NL, AT, LV, LT ; testing with EE</i>								<i>Prüm Treaty</i>
SE	Into force 1 August 2011	Implementation summer 2011 CODIS 7.0 installed								Evaluation planned for December 2012
UK	The legislation required to address the European Court of Human Rights decision in S & Marper has been passed by Parliament. UK is currently implementing the changes required to ensure DNA retention is in line with that ECtHR ruling. Exercise needs to be completed before evaluating options in respect of Prüm.	Currently evaluating a range of options for the changes necessary to deliver the significant business and technical changes required to meet the obligations arising from the Prüm Decision. Strategic planning and mapping of the way forward is continuing.								

DNA operational data exchange																											
	BE	BG	CZ	DK	DE	EE	EL	ES	FR	IE	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	UK
BE	x																										
BG		x																									
CZ			x																								
DK				x																							
DE					x																						
EE						x																					
EL							x																				
ES								x																			
FR									x																		
IE										x																	
IT											x																
CY												x															
LV													x														
LT														x													
LU															x												
HU																x											
MT																	x										
NL																		x									
AT																			x								
PL																				x							
PT																					x						
RO																						x					
SI																							x				
SK																								x			
FI																										x	
SE																										x	
UK																											x

STATE OF PLAY: DACTYLOSCOPIC DATA -

Operational Member States are indicated in italic.

Regular updates of the table should be sent to prum@consilium.europa.eu

MS	Implementation			Evaluation						Observations
	legal	technical	supporting MS	Questionnaire	Pilot run	Visit	Evaluation report	team ⁵	Council Decision	
BE		AFIS put in place in 2010, testing with AT, CY	ES BG							
<i>BG</i>		<i>Operational with AT, DE, ES, SK, LU, SI, CZ, FR, NL, LT</i>	<i>AT</i>	<i>6944/10</i>	<i>X</i>	<i>X</i>	<i>16014/10</i>	<i>AT ES</i>	<i>2010/758/EU OJ L322/43</i>	
<i>CZ</i>		<i>Operational with BG, AT, SK; testing with other countries</i>	<i>SK AT</i>	<i>9804/11</i>	<i>X</i>	<i>X</i>	<i>12063/11</i>	<i>SK AT</i>	<i>2011/472/EU OJ L 190/72</i>	
DK	Legislation passed in June 2008	Implementation of new AFIS ongoing	AT SK							Operational before end of 2013
<i>DE</i>	<i>Completed on federal level in June 2009</i>	<i>Operational with AT, ES, LU, SI, SK, BG, FR, NL</i>								<i>Prüm Treaty</i>
EE	passed Parliament on 1 August 2012	AFIS software upgrade and hardware installation completed	AT LT	11856/12	X	X	14274/12	AT		Operational probably January 2013

⁵ Lead MS in bold

MS	Implementation			Evaluation						Observations
	legal	technical	supporting MS	Questionnaire	Pilot run	Visit	Evaluation report	team ⁵	Council Decision	
EL		Tendering procedure for new AFIS								
ES		<i>Operational with DE, AT, BG, FR; testing with BE, SK, SI, LU, CY</i>								<i>Prüm Treaty</i>
FR		<i>Operational with DE, ES, LU, AT, SK, BG; tests planned with CY, SI, CZ, LT, NL MT</i>	<i>DE ES</i>	<i>7999/11</i>	<i>X</i>	<i>X</i>	<i>9959/11</i>	<i>DE ES LU</i>	<i>2011/355/EU OJ L 161/23</i>	
IE	Legislation allowing for searching and exchange of data is in place. Separate legislation governing data protection aspects is currently being drafted. Legislation is expected to be in force by end of 2011.	AFIS system exists. Signing of contract to provide the software upgrade and ancillary works required has been delayed pending budgetary clearance.	ES LU							Operational end of 2013
IT	June 2009	Technical planning for modernisation of national system and implementation ready; contracts with the suppliers need to be finalised								
CY	Legislation was adopted by Ministerial Council on 6 June 2012	AFIS system exists Technical cooperation with AT Evaluation visit successful in November 2011	AT DE SI	15035/11	X	X	17659/11	AT DE		Awaiting Council Decision after completion of legal implementation

MS	Implementation			Evaluation						Observations
	legal	technical	supporting MS	Questionnaire	Pilot run	Visit	Evaluation report	team ⁵	Council Decision	
LV	On 21 May 21 2009, the current Law on Biometric Data Processing System (BDPS) came into force, which provides the legal base for the exchange of fingerprint data between EU MS. BDPS currently is under development and it will be a modern, centralised and unique system in Latvia, which will gather all biometric information from all national institutions responsible for collecting of such data. BDPS will provide the necessary fingerprint data for exchange under the Prüm Decision requirements.									Technical ready spring 2013
LT		<i>Operational with AT, BG, DE, SK, NL; soon testing with EE, FR, CY</i>		<i>12994/11</i>		<i>X</i>	<i>13839/11</i>	<i>AT</i>	<i>2011/888/EU OJ L 344/38</i>	
LU		<i>Operational with SI, AT, DE, FR, BG, ES; testing with NL</i>								<i>Prüm Treaty</i>
HU		<i>Testing with BG, CY</i>	<i>AT DE NL SK</i>	<i>13796/11</i>	<i>X</i>	<i>X</i>	<i>11358/12</i>	<i>AT (DE) SK</i>	<i>2012/446/EU OJ L 202/23</i>	

MS	Implementation			Evaluation						Observations
	legal	technical	supporting MS	Questionnaire	Pilot run	Visit	Evaluation report	team ⁵	Council Decision	
MT	Completed	Testing with FR, AT	AT	13651/12						
NL		<i>Operational with AT, BG, LT, DE testing with ES, LU</i>	DE	12993/11	X	X	15713/11		2012/46/EU OJ L 26/32	
AT	<i>Accomplished end of 2009</i>	<i>Operational with DE, LU, SI, ES, SK, BG, CZ, LT, FR, NL, HU</i>								<i>Prüm Treaty</i>
PL	Legislation passed Parliament on 16 September 2011	Implementation started, upgraded 4.0 system AFIS, purchase Prüm interface and NCP organization still ongoing.								Technically ready end of 2013
PT	Ongoing	Re-evaluation of the situation								
RO	Ongoing	To date, the interface ANSI/NIST-ITL 1-200 version 4.22b is not yet acquired. However, the interface is a precondition of making AFIS operational. This is supposed to take place 6 months after the acquisition of the interface which is dependent on funding not yet approved.	AT							Evaluation before end of 2012
SI		<i>Operational with AT, DE, LU, BG, SK; testing with CY, NL, CZ, FR</i>								<i>Prüm Treaty</i>
SK		<i>Operational with AT, BG, FR, DE, CZ, SI, LT testing with HU</i>	AT	9024/10	X	X	14178/1/10	AT DE	2010/682/EU, OJ L 293/58	

MS	Implementation			Evaluation						Observations
	legal	technical	supporting MS	Questionnaire	Pilot run	Visit	Evaluation report	team ⁵	Council Decision	
FI		Contract with AFIS provider to be signed in autumn, reading for testing in 2013								
SE	Into force 1 August 2011	Implementation project ongoing, procurement period finished Production spring 2013								Evaluation planned for May 2013
UK	The legislation required to address the European Court of Human Rights decision in S & Marper has been passed by Parliament. UK is currently implementing the changes required to ensure FP retention is in line with that ECtHR ruling. Exercise needs to be completed before evaluating options in respect of Prüm	Currently evaluating a range of options for the changes necessary to deliver the significant business and technical changes required to meet the obligations arising from the Prüm Decision. Strategic planning and mapping of the way forward is continuing.								

FP operational data exchange																											
	BE	BG	CZ	DK	DE	EE	EL	ES	FR	IE	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	UK
BE	x																										
BG		x																									
CZ			x																								
DK				x																							
DE					x																						
EE						x																					
EL							x																				
ES								x																			
FR									x																		
IE										x																	
IT											x																
CY												x															
LV													x														
LT														x													
LU															x												
HU																x											
MT																	x										
NL																		x									
AT																			x								
PL																				x							
PT																						x					
RO																							x				
SI																								x			
SK																									x		
FI																										x	
SE																										x	
UK																											x

STATE OF PLAY: VRD

Operational Member States are indicated in italic.

Regular updates of the table should be sent to prum@consilium.europa.eu

MS	Implementation			Evaluation						Observations
	legal	technical	supporting MS	Questionnaire	Pilot run	Visit	Evaluation report	Team	Council Decision	
<i>BE</i>		<i>Operational (incoming requests) with DE, ES, AT, LU, NL, RO, SI, FI, PL (outgoing requests) with DE, ES, AT, LU, NL, RO, SI, FI, PL</i> <i>DIW ok for incoming / outgoing, police not ok for outgoing requests</i>								<i>Prüm Treaty</i>
BG		EUCARIS – Prüm application installed		10152/12						Evaluation visit after decision on communication channel
CZ	Legislation for new central register under discussion in Parliament	Internal discussions ongoing								Evaluation 2012/2013
DK	Legislation passed in June 2008	Test environment successfully installed, by early 2013 production environment installed								Evaluation February 2013
<i>DE</i>	<i>Completed on federal level</i>	<i>Operational for incoming requests with ES, AT, LU, NL, BE, FR, PL on regional level for outgoing requests with ES, AT, LU, NL, BE, FR- for HH, BW, HE, SN, BR, NI, RP, SL, BY, SH</i>								<i>Prüm Treaty</i>
EE		Technically ready, awaiting solution of administrative problems								
EL		Internal procedures speeded up								

MS	Implementation			Evaluation						Observations
	legal	technical	supporting MS	Questionnaire	Pilot run	Visit	Evaluation report	Team	Council Decision	
ES		<i>Operational for incoming requests with FR, DE, AT, LU, NL, BE, FI, SI, RO, PL outgoing requests with FR, DE, AT, LU, NL, BE, FI, SI, RO, PL</i>							<i>Prüm Treaty</i>	
FR		<i>Operational for incoming requests with DE, ES, AT, LU, NL, BE, FI, SI, R, PL for outgoing requests with DE, ES, AT, LU, NL, BE, FI, SI, RO, PL</i>							<i>Prüm Treaty</i>	
IE	Legislative provisions for physical searching and exchange of VRD in place. Additional data protection legislation is being drafted and is expected to be in place by the end of 2012. Passing legislation by mid 2013	Technical implementation for incoming requests is complete and has been successfully tested. Installation of additional EUCARIS access points in the Garda Síochána (Irish Police) to generate outgoing requests is ongoing. Technically ready	NL							Evaluation second half of 2013
IT		EUCARIS installed, testing phase concluded; internal procedures set up;								

MS	Implementation			Evaluation						Observations
	legal	technical	supporting MS	Questionnaire	Pilot run	Visit	Evaluation report	Team	Council Decision	
CY	Discussions concluded,	Final stage of EUCARIS implementation - direct contact with EUCARIS helpdesk	NL							Questionnaire by mid October; in early November ready for evaluation
LV	Full member of the EUCARIS Treaty since July 2010.	Preparatory work ongoing.								Pending the completion of some legal issues, evaluation visit possible in November 2012
LT	Came into force on 18-11-2011			6100/12	X	X	13610/12			Evaluation in June 2012; awaiting evaluation report
LU		<i>Operational BE, DE, ES, FR, NL, AT, RO, SI, FI, PL</i>								<i>Prüm Treaty</i>
HU	Council Decisions implemented	Pilot run in preparation		13902/11						Evaluation visit planned for 2012/2013
MT	ongoing	Preparatory work ongoing. Tender Document finalised and will be issued by end April 2011.								
NL		<i>Operational for incoming requests with DE, AT, LU, FR, ES, RO, SI, F, PLI for outgoing requests with DE, AT, LU, FR, ES, BE, RO, SI, FI, PL</i>								<i>Prüm Treaty</i>
AT	<i>Accomplished end 2009 cf. 5864/10</i>	<i>Operational for incoming requests with DE, FR, ES, BE, NL, LU, RO, SI, FI, PL for outgoing requests DE, FR, ES, BE, NL, LU, RO, SI, FI, PL</i>								<i>Prüm Treaty</i>
PL		<i>Operational BE, DE, ES, FR, LU, NL, AT, RO, SI, FI.</i>	NL	7728/11 + COR 1	X	X	7270/12		2012/236/EU OJ L 118/8	
PT	Draft legislation is under evaluation.	Implementation of the new car register information system – SIRAUTO – in 2012 .								Accession to EUCARIS after implementation of SIRAUTO

MS	Implementation			Evaluation						Observations
	legal	technical	supporting MS	Questionnaire	Pilot run	Visit	Evaluation report	Team	Council Decision	
RO		<i>Operational with AT, BE, DE, ES, FI, FR, LU, NL, SI, PL.</i>		14007/10	X	X	8738/11 + ADD 1		2011/547/EU OJ L 242/8	
SI		<i>Operational with BE, ES, FR, DE, LU, NL, AT, RO, SI, FI, PL.</i>		11806/10	X	X	8740/11	NL BE	2011/387/EU OJ L 173/9	
SK		Preparations ongoing EUCARIS test within testing environment; production environment installed end of 2012.								
FI		<i>Operational with BE, ES, FR, DE, LU, NL, AT, RO, SI, FI, PL.</i>		6677/10	X	X	9032/10		2010/559/EU OJ L 245/34	
SE	Into force 1 August 2011			16490/11	X	X	11349/12			Evaluation in December 2011; waiting for Council Decision.

MS	Implementation			Evaluation						Observations
	legal	technical	supporting MS	Questionnaire	Pilot run	Visit	Evaluation report	Team	Council Decision	
UK	Secondary legislation is needed to ensure personal data can be exchanged.	Currently evaluating a range of options for the changes necessary to deliver the significant business and technical changes required to meet the obligations arising from the Prüm Decision. Strategic planning was completed in April 2010 and a business case is being prepared, which needs funding.								

VRD operational data exchange (27/10/2011)																											
	BE	BG	CZ	DK	DE	EE	EL	ES	FR	IE	IT	CY	LV	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	UK
BE	x																										
BG		x																									
CZ			x																								
DK				x																							
DE					x																						
EE						x																					
EL							x																				
ES								x																			
FR									x																		
IE										x																	
IT											x																
CY												x															
LV													x														
LT														x													
LU															x												
HU																x											
MT																	x										
NL																		x									
AT																			x								
PL																				x							
PT																					x						
RO																						x					
SI																							x				
SK																								x			
FI																									x		
SE																										x	
UK																											x

Anlage 3



**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 26 July 2012

12207/12

**Interinstitutional File:
2008/0242 (COD)**

LIMITE

**EURODAC 12
ENFOPOL 220
CODEC 1841**

OUTCOME OF PROCEEDINGS

of::	Asylum Working Party
on::	12 July 2012
No. Cion prop.:	10638/12 EURODAC 3 ENFOPOL 157 CODEC 1503
Subject:	Amended proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No [.../...] (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person) and to request comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (Recast version)

1. At its meeting of 12 July 2012, the Asylum Working Party examined the above-mentioned amended proposal, with the exception of Articles 2(k), 16(1), 25(4) and 35. Following an invitation by the Presidency, certain delegations submitted written contributions after the meeting.
2. The results of the discussions, as well as the above written contributions, are set out in the Annex to this Outcome of Proceedings, with delegations' comments in the footnotes.

ANNEX

↓ 2725/2000/EC (adapted)

⇒ new

2008/0242 (COD)

Amended proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No [.../...] (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person) and to request comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice¹ (Recast version)

¹ **DE, EE, EL, ES, FI, FR, HU, LT, LV, AT, PT, RO, SE, SK, UK** : general scrutiny reservations and **NL** parliamentary scrutiny reservation on the proposal. **BE** expressed concerns about the preventive use of the EURODAC system, which might lead to abuses, as well as in relation to other issues such as the notion of "serious crimes", the independence of the verifying authority, the access conditions of EUROPOL to EURODAC (for this issue supported by **HU**) and the data-protection effects for the asylum seekers. **Cion** pointed out that there is no concrete reference to the EURODAC in the AMF proposal. **Cion** also underlined that a MS is entitled to consider that the Prüm check has taken place and proceed to use EURODAC for law enforcement purposes, even if this MS is connected within the Prüm system with only one other MS.

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union ~~establishing the European Community~~, and in particular Article 78 point (2)(e) ~~63 point (1)(a)~~ ⇨ , Article 87 point (2)(a) and Article 88 point (2)(a) ⇐ thereof,

Having regard to the proposal from the Commission²,

Having regard to the opinion of the European Data Protection Supervisor³,

~~Having regard to the opinion of the European Parliament⁴~~

⊗ Acting in accordance with the ordinary legislative procedure, ⊗

Whereas:⁵

² COM(2012) XXX.

³ OJ L 92 10.04.2010, p. 1

⁴ ~~OJ C 189, 7.7.2000, p. 105 and p. 227 and opinion delivered on 21 September 2000 (not yet published in the Official Journal).~~

⁵ **FR, NL, SE, UK:** scrutiny reservations on all the Recitals.

↓ new

- (1) A number of substantive changes are to be made to Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention⁶ and Council Regulation (EC) No 407/2002 of 28 February 2002 laying down certain rules to implement Regulation (EC) No 2725/2000 concerning the establishment of "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention⁷. In the interest of clarity, those Regulations should be recast.

↓ 2725/2000/EC recital 1

- ~~(1) Member States have ratified the Geneva Convention of 28 July 1951, as amended by the New York Protocol of 31 January 1967, relating to the Status of Refugees.~~

↓ 2725/2000/EC recital 2 (adapted)

- ~~(2) Member States have concluded the Convention determining the State responsible for examining applications for asylum lodged in one of the Member States of the European Communities, signed in Dublin on 15 June 1990 (hereinafter referred to as "the Dublin Convention").~~

⁶ OJ L 316, 15.12.2000, p. 1.

⁷ OJ L 62, 5.3.2002, p. 1.

↓ new

- (2) A common policy on asylum, including a Common European Asylum System, is a constituent part of the European Union's objective of progressively establishing an area of freedom, security and justice open to those who, forced by circumstances, legitimately seek international protection in the Union.
- (3) The European Council of 4 November 2004 adopted The Hague Programme which sets the objectives to be implemented in the area of freedom, security and justice in the period 2005-2010. The European Pact on Immigration and Asylum endorsed by the European Council of 15-16 October 2008 called for the completion of the establishment of a Common European Asylum System by creating a single asylum procedure comprising common guarantees and a uniform status for refugees and the beneficiaries of subsidiary protection.

↓ 2725/2000/EC recital 3 (adapted)

⇒ new

- (4) For the purposes of applying ~~the Dublin Convention~~ ☒ Council Regulation (EU) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person]⁸ ☒, it is necessary to establish the identity of applicants for ~~asylum~~ ⇒ international protection ⇐ and of persons apprehended in connection with the unlawful crossing of the external borders of the Community. It is also desirable, in order effectively to apply the ~~Dublin Convention~~ ☒ Council Regulation (EU) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] ☒, and in particular points ~~(c) and (e)~~ (b) and (d) of Article ~~10(1)~~ 18(1)⁹ thereof, to allow each Member State to check whether an ~~alien~~ ☒ third country national or stateless person ☒ found illegally ~~present~~ ☒ staying ☒ on its territory has applied for ~~asylum~~ ⇒ international protection ⇐ in another Member State.

↓ 2725/2000/EC recital 4

- (5) Fingerprints constitute an important element in establishing the exact identity of such persons. It is necessary to set up a system for the comparison of their fingerprint data.

⁸ COM(2008)XXX.

⁹ SK pointed out that reference should rather be made to Art. 16(2)(b) and (d).

↓ 2725/2000/EC recital 5

⇒ new

- (6) To this end, it is necessary to set up a system known as "~~Eurodac~~EURODAC", consisting of a Central ~~Unit~~ ⇒ System ⇐, ~~to be established within the Commission and~~ which will operate a computerised central database of fingerprint data, as well as of the electronic means of transmission between the Member States and the ~~central database~~ ⇒ Central System, hereinafter the "Communication Infrastructure". ⇐

↓ new

- (7) The Hague Programme called for the improvement of access to existing data filing systems in the European Union. In addition, The Stockholm Programme called for well targeted data collection and a development of information exchange and its tools that is driven by law enforcement needs.
- (8) It is essential in the fight against terrorist offences and other serious criminal offences for the law enforcement authorities to have the fullest and most up-to-date information if they are to perform their tasks. The information contained in EURODAC is necessary for the purposes of the prevention, detection and investigation of terrorist offences and other serious criminal offences. Therefore, the data in EURODAC should be available, subject to the conditions set out in this Regulation, for comparison by the designated authorities of Member States and Europol.

- (9) The Commission outlined in its Communication to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European data bases in the area of Justice and Home Affairs¹⁰ of 24 November 2005 that authorities responsible for internal security could have access to EURODAC in well defined cases, when there would be a substantiated suspicion that the perpetrator of a terrorist or other serious criminal offence has applied for asylum. In this Communication the Commission also found that the proportionality principle requires that EURODAC be queried for these purposes only once there is an overriding public security concern, that is, if the act committed by the criminal or terrorist to be identified is so reprehensible that it justifies querying a database that registers persons with a clean criminal record and it concluded that the threshold for authorities responsible for internal security to query EURODAC must therefore always be significantly higher than the threshold for querying criminal databases.
- (10) Moreover, Europol has a key role with respect to cooperation between Member States' authorities in the field of cross-border crime investigation in supporting Union-wide crime prevention, analyses and investigation. Consequently, Europol should also have access to EURODAC data within the framework of its tasks and in accordance with the Decision establishing the European Police Office (Europol) No (2009/371/JHA).¹¹

¹⁰ COM(2005) 597, 24.11.2005.

¹¹ OJ L 121, 15.5.2009, p. 37

- (11) Since EURODAC has been established to facilitate the application of Council Regulation (EU) No [...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], access to EURODAC for the purposes of preventing, detecting or investigating terrorist offences and other serious criminal offences constitutes a change of the original purpose of EURODAC, which interferes with the right to respect the private life of individuals whose personal data are processed in EURODAC. Any such interference must be in accordance with the law, which must be formulated with sufficient precision to allow individuals to adjust their conduct and it must protect individuals against arbitrariness and indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise. Any interference must be necessary in a democratic society to attain a legitimate and proportionate interest and proportionate to the legitimate objective it aims to achieve.
- (12) Even though the original purpose for the establishment of EURODAC did not require the facility of requesting comparisons of data with the database on the basis of a latent which is the dactyloscopic trace which may be found at a crime scene, such a facility is a fundamental one in the field of police cooperation. The possibility to compare a latent with the fingerprint data which is stored in EURODAC will provide the designated authorities of the Member States with a very valuable tool in preventing, detecting and investigating terrorist offences and other serious criminal offences, when for example the only evidence available at a crime scene are latents.

- (13) This Regulation also lays down the conditions under which requests for comparison of fingerprint data with EURODAC data for the purposes of preventing, detecting or investigating terrorist offences and other serious criminal offences should be allowed and the necessary safeguards to ensure the protection of the fundamental right to respect for the private life of individuals whose personal data are processed in EURODAC.
- (14) In view of ensuring equal treatment for all applicants and beneficiaries of international protection, as well as in order to ensure consistency with current Union asylum *acquis*, in particular with Council Directive 2004/83/EC of 29 April 2004 on minimum standards for the qualification and status of third country nationals or stateless persons as refugees or as persons who otherwise need international protection and the content of the protection granted¹² and Regulation (EU) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], it is appropriate to extend the scope of this Regulation to order to include applicants for subsidiary protection and persons enjoying subsidiary protection.

¹² OJ L 304, 30.9.2004, p. 12. **SK:** This reference to the Qualifications Directive shall be updated as to cite amended Directive 2011/95/EU.

↓ 2725/2000/EC recital 6 (adapted)

⇒ new

- (15) It is also necessary to require the Member States promptly to take ⇒ and transmit ⇐ fingerprints ⇒ data ⇐ of every applicant for ~~asylum~~ ⇒ international protection ⇐ and of every ~~alien~~ ⊗ third country national or stateless person ⊗ who is apprehended in connection with the irregular crossing of an external border of a Member State, if they are at least 14 years of age.

↓ 2725/2000/EC recital 7 (adapted)

⇒ new

- (16) It is necessary to lay down precise rules on the transmission of such fingerprint data to the Central ~~Unit~~ ⇒ System ⇐, the recording of such fingerprint data and other relevant data in the Central ~~Unit~~ ⇒ System ⇐, their storage, their comparison with other fingerprint data, the transmission of the results of such comparison and the ~~blocking~~ ⇒ marking ⇐ and erasure of the recorded data. Such rules may be different for, and should be specifically adapted to, the situation of different categories of ~~aliens~~ ⊗ third country nationals or stateless persons ⊗.

↓ new

- (17) Hits obtained from EURODAC should be verified by a fingerprint expert in order to ensure the accurate determination of responsibility under Regulation (EU) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person].

↓ 2725/2000/EC recital 8 (adapted)

⇒ new

- (18) ~~Aliens~~ ⊗ Third country nationals or stateless persons ⊗ who have requested ~~asylum~~ ⇒ international protection ⇐ in one Member State may have the option of requesting ~~asylum~~ ⇒ international protection ⇐ in another Member State for many years to come. Therefore, the maximum period during which fingerprint data should be kept by the Central ~~Unit~~ ⇒ System ⇐ should be of considerable length. Given that most ~~aliens~~ ⊗ third country nationals or stateless persons ⊗ who have stayed in the ~~Community~~ ⊗ European Union ⊗ for several years will have obtained a settled status or even citizenship of a Member State after that period, a period of ten years should be considered a reasonable period for the conservation of fingerprint data.

↓ 2725/2000/EC recital 9 (adapted)

- (19) The conservation period should be shorter in certain special situations where there is no need to keep fingerprint data for that length of time. Fingerprint data should be erased immediately once ~~aliens~~ third country nationals or stateless persons obtain citizenship of a Member State.

↓ new

- (20) It is appropriate to store data relating to those data subjects whose fingerprints were initially recorded in EURODAC upon lodging their applications for international protection and who have been granted international protection in a Member State in order to allow data recorded upon lodging an application for international protection to be compared against them.

(21) The European Agency for the operational management of large-scale information systems in the area of freedom security and justice established by Regulation (EU) n° 1077/2011 of the European Parliament and of the Council of 25 October 2011¹³ (the "Agency") has been entrusted with the Commission's tasks relating to the operational management of EURODAC in accordance with this Regulation and with certain tasks relating to the communication infrastructure as from the date on which the Agency takes up its responsibilities as of 1 December 2012. The Agency should take up the tasks entrusted to it under this Regulation and the relevant provisions of Regulation (EU) No 1077/2011 should be amended accordingly. In addition, Europol should have observer status at the meetings of the Management Board of the Agency, when a question in relation to the application of this Regulation concerning access for consultation of Eurodac by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences is on the agenda. Europol should be able to appoint a representative to the Eurodac Advisory Group of the Agency.

(22) The Staff Regulations of Officials of the European Union (Staff Regulations of Officials) and the Conditions of Employment of Other Servants of the European Union (Conditions of Employment), laid down in Regulation (EEC, Euratom, ECSC) No 259/68 (15) (together referred to as the 'Staff Regulations'), should apply to all staff working in the Agency on matters pertaining to this Regulation.

¹³ OJ L 286, 1.11.2011, p. 1.

↓ 2725/2000/EC recital 10 (adapted)

⇒ new

- (23) It is necessary to lay down clearly the respective responsibilities of the Commission ⇒ and the Agency ⇐, in respect of the Central-Unit ⇐ System ⇐ ⇐ and the Communication Infrastructure ⇐, and of the Member States, as regards data ~~use~~ processing, data security, access to, and correction of, recorded data.

↓ new

- (24) It is necessary to designate the competent Member States' authorities as well as the National Central Access Point through which the requests for comparison with EURODAC data are done and to keep a list of the operating units within the designated authorities that are authorised to request such comparison for the specific purposes of the prevention, detection and investigation of terrorist offences as referred to in the Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism¹⁴ and of other serious criminal offences as referred to in the Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States¹⁵.

¹⁴ OJ L 164, 22.6.2002, p. 3.

¹⁵ OJ L 190, 18.7.2002, p. 1.

(25) Requests for comparison with data stored in the EURODAC central database shall be made by the operating units within the designated authorities to the National Access Point, through the verifying authority and shall be reasoned. The operating units within the designated authorities that are authorised to request comparisons with EURODAC data shall not act as a verifying authority. The verifying authorities should be responsible for ensuring strict compliance with the conditions for access as established in this Regulation. The verifying authorities should then forward the request for comparison through the National Access Point to the EURODAC Central System following verification of whether all conditions for access are fulfilled. In the exceptional case of urgency where early access is necessary to respond to a specific and actual threat related to terrorist offences or serious crime, the verifying authority should process the request immediately and only do the verification afterwards. ¹⁶

¹⁶ **AT** reservation on this Recital, which it considers be without added value; **AT** pointed out that the verification authorities carry out in practice the tasks given to the operating units.

(26) For the purposes of protection of personal data, and to exclude systematic comparisons which should be forbidden, the processing of EURODAC data should only take place on a case-by-case basis and when it is necessary for the purposes of preventing, detecting and investigating terrorist offences and other serious criminal offences. In addition access should only be allowed when comparisons with the national databases of the Member State and with the Automated Fingerprint Databases of other Member States under the Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime¹⁷ have returned negative results. This condition requires prior implementation of the Council Decision as it shall not be permitted to conduct a EURODAC check for law enforcement purposes where these above steps have not been first undertaken.¹⁸ A specific case exists in particular when the request for comparison is connected to a specific and concrete situation or to a specific and concrete danger associated with a terrorist or other serious criminal offence, or to specific persons in respect of whom there are serious grounds for believing that the persons will commit or have committed terrorist offences or other serious criminal offences. A specific case also exists when the request for comparison is connected to a person who is a victim of a terrorist or other serious criminal offence. The designated authorities and Europol should thus only request a comparison with EURODAC when they have reasonable grounds to believe that such a comparison will provide information that will substantially assist them in preventing, detecting or investigating a terrorist or other serious criminal offence.¹⁹

¹⁷ OJ L 210, 6.8.2008, p. 1.

¹⁸ EL questioned the added value of the last part of this Recital (starting from "A specific case" until the end of it).

¹⁹ LU: scrutiny reservation on this Recital.

(27) In case the requesting Member State establishes that EURODAC data pertains to a minor, these data may only be used for law enforcement purposes by the requesting Member State in accordance with that State's laws for minors and in accordance with the obligation to give primary consideration to the child's best interest.

↓ 2725/2000/EC recital 11

(28) While the non-contractual liability of the Community in connection with the operation of the ~~Eurodac~~EURODAC system will be governed by the relevant provisions of the Treaty, it is necessary to lay down specific rules for the non-contractual liability of the Member States in connection with the operation of the system.

↓ 2725/2000/EC recital 12

(29) In accordance with the principle of subsidiarity as set out in Article 5 of the Treaty, the objective of the proposed measures, namely the creation ~~within the Commission~~ of a system for the comparison of fingerprint data to assist the implementation of the Community's asylum policy, cannot, by its very nature, be sufficiently achieved by the Member States and can therefore be better achieved by the Community. In accordance with the principle of proportionality as set out in the said Article, this Regulation does not go beyond what is necessary to achieve ~~that~~ those objectives.

↓ 2725/2000/EC recital 15 (adapted)

⇒ new

- (30) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data²⁰ applies to the processing of personal data by the Member States ~~carried out in application of this Regulation within the framework of the Eurodac system~~ ⇒ unless such processing takes place by Member States' designated authorities for the purposes of the prevention, detection and investigation of terrorist offences and other serious criminal offences ⇐.
-

↓ new

- (31) Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters²¹ applies to all²² processing of personal data by Member States' designated authorities for the purposes of the prevention, detection and investigation of terrorist offences and other serious criminal offences pursuant to this Regulation.

²⁰ OJ L 281, 23.11.1995, p. 31.

²¹ OJ L 350, 30.12.2008, p. 60.

²² **DE:** clarification is needed on whether Framework Decision 2008/977/JHA governs domestic data processing, along with the exchange of personal data between competent authorities in the MS (cooperation). **DE** also pointed out that, although the subject-matter of this proposal should be limited, the fact that the scope of the above Decision is not limited to terrorist offences and other serious criminal offences should be reflected in this Recital. **Cion** considers these suggestions reasonable.

↓ 2725/2000/EC recital 16

~~(16) By virtue of Article 286 of the Treaty, Directive 95/46/EC also applies to Community institutions and bodies. Since the Central Unit will be established within the Commission, that Directive will apply to the processing of personal data by that Unit.~~

↓ 2725/2000/EC recital 17

(32) The principles set out in Directive 95/46/EC regarding the protection of the rights and freedoms of individuals, notably their right to privacy, with regard to the processing of personal data should be supplemented or clarified, in particular as far as certain sectors are concerned.

↓ new

(33) Transfers of data obtained pursuant to this Decision to third countries or international organisations or private entities should be prohibited, in order to ensure the right to asylum and to safeguard applicants for international protection from having their data disclosed to any third country. This prohibition shall be without prejudice to the right of Member States to transfer such data to third countries to which Regulation (EU) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] applies, in order to ensure that Member States have the possibility of cooperating with such third countries for the purposes of this Regulation.

- (34) National competent authorities for the supervision of the processing of personal data should monitor the lawfulness of the processing of personal data by the Member States, and the supervisory authority set up by the Europol Decision should monitor the lawfulness of data processing activities performed by Europol.²³
- (35) Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data²⁴ and in particular Articles 21 and 22 thereof concerning confidentiality and security of processing apply to the processing of personal data by Union institutions, bodies, offices and agencies carried out in application of this Regulation. However, certain points should be clarified in respect of the responsibility for the processing of data and of the supervision of data protection.
- (36) It is appropriate that national supervisory authorities monitor the lawfulness of the processing of personal data by the Member States, whilst the European Data Protection Supervisor, as referred to in Article 41 of Regulation (EC) No 45/2001, should monitor the activities of the Union institutions, bodies, offices and agencies in relation to the processing of personal data carried out in application of this Regulation.

²³ **DE:** Recitals 34 and 36 should refer to the provisions on national supervisory authorities under Art. 28 Dir. 95/46/EC and Art. 25 Framework Decision 2008/977/JHA and their wording should be revised for consistency purposes. **Cion** referred to its comments with regard to Art. 33(5).

²⁴ OJ L 8, 12.1.2001, p. 1.

↓ 2725/2000/EC recital 18

⇒ new

- (37) It is appropriate to monitor and evaluate the performance of ~~Eurodac~~EURODAC ⇒ at regular intervals ⇐.
-

↓ 2725/2000/EC recital 19 (adapted)

⇒ new

- (38) Member States should provide for a system of ~~effective, proportionate and dissuasive~~ penalties to sanction the ~~processing use~~ of data ~~entered~~ in the ~~central database~~ ⇒ Central System ⇐ contrary to the purpose of ~~Eurodac~~EURODAC.
-

↓ new

- (39) It is necessary that Member States are informed of the status of particular asylum procedures, with a view to facilitating the adequate application of Regulation (EU) No [...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person].
- (40) This Regulation respects and has to be applied in accordance with fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union. In particular, this Regulation fully respects the individual's right to protection of his or her personal data and the right to asylum.

(41) In accordance with Articles 1 and 2 of the Protocol on the position of Denmark annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application. As regards Denmark, this Regulation, with the exception of the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43, constitutes amendment to the EURODAC Regulation within the meaning of the Agreement between the European Community and the Kingdom of Denmark on the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in Denmark or any other Member State of the European Union and 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention²⁵. Consequently, in accordance with Article 3 thereof, Denmark is to notify the Commission whether it will implement the contents of this Regulation and when it does so, this Regulation creates mutual obligations under international law between Denmark and the European Union. Once this Recast Regulation is adopted and subject to a Commission recommendation for a Council Decision authorising the opening of negotiations, Denmark will be consulted as to whether it wishes to enter into negotiations on complementary agreements also covering the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43.

(42) In accordance with Article 3 of the Protocol on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, and without prejudice to Article 4 of that Protocol, the United Kingdom *[is not taking part in the adoption of this Regulation and is not bound by it or subject to its application / has notified its wish to take part in the adoption and application of this Regulation]*.

²⁵ OJ L 66, 8.3.2006, p. 38.

- (43) In accordance with Article 3 of the Protocol on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, and without prejudice to Article 4 of that Protocol, Ireland *[is not taking part in the adoption of this Regulation and is not bound by it or subject to its application / has notified its wish to take part in the adoption and application of this Regulation]*.
- (44) As regards the Republic of Iceland and the Kingdom of Norway, this Regulation, with the exception of the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43, constitutes a new measure related to EURODAC within the meaning of the Agreement between the European Community and the Republic of Iceland and the Kingdom of Norway concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Iceland or Norway²⁶. Consequently, subject to their decision to implement it in their internal legal order, this Regulation shall be applied between the Republic of Iceland and the Kingdom of Norway in their mutual relations and in their relations with the Member States of the European Union. Once this Recast Regulation is adopted and subject to a Commission recommendation for a Council Decision authorising the opening of negotiations, the Republic of Iceland and the Kingdom of Norway will be consulted as to whether they wish to enter into negotiations on complementary agreements also covering the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43.

²⁶ OJ L 93, 3.4.2001, p. 40.

(45) As regards the Swiss Confederation, this Regulation, with the exception of the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43, constitutes a new measure related to EURODAC within the meaning of the Agreement between the European Community and the Swiss Confederation concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Switzerland²⁷. Consequently, subject to its decision to implement it in its internal legal order, this Regulation shall be applied between the Swiss Confederation and the Member States of the European Union. Once this Recast Regulation is adopted and subject to a Commission recommendation for a Council Decision authorising the opening of negotiations, the Swiss Confederation will be consulted as to whether it wishes to enter into negotiations on complementary agreements also covering the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43, subject to a separate agreement on the application of relevant provisions of Council Decision 2008/615/JHA on the stepping up of cross-border cooperation.

²⁷ OJ L 53, 27.2.2008, p. 5

(46) As regards the Principality of Liechtenstein, this Regulation, with the exception of the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43, constitutes a new measure related to EURODAC within the meaning of the Protocol between the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Community and the Swiss Confederation concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Switzerland²⁸. Consequently, subject to its decision to implement it in its internal legal order, this Regulation shall be applied between the Principality of Liechtenstein, the Swiss Confederation and the Member States of the European Union. Once this Recast Regulation is adopted and subject to a Commission recommendation for a Council Decision authorising the opening of negotiations, the Principality of Liechtenstein will be consulted as to whether it wishes to enter into negotiations on complementary agreements also covering the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43, subject to a separate agreement on their application of relevant provisions of Council Decision 2008/615/JHA on the stepping up of cross-border cooperation.

↓ 2725/2000/EC recital 22 (adapted)

(47) It is appropriate to restrict the territorial scope of this Regulation so as to align it on the territorial scope of ~~the Dublin Convention~~ Regulation (EU) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] .

²⁸ OJ L 160, 18.6.2011, p. 39.

HAVE ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS

Article 1

Purpose of "~~Eurodac~~EURODAC"²⁹

1. A system known as "~~Eurodac~~EURODAC" is hereby established, the purpose of which shall be to assist in determining which Member State is to be responsible pursuant to ~~the Dublin Convention~~ Regulation (EU) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] for examining an application for ~~asylum~~ international protection lodged in a Member State by a third country national or a stateless person , and otherwise to facilitate the application of the Dublin ~~Convention~~ Regulation under the conditions set out in this Regulation.

²⁹ **NL**, supported by **BG, SI, UK**, suggested contemplating the possibility of providing for access to the EURODAC data in order to identify victims of natural disasters, etc (limited extension of the scope of the proposal), if there are no other means to do so. **Cion** recalled that victims of trafficking in human beings are covered by the scope of the proposal; however, victims of natural disasters, accidents, etc. are outside, also because the legal basis of the draft Regulation does not cover them. **NL** suggested, alternatively, putting this wording in a Recital.

~~2. Eurodac shall consist of:~~

~~(a) the Central Unit referred to in Article 3;~~

~~(b) a computerised central database in which the data referred to in Article 5(1), Article 8(2) and Article 11(2) are processed for the purpose of comparing the fingerprint data of applicants for asylum and of the categories of aliens referred to in Article 8(1) and Article 11(1);~~

~~(c) means of data transmission between the Member States and the central database.~~

2. This Regulation also lays down the conditions under which Member States' designated authorities and the European Police Office (Europol) may request the comparison of fingerprint data with those stored in the EURODAC central database for the purposes of the prevention, detection and investigation of terrorist offences and other serious criminal offences.³⁰

³⁰ **DE:** queried about which activities are covered by the word “detection” and whether “prevention” means averting a danger and “investigation” means law enforcement. It pointed out that such events and the authorities entitled to have access should be clearly identified. In the same context, **BE** pointed out that the term "prevention" may not be comprehensive enough, as it does not cover the administrative investigation and suggested replacing it by drawing on Arts 2(b) "criminal investigation" and (c) "criminal intelligence operation" of the Framework Decision 200-/960/JHA. **Cion:** these terms are standard language in the relevant acquis. **AT** suggested expanding the scope of the proposal in order to cover all crimes and entered a reservation on all the relevant provisions, i.e. Recitals 24 and 30, as well as Arts 1(2), 2(4) and 40(8). **Cion** could not agree with such expansions of the proposal's scope, also for the disproportionate additional cost it would entail.

↓ 2725/2000/EC (adapted)

⇒ new

3. Without prejudice to the processing use of data intended for ~~Eurodac~~ EURODAC by the Member State of origin in databases set up under the latter's national law, fingerprint data and other personal data may be processed in ~~Eurodac~~ EURODAC only for the purposes set out in ⇒ this Regulation and ⇐ Article ~~15(1)~~ 32(1) of the Dublin ~~Convention~~ ⊗ Regulation ⊗ .
-

↓ 2725/2000/EC (adapted)

⇒ new

Article 2

Definitions

1. For the purposes of this Regulation:
- (a) "the Dublin ~~Convention~~ ⊗ Regulation ⊗ " means the ~~Convention determining the State responsible for examining applications for asylum lodged in one of the Member States of the European Communities, signed at Dublin on 15 June 1990~~ ⊗ Regulation (EU) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] ⊗;

- (b) an "applicant for ~~asylum~~ ⇒ international protection ⇐" means an ~~alien~~ ⇔ third-country national or a stateless person ⇔ who has made an application for ~~asylum or on whose behalf such an application has been made~~ ⇒ international protection as defined in Article 2(g) of Council Directive 2004/83/EC³¹ in respect of which a final decision has not yet been taken ⇐;
- (c)³² "Member State of origin" means:
- (i) in relation to an ~~applicant for asylum~~ ⇔ person covered by Article 6 ⇔, the Member State which transmits the personal data to the Central ~~Unit~~ ⇒ System ⇐ and receives the results of the comparison;
 - (ii) in relation to a person covered by Article ~~8~~ 11, the Member State which transmits the personal data to the Central ~~Unit~~ ⇒ System ⇐;
 - (iii) in relation to a person covered by Article ~~11~~ 14, the Member State which transmits such data to the Central ~~Unit~~ ⇒ System ⇐ and receives the results of the comparison;

³¹ **DE:** This reference to the Qualification Directive shall be updated as to cite amended Directive 2011/95/EU. **Cion:** the former Directive is cited due to the variable geometry issues. **HU** suggested reverting to the 2009 proposal for a Council Decision on requesting comparisons with EURODAC data by MS law enforcement authorities, in particular with regard to data protection objectives linked with the law enforcement authorities.

³² **FI, LT:** cross-references in points (i)-(iii) should be updated as to cite Arts. 9, 14 and 17 respectively.

↓ 2725/2000/EC (adapted)

⇒ new

- (d) "refugee" ⇒ "person granted international protection" ⇐ means a ☒ third country national or a stateless ☒ person who has been recognised as a refugee in accordance with the Geneva Convention on Refugees of 28 July 1951, as amended by the New York Protocol of 31 January 1967 ⇒ entitled to international protection as defined in point (a) of Article 2 of Council Directive 2004/83/EC ⇐;
- (e)³³ "hit" shall mean the existence of a match or matches established by the Central Unit ⇒ System ⇐ by comparison between fingerprint data recorded in the databank ☒ central database ☒ and those transmitted by a Member State with regard to a person, without prejudice to the requirement that Member States shall immediately check the results of the comparison pursuant to Article ~~4(6)~~ 18(4);

↓ new

- (f) "National Acces Point" means the designated national system which communicates with the Central System;
- (g) "Agency" means the Agency established by Regulation (EU) No 1077/2011;

³³ **FI:** cross reference should be made to Art. 25(4).

- (h) 'Europol' means the European Police Office as established by Decision 2009/371/JHA;
- (i) 'EURODAC data' means all fingerprint data stored in the central database in accordance with Article 11 and Article 16(2);³⁴
- (j) 'terrorist offences' means the offences under national law which correspond or are equivalent to the offences referred to in Articles 1 to 4 of Framework Decision 2002/475/JHA;
- (k) 'serious criminal offences' means the forms of crime which correspond or are equivalent to those referred to in Article 2(2) of Framework Decision 2002/584/JHA if they are punishable by a custodial sentence or a detention order for a maximum period of at least three years under national law;³⁵
- (l) 'fingerprint data' means the data relating to fingerprints of all or at least the index fingers, and if those are missing, the prints of all other fingers of a person, or a latent.³⁶

³⁴ **FI:** cross reference should be made to Arts 11 and 14(2).

³⁵ **AT:** reservation and **SI:** scrutiny reservation on this definition; **AT** suggested including reference to Art. 2(1) of Framework Decision 2002/584/JHA; **SI** suggested including in the scope of the provision criminal offences committed in the context of illegal immigration cases.

³⁶ **SE:** suggesting a more flexible approach in fingerprint taking, including in the scope of the provision the deep-scan and flat fingerprints. **Cion:** it is intended to maintain the fingerprint form in the draft Regulation and in its Annex I. **Cion** further pointed out that flat fingerprints might not be recognisable by the EURODAC system, which identifies roll-up fingerprints. Certain IT modifications need to be done in order to take into account latent fingerprints from a crime scene; all these issues may be reconsidered in future evaluations of the EURODAC system.

↓ 2725/2000/EC (adapted)

⇒ new

2. The terms defined in Article 2 of Directive 95/46/EC shall have the same meaning in this Regulation ⇒ unless the processing of personal data takes place by Member States' designated authorities for the purposes of the prevention, detection and investigation of terrorist offences and other serious criminal offences ⇐.

3. Unless stated otherwise, the terms defined in Article ~~1~~ 2 of the Dublin ~~Convention~~ Regulation shall have the same meaning in this Regulation.

↓ new

4. The terms defined in Article 2 of the Framework Decision 2008/977/JHA shall have the same meaning in this Regulation in so far as personal data are processed by Member States' designated authorities for the purposes of the prevention, detection and investigation of terrorist offences and other serious criminal offences pursuant to this Regulation.

↓ 2725/2000/EC (adapted)

Article 3

~~Central Unit~~ ☒ **System architecture and basic principles** ☒

~~1. A Central Unit shall be established within the Commission which shall be responsible for operating the central database referred to in Article 1(2)(b) on behalf of the Member States. The Central Unit shall be equipped with a computerised fingerprint recognition system.~~

↓ new

1. EURODAC shall consist of:

(a) a computerised central fingerprint database (Central System) composed of

– a Central Unit,

– a Business Continuity System.

(b) a communication infrastructure between the Central System and Member States that provides an encrypted virtual network dedicated to EURODAC data (Communication Infrastructure).

2. Each Member State shall have a single National Access Point.

↓ 2725/2000/EC (adapted)

⇒ new

2.3. Data on ~~applicants for asylum~~, persons covered by Articles ~~8~~ and persons covered by ~~Article 11~~ 9, 14 and 17 which are processed in the Central ~~Unit~~ ⇒ System ⇐ shall be processed on behalf of the Member State of origin under the conditions set out in this Regulation ☒ and separated by appropriate technical means ☒.

↓ 2725/2000/EC Article 1(2) third subparagraph

⇒ new

4. The rules governing ~~Eurodac~~ EURODAC shall also apply to operations effected by the Member States as from the transmission of data to the Central ~~Unit~~ ⇒ System ⇐ until use is made of the results of the comparison.

↓ 2725/2000/EC Article 4(1) second sentence

⇒ new

5. The procedure for taking fingerprints shall be determined ⇒ and applied ⇐ in accordance with the national practice of the Member State concerned and in accordance with the safeguards laid down in ⇒ the Charter of Fundamental Rights of the European Union, in the Convention for the Protection of Human Rights and Fundamental Freedoms and ⇐ ~~the European Convention on Human Rights and~~ in the United Nations Convention on the Rights of the Child.
-

↓ new

Article 4

Operational management

1. The Agency, shall be responsible for the operational management of EURODAC. The Agency shall ensure, in cooperation with the Member States, that at all times the best available technology, subject to a cost-benefit analysis, is used for the Central System.
2. The Agency shall also be responsible for the following tasks relating to the Communication Infrastructure:
 - (a) supervision;
 - (b) security;

(c) the coordination of relations between the Member States and the provider.

3. The Commission shall be responsible for all other tasks relating to the Communication Infrastructure, in particular:

(a) tasks relating to implementation of the budget;

(b) acquisition and renewal;

(c) contractual matters.

4. Before the Agency takes up its responsibilities, the Commission shall be responsible for all tasks attributed to the Agency by this Regulation.

5. Operational management of EURODAC shall consist of all the tasks necessary to keep EURODAC functioning 24 hours a day, 7 days a week in accordance with this Regulation, in particular the maintenance work and technical developments necessary to ensure that the system functions at a satisfactory level of operational quality, in particular as regards the time required for interrogation of the Central System.

6. Without prejudice to Article 17 of Regulation No 31 (EEC), 11 (EAEC)³⁷, the Agency shall apply appropriate rules of professional secrecy or other equivalent duties of confidentiality to all its staff required to work with EURODAC data. This obligation shall also apply after such staff leave office or employment or after the termination of their activities.

³⁷ OJ 45, 14.6.1962, p. 1385.

Article 5

Designated Authorities for the purpose of law enforcement access³⁸

1. Member States shall designate the authorities which are authorised to access EURODAC data pursuant to this Regulation. Designated authorities shall be authorities of the Member States which are responsible³⁹ for the prevention, detection or investigation of terrorist offences and other serious criminal offences.⁴⁰

³⁸ **ES:** scrutiny reservation on the provision.

³⁹ **IT:** scrutiny reservation on the provision, suggested replacing "responsible" with the broader concept of "competent". **Cion** pointed out that the authority shall not be merely competent but specifically designated to request data from the EURODAC data base.

⁴⁰ **DE:** the following sentence, which was included in Art. 3(1) of the 2009 proposal for a Council Decision on requesting comparisons with EURODAC data by MS law enforcement authorities - and was agreed during those negotiations among delegations, should be added in this provision: "Designated authorities shall not include agencies or units dealing especially with national security issues". **NL, Cion** could agree with this suggestion. **BG, EE, EL, ES, FR, IE, IT AT, RO, SE, SI UK** scrutiny reservations on it, having concerns mainly about the exclusion of national security services. **IT, RO** pointed out that MS should be entitled to appoint the designated authorities of their choice; **SI:** such a suggestion would have additional administrative burden. **DE** stressed that intelligence service should not be given access to EURODAC expressly, although acknowledging that in certain national administrations intelligence services are also responsible for threat prevention.. **CZ** pointed out that the wording of the provision should be "... prevention, **or** detection, or investigation, ..." in order to make clear that all the competent units involved should be entitled to have access. In reply to **CZ** and **FR, Cion** pointed out that the designated authorities would not have to be the same person/entity responsible for all the tasks described in this provision and agreed to clarify it; it would be acceptable to have within the same authority entities with clearly separated functions. **Cion** also confirmed that a designated authority and a verifying authority should not be part of the same Unit, but could both belong to the same broader authority. **SE** queried whether it would be acceptable to continue having the Migration Authority as a contact point for the Central System and pointed out that in order to make clear the objective of this provision, either a definition of designated authorities should be added or alternatively, the following wording should be added in para. 1: "**Without prejudice to Art. 27(2),** Member States ... data, **for the purpose of law enforcement ...**". **Cion** welcomed this suggestion for clarification and pointed out that the designated authorities can request comparison with the EURODAC data only for law enforcement purposes.

2. Every Member State shall keep a list of the designated authorities.
3. At national level, each Member State shall keep a list of the operating units within the designated authorities that are authorised to request comparisons with EURODAC data through the National Access Point.

Article 6

Verifying Authorities⁴¹

1. Each Member State shall designate a single national body to act as its verifying authority. The verifying authority shall be an authority of the Member State which is responsible for the prevention, detection or investigation of terrorist offences and other serious criminal offences.⁴²

⁴¹ **FR:** scrutiny reservation on the Article, in particular on the concept of verifying authority. **CZ, AT,** suggested deleting Art. 6 and relevant provisions in Art. 19, as it is against the verifying authority concept, which could create a disproportionate administrative burden. If this provision is kept, it should be titled "police - format authorities". In this context, **AT** suggested referring to the national contact points' prompt exchange of data. **EL:** District Attorneys could oversee the verification in order to ensure the independence of the verifying authorities. In the same context, **BE** points out that the verifying authority should be a distinct, judicial one (or with guarantees for a similar independence), and suggested to draw on the PNR relevant provisions. **Cion** would not oppose such suggestion, although it might cause operational problems.

⁴² **DE:** the following sentence, included in Art. 4(1) of the 2009 proposal for a Council Decision on requesting comparisons with EURODAC data by MS law enforcement authorities and agreed then among delegations, should be added in this provision: "Verifying authorities shall not include agencies or units dealing especially with national security issues". **SE:** in order to make clear the objective of this provision, either a definition of verifying authorities should be added, or alternatively, the following wording should be added in para. 1: "Each MS shall **for the purpose of law enforcement access...**". **Cion** welcomed this suggestion (see the relevant comment under Art. 5). **LT:** due to the likely in most MS common administrative structure of law enforcement authorities, it considers that verifying authorities should be viewed as a unit, rather than "body" or "institution" (see also relevant commentary under Art. 5).

2. The verifying authority shall ensure that the conditions for requesting comparisons of fingerprints with EURODAC data are fulfilled.

Only the verifying authority shall be authorised to forward requests for comparison of fingerprints to the National Access Point which communicates with the Central System.

Article 7

Europol⁴³

1. Europol shall designate a specialised unit with duly empowered Europol officials to act as its verifying authority and shall designate in agreement with any Member State the National Access Point of that Member State which shall communicate its requests for comparison of fingerprint data to the Central System.
2. Europol shall designate an operating unit that is authorised to request comparisons with EURODAC data through its designated National Access Point.

⁴³ **UK**, supported by **FR, HU, SE**, queried if there are any operational benefits of EUROPOL's access to the EURODAC data, given the primary strategic character of its remit. **Cion**: if all the conditions for its access are met, EUROPOL's access could be beneficial to its fighting against serious crime. **FI**: scrutiny reservation on the provision; given that EURODAC is a centralised system, EUROPOL could be given a direct access to it, instead of having access through the national access points of a MS. **Cion** recalled that in the context of the VIS, the direct access of EUROPOL has caused some problems.

↓ 2725/2000/EC (adapted)

⇒ new

Article ~~8~~ 3

⊗ Statistics ⊗

3.1. ⁴⁴ The ~~Central Unit~~ ⊗ Agency ⊗ shall draw up statistics on ~~its~~ ⊗ the ⊗ work ⊗ of the Central System ⊗ every ~~quarter~~ ⇒ month ⇐, indicating ⇒ in particular ⇐ :

- (a) the number of data sets transmitted on persons referred to in Articles 9(1), ~~8(1) and 11(1)~~ 14(1) and 17(1) ;
- (b) the number of hits for applicants for ~~asylum~~ ⇒ international protection ⇐ who have lodged an application for ~~asylum~~ ⇒ international protection ⇐ in another Member State;
- (c) the number of hits for persons referred to in Article ~~8(1)~~ 14(1) who have subsequently lodged an application for ~~asylum~~ ⇒ international protection ⇐;

⁴⁴ **SI:** reservation on para. 1; it pointed out that additional statistics regarding the access of law enforcement authorities to the EURODAC, should be drawn up at the level of the Central Unit. In this logic - and taking Art. 40 into account - MS could assess, on the basis of the annual reports, the effectiveness of the access to EURODAC Central Unit. In the same vein, **FI**, supporting **SI**, suggested that statistics made on the comparisons under Art. 19 should also be drawn up at the level of the Central Unit. **Cion** welcomed this suggestion.

- (d) the number of hits for persons referred to in Article ~~11(1)~~ 17(1) who had previously lodged an application for ~~asylum~~ ⇒ international protection ⇐ in another Member State;
- (e) the number of fingerprint data which the Central ~~Unit~~ ⇒ System ⇐ had to ⇒ repeatedly ⇐ request ~~a second time~~ from the Member States of origin because the fingerprint data originally transmitted did not lend themselves to comparison using the computerised fingerprint recognition system;5
-

↓ new

- (f) the number of requests for marking and unmarking transmitted in accordance with Article 18(1) and (2).
- (g) the number of hits for persons referred to in Article 18(1) for whom hits have been recorded under points (b) and (d) of this Article.

45

⁴⁵ **FI, SI, SK** suggested adding two new points (h) and (i), which should read: "the number of requests for purposes referred to in Art. 20(1)" and " the number of requests for purposes referred to in Art. 21(1)" respectively. **Cion** welcomed this suggestion.

↓ 2725/2000/EC

⇒ new

2. At the end of each year, statistical data shall be established in the form of a compilation of the ⇒ monthly ⇐ ~~quarterly~~ statistics ~~drawn up since the beginning of Eurodac's activities~~ ⇒ for that year ⇐, including an indication of the number of persons for whom hits have been recorded under ⇒ points ⇐ (b), (c), and (d). ⇒ The statistics shall contain a breakdown of data for each Member State. ⇐

~~4. Pursuant to the procedure laid down in Article 23(2), the Central Unit may be charged with carrying out certain other statistical tasks on the basis of the data processed at the Central Unit.~~

CHAPTER II

APPLICANTS FOR ~~ASYLUM~~ ⊗ INTERNATIONAL PROTECTION ⊗

Article ~~9~~ 4

Collection, transmission and comparison of fingerprints

1. Each Member State shall promptly take the fingerprints of all fingers of every applicant for ~~asylum~~ ⇒ international protection ⇐ of at least 14 years of age and shall promptly ⇒ as soon as possible and no later than 72 hours after the lodging of that application for international protection as defined by Article 20(2) of the Dublin Regulation ⇐ transmit ⊗ them together with ⊗ the data referred to in points ~~(a)~~ (b) to ~~(f)~~ (g) of Article ~~5(1)~~ 11 to the Central ~~Unit~~ ⇒ System ⇐.

↓ new

⇒ Non compliance with the 72 hours time limit does not relieve Member States of the obligation to take and transmit the fingerprints to the Central System. Where the condition of the fingertips does not allow to take the fingerprints in a quality ensuring appropriate comparison under Article 25 of this Regulation, the Member State of origin shall retake the fingerprints of the applicant and resend them as soon as possible and no later than 48 hours⁴⁶ after they have been successfully taken. ⇐

↓ 2725/2000/EC

~~(2) The data referred to in Article 5(1) shall be immediately recorded in the central database by the Central Unit, or, provided that the technical conditions for such purposes are met, directly by the Member State of origin.~~

↓ new

2. By way of derogation from paragraph 1, where it is not possible to take the fingerprints of an applicant on account of measures taken to ensure the health of the applicant or the protection of public health, Member States shall take and send the fingerprints of the applicant as soon as possible and no later than 48 hours after these grounds no longer prevail.

⁴⁶ **SK:** suggested deleting the wording "and no later than 48 hours". **Cion** pointed out that in accordance with the 2007 Evaluation of the EURODAC and Dublin Regulations and in line with the Dublin recast proposal, fingerprints can be timely submitted to the Central System.

3. Fingerprint data within the meaning of point ~~(b)~~ (a) of Article ~~5(1)~~ 11, transmitted by any Member State, ~~☒~~ with exception to those transmitted in accordance with Article 10 point (b) ~~☒~~ shall be compared ~~⇒ automatically ⇐~~ with the fingerprint data transmitted by other Member States and already stored in the ~~Ce~~ntral ~~database~~ ~~⇒ System ⇐~~.⁴⁷
4. The Central ~~Unit~~ ~~⇒ System ⇐~~ shall ensure, on the request of a Member State, that the comparison referred to in paragraph 3 covers the fingerprint data previously transmitted by that Member State, in addition to the data from other Member States.
5. The Central ~~Unit~~ ~~⇒ System ⇐~~ shall ~~forthwith~~ ~~⇒ automatically~~⁴⁸ ~~⇐~~ transmit the hit or the negative result of the comparison to the Member State of origin. Where there is a hit, it shall transmit for all data sets corresponding to the hit, the data referred to in Article ~~5(1)~~ 8(a)⁴⁹ to ~~(⇐ g ⇐)~~, ~~although in the case of the data referred to in Article 5(1)(b), only insofar as they were the basis for the hit~~ ~~⇒~~ along with, where appropriate, the mark referred to in Article 18(1) ~~⇐~~.

~~Direct transmission to the Member State of origin of the result of the comparison shall be permissible where the technical conditions for such purpose are met.~~

- ~~7. The implementing rules setting out the procedures necessary for the application of paragraphs 1 to 6 shall be adopted in accordance with the procedure laid down in Article ~~22(1)~~.~~

⁴⁷ **SI:** reservation, opposes the limitation of comparison only in an automatic manner on the central level; supports the current Regulation provision - i.e. delete the word “automatically”. **Cion** underlined that the system is capable only of automated check

⁴⁸ **SI:** reservation on the same grounds as for para.5 of this Article.

⁴⁹ **DE, FI, LT, RO:** reference should be made to Art. 11 -(a)-(k), as in the first paragraph of Art. 9. In the same vein, **FI** specified that the reference should be also made to Art 14(2), in order to include fingerprints from category 2 persons.

*Article 10***Information on the status of the data subject**

The following information shall be sent to the Central System in order to be stored in accordance with Article 9 for the purpose of transmission under Article 9(5):

- (a) When an applicant for international protection or another person as referred to in point (d) of Article 18(1) of the Dublin Regulation arrives in the responsible Member State following a transfer pursuant to a decision acceding to a request to take him/her back as referred to in Article 24 of the Dublin Regulation, the responsible Member State shall update its dataset recorded in conformity with Article 8 of this Regulation relating to the person concerned by adding their date of arrival.⁵⁰
- (b) When an applicant for international protection arrives in the responsible Member State following a transfer pursuant to a decision acceding to a request to take charge of them⁵¹ as referred to in Article 22 of the Dublin Regulation, the responsible Member State shall send a dataset in conformity with Article 11 of this Regulation relating to the person concerned and include their date of arrival.
- (c) As soon as the Member State of origin can establish that the person concerned whose data was recorded in EURODAC in accordance with Article 11 of this Regulation has left the territory of the Member States, it shall update its dataset recorded in conformity with Article 11 of this Regulation relating to the person concerned by adding the date when the person left the territory, in order to facilitate the application of Articles 19(2) and 20(5) of the Dublin Regulation.

⁵⁰ **LT, RO:** reference should be made to Art. 11(h) of the Dublin proposal, instead of Art. 8. **Cion** agrees with this submission.

⁵¹ **RO:** "them" should be replaced by "him/her".

- (d) As soon as the Member State of origin ensures that the person concerned whose data was recorded in EURODAC in accordance with Article 11 has left the territory of the Member States in compliance with a return decision or removal order it issued following the withdrawal or rejection of the application as provided for in Article 19(3) of the Dublin Regulation, it shall update its dataset recorded in conformity with Article 11 relating to the person concerned by adding the date of his/her removal or when the person left the territory.
- (e) The Member State which assumes responsibility in accordance with Article 17(1) of the Dublin Regulation shall update its dataset recorded in conformity with Article 11 of this Regulation relating to that applicant by adding the date when the decision to examine the application was taken.

↓ 2725/2000/EC
⇒ new

Article 11 ~~5~~

Recording of data

~~1~~ Only the following data shall be recorded in the eCentral ~~database~~ ⇒ System ⇐ :

- (~~a~~) fingerprint data;

- (b~~a~~) Member State of origin, place and date of the application for ~~asylum~~ ⇒ international protection; in the cases referred to in point (b) of Article 10, the date of application shall be the one entered by the Member State who transferred the applicant ⇐;⁵²
- (c) sex;
- (d) reference number used by the Member State of origin;
- (e) date on which the fingerprints were taken;
- (f) date on which the data were transmitted to the Central ~~Unit~~ ⇒ System ⇐;
- ~~(g) date on which the data were entered in the central database;~~
-

↓ new

- (g) operator user ID.⁵³

⁵² **RO:** queried whether the noting of the date of the application for international protection as the date of the application in the second MS where this TCN was transferred as a result of a take charge procedure could affect the correctness of the statistical data. To this effect, **RO** suggested mentioning the actual date of the applicant's request in the responsible MS, indicating the fact that he/she was transferred, in accordance with Art. 11(h).

Furthermore, **RO** suggested for the sake of coherence with the Dublin proposal the deletion of the wording "in the cases... who transferred the applicant".

⁵³ **AT:** reservation; revealing such personal data could be dangerous for its competent officers.

~~(h) details in respect of the recipient(s) of the data transmitted and the date(s) of transmission(s);~~

(h) where applicable in accordance with Article 10 point (a) or point (b), the date of the arrival of the person concerned after a successful transfer;

(i) where applicable in accordance with Article 10 point (c), the date when the person concerned left the territory of the Member States;

(j) where applicable in accordance with Article 10 point (d), the date when the person concerned left or was removed from the territory of the Member States;

(k) where applicable in accordance with Article 10 point (e), the date when the decision to examine the application was taken.

~~2. After recording the data in the central database, the Central Unit shall destroy the media used for transmitting the data, unless the Member State of origin has requested their return.~~

Article ~~12~~ 6
Data storage⁵⁴

Each set of data, as referred to in Article ~~5(1)~~ 11, shall be stored in the ~~Central database~~ Central System for ten years from the date on which the fingerprints were taken.

Upon expiry of this period, the Central ~~Unit~~ System shall automatically erase the data from the ~~Central database~~ System.

Article ~~13~~ 7
Advance data erasure

1. Data relating to a person who has acquired citizenship of any Member State before expiry of the period referred to in Article ~~6~~ 12 shall be erased from the Central ~~Unit~~ System, in accordance with Article ~~15(3)~~ 27(4) as soon as the Member State of origin becomes aware that the person has acquired such citizenship.

↓ new

2. The Central System shall inform all Member States of origin about the erasure of data for the reason specified in paragraph 1 by another Member State of origin having produced a hit with data which they transmitted relating to persons referred to in Article 9(1) or Article 14(1).

⁵⁴ **RO:** in case of automatic deletion of fingerprints, without exceptions for (multiple) hits, the proper application of the Dublin Regulation may be hindered. In this context, it pointed out that Art. 13(2) of the EURODAC proposal provides for informing through the Central System all MS on the origin of the fingerprints which entailed the hit, whereas there is no such requirement for the more frequently used Art. 12 of the EURODAC proposal. **Cion** pointed out that in accordance with the 2007 Evaluation of the EURODAC Regulation the 10-year storage period was deemed sufficient and requested further evidence from **RO** related to its submissions.

CHAPTER III

~~ALIENS~~ ⊗ THIRD COUNTRY NATIONALS OR STATELESS PERSONS ⊗ APPREHENDED IN CONNECTION WITH THE IRREGULAR CROSSING OF AN EXTERNAL BORDER

Article 14 ^g

Collection and transmission of fingerprint data

1. Each Member State shall, ~~in accordance with the safeguards laid down in the European Convention on Human Rights and in the United Nations Convention on the Rights of the Child~~ promptly take the fingerprints of all fingers of every ~~alien~~ ⊗ third country national or stateless person ⊗ of at least 14 years of age⁵⁵ who is apprehended by the competent control authorities in connection with the irregular crossing by land, sea or air of the border of that Member State having come from a third country and who is not turned back ⇒ or who remains physically on the territory of the Member States and who is not kept in custody, confinement or detention during the entirety of the period between apprehension and removal on the basis of the decision to turn them back ⇐ .

⁵⁵ LV (which suggested aligning this provision with the VIS Regulation), SE, SI: reservations, are in favour of a 12-year limit. Cion will further reflect on this issue.

2. The Member State concerned shall promptly \Rightarrow as soon as possible and no later than 72 hours from the date of apprehension \Leftarrow ⁵⁶ transmit to the Central Unit \Rightarrow System \Leftarrow the following data in relation to any alien \boxtimes third country national or stateless person \boxtimes , as referred to in paragraph 1, who is not turned back:

- (a) fingerprint data;
- (b) Member State of origin, place and date of the apprehension;
- (c) sex;
- (d) reference number used by the Member State of origin;
- (e) date on which the fingerprints were taken;
- (f) date on which the data were transmitted to the Central Unit \Rightarrow System \Leftarrow ;

\Downarrow new

(g) operator user ID.⁵⁷

⁵⁶ **EL:** queried whether, in cases where after the notification the person concerned was not accepted by the country where had to be returned, the relevant data would need to be introduced in the EURODAC system. **Cion** stressed that the 72-hour deadline begins from the taking of the fingerprints. **EL** suggested that the deadline should start running from the positive answer of the third country to the readmission request.

⁵⁷ **AT:** reservation; revealing such data could be dangerous for its competent officers. **Cion** this data is collected in order to ensure that no inappropriate person is involved with the procedure.

3. By way of derogation from paragraph 2, as regards persons apprehended in the manner described in paragraph 1 who remain physically on the territory of the Member States but are kept in custody, confinement⁵⁸ or detention upon their apprehension for a period exceeding 72 hours, the transmission of the data specified in paragraph 2 relating to those persons shall take place before their release from custody, confinement or detention.
4. Non compliance with the 72 hours time limit referred to in paragraph 2 does not relieve Member States of the obligation to take and transmit the fingerprints to the Central System. Where the condition of the fingertips does not allow to take the fingerprints in a quality ensuring appropriate comparison under Article 25, the Member State of origin shall retake the fingerprints of such person and resend them as soon as possible and no later than 48 hours after they have been successfully taken.
5. By way of derogation from paragraph 1, where it is not possible to take the fingerprints of such person on account of measures taken to ensure the health of the person or the protection of public health, the Member State concerned shall take and send the fingerprints of the person, in accordance with the deadline set out in paragraph 2, once these grounds no longer prevail.

⁵⁸ **FR:** scrutiny reservation on the term "confinement". **Cion** recalled that it is an acquis communautaire term and that it implies detention, not necessarily in prison.

↓ 2725/2000/EC (adapted)

⇒ new

Article 15 ~~9~~

Recording of data

1. The data referred to ~~in Article 5(1)(g) and~~ in Article ~~8(2)~~ 14(2) shall be recorded in the ~~central database~~ ⇒ Central System ⇐.

Without prejudice to Article ~~3(2)~~8, data transmitted to the Central ~~Unit~~ ⇒ System ⇐ pursuant to Article ~~8(2)~~ 14(2) shall be recorded for the sole purpose of comparison with data on applicants for ~~asylum~~ ⇒ international protection ⇐ transmitted subsequently to the Central ~~Unit~~ ⇒ System ⇐.

The Central ~~Unit~~ ⇒ System ⇐ shall not compare data transmitted to it pursuant to Article ~~8(2)~~ 14(2) with any data previously recorded in the ~~central database~~ ⇒ Central System ⇐, nor with data subsequently transmitted to the Central ~~Unit~~ ⇒ System ⇐ pursuant to Article ~~8(2)~~ 14(2).⁵⁹

2. ~~The procedures provided for in Article 4(1), second sentence, Article 4(2) and Article 5(2) as well as the provisions laid down pursuant to Article 4(7) shall apply.~~ As regards the comparison of data on applicants for ~~asylum~~ ⇒ international protection ⇐ subsequently transmitted to the Central ~~Unit~~ ⇒ System ⇐ with the data referred to in paragraph 1, the procedures provided for in Article ~~4(3), (5) and (6)~~ 9(3) and (5) and in Article 25(4) shall apply.

⁵⁹ **LT:** drew attention to the fact that, whereas comparison with previously recorded data is not allowed by this provision, this comparison is possible under Art. 17(a)-(c). If it were possible also under Art. 15, it would help MS to indentify a person apprehended in connection with an irregular crossing of an external border and to determine the MS responsible.

Article ~~16~~ ~~10~~

Storage of data

1. Each set of data relating to an ~~alien~~ third country national or stateless person as referred to in Article ~~8(1)~~ 14(1) shall be stored in the ~~central database~~ Central System for one year⁶⁰ ~~two years~~ from the date on which the fingerprints of the ~~alien~~ third country national or stateless person were taken. Upon expiry of this period, the Central ~~Unit~~ System shall automatically erase the data from the ~~central database~~ Central System .

2. The data relating to an ~~alien~~ third country national or stateless person as referred to in Article ~~8(1)~~ 14(1) shall be erased from the ~~central database~~ Central System in accordance with Article ~~15(3)~~ 28(3) as soon as the Member State of origin becomes aware of one of the following circumstances before the ~~two~~ one -year period⁶¹ mentioned in paragraph 1 has expired:
 - (a) the ~~alien~~ third country national or stateless person has been issued with a residence ~~permit~~ document ;⁶²

⁶⁰ **CZ, DE, IE, LT, LV** (both **LT** and **LV** pointed out the risk of abuses, which would jeopardise the whole CEAS and recalled that the majority of delegations supported the two-year option in the discussions of the previous proposals), **AT, RO, SE, SI, UK:** reservations, stressing that the storage period should be two years instead of one. **FR:** scrutiny reservation on the provision. **SK:** supported the current one-year option. **Cion:** for asylum-linked (the main objective of the EURODAC Regulation is to facilitate the functioning of the Dublin Regulation), as well as for data-protection purposes, it would prefer the one-year period storage. **Cion** also recalled the EP position on this issue, in view of the future negotiations within the ordinary procedure.

⁶¹ **SI:** reservation on the same grounds as for para.1 of this Article.

⁶² In the same vein, **FI** pointed out that the data should not be erased if the TCN has been issued a residence permit, but rather mark this data in the same way with the data on person who have been granted international protection. This would also help the determination of the Member State responsible to examine the application for international protection.

- (b) the ~~alien~~ ☒ third country national or stateless person ☒ has left the territory of the Member States;
- (c) the ~~alien~~ ☒ third country national or stateless person ☒ has acquired the citizenship of any Member State.
-

↓ new

3. The Central System shall inform all Member States of origin about the erasure of data for the reason specified in point (a) or (b) of paragraph 2 or by another Member State of origin having produced a hit with data which they transmitted relating to persons referred to in Article 14(1).
4. The Central System shall inform all Member States of origin about the erasure of data for the reason specified in point (c) of paragraph 2 by another Member State of origin having produced a hit with data which they transmitted relating to persons referred to in Article 9(1) or Article 14(1).

CHAPTER IV

~~ALIENS~~ ⊗ THIRD COUNTRY NATIONALS OR STATELESS PERSONS ⊗ FOUND ILLEGALLY ~~PRESENT~~ ⊗ STAYING ⊗ IN A MEMBER STATE

Article 17 ~~11~~

Comparison of fingerprint data⁶³

1. With a view to checking whether an ~~an alien~~ ⊗ third country national or a stateless person ⊗ found illegally ~~present~~ ⊗ staying ⊗ within its territory has previously lodged an application for ~~asylum~~ ⇒ international protection ⇐ in another Member State, each Member State may transmit to the Central ~~Unit~~ ⇒ System ⇐ any fingerprint data relating to fingerprints which it may have taken of any such ~~alien~~ ⊗ third country national or stateless person ⊗ of at least 14 years of age together with the reference number used by that Member State.

⁶³ **DE:** a period for transmitting fingerprints to the EURODAC Central System should be provided for in this Article, as is the case for Art. 9(1) on asylum applicants and Art. 14(4) on illegal entry. **Cion** recalled that there is no provision for data storage regarding the Category 3 people, (who are only checked if they have ever applied for international protection) as long as EURODAC is an asylum and not an illegal immigration instrument. In addition, it would not be appropriate to impose a deadline for sending data under this provision, as long as it is an optional one. **AT:** reservation, wants an extended scope for the provision, in order to cover cases where the removal operation is not imminent and/or are obstacles.

As a general rule there are grounds for checking whether the ~~alien~~ ☒ third country national or stateless person ☒ has previously lodged an application for ~~asylum~~ ⇒ international protection ⇐ in another Member State where:

- (a) the ~~alien~~ ☒ third country national or stateless person ☒ declares that he/she has lodged an application for ~~asylum~~ ⇒ international protection ⇐ but without indicating the Member State in which he/she made the application;
- (b) the ~~alien~~ ☒ third country national or stateless person ☒ does not request ~~asylum~~ ⇒ international protection ⇐ but objects to being returned to his/her country of origin by claiming that he/she would be in danger, or
- (c) the ~~alien~~ ☒ third country national or stateless person ☒ otherwise seeks to prevent his/her removal by refusing to cooperate in establishing his/her identity, in particular by showing no, or false, identity papers.

2. Where Member States take part in the procedure referred to in paragraph 1, they shall transmit to the Central ~~Unit~~ ⇒ System ⇐ the fingerprint data relating to all or at least the index fingers, and, if those are missing, the prints of all other fingers, of ~~aliens~~ ☒ third country nationals or stateless persons ☒ referred to in paragraph 1.

3.⁶⁴ The fingerprint data of an ~~alien~~ ☒ third country national or a stateless person ☒ as referred to in paragraph 1 shall be transmitted to the Central ~~Unit~~ ⇒ System ⇐ solely for the purpose of comparison with the fingerprint data of applicants for ~~asylum~~ ⇒ international protection ⇐ transmitted by other Member States and already recorded in the ~~central database~~ ⇒ Central System ⇐.

⁶⁴ **SK:** reservation on this paragraph.

The fingerprint data of such ~~an alien~~ third country national or a stateless person shall not be recorded in the ~~central database~~ Central System , nor shall they be compared with the data transmitted to the Central ~~Unit~~ System pursuant to Article ~~8(2)~~ 14(2).

4. As regards the comparison of fingerprint data transmitted under this Article with the fingerprint data of applicants for ~~asylum~~ international protection transmitted by other Member States which have already been stored in the Central ~~Unit~~ System , the procedures provided for in Article ~~4(3) (5) and (6)~~ 9(3) and (5) ⁶⁵ ~~as well as the provisions laid down pursuant to Article 4(7)~~ shall apply.

~~5. Once the results of the comparison have been transmitted to the Member State of origin, the Central Unit shall forthwith:~~

~~(a) erase the fingerprint data and other data transmitted to it under paragraph 1; and~~

~~(b) destroy the media used by the Member State of origin for transmitting the data to the Central Unit, unless the Member State of origin has requested their return.~~

⁶⁵ **SK:** reference to Art. 25(4) should be added.

CHAPTER V

~~RECOGNISED REFUGEES~~ ☒ PERSONS GRANTED INTERNATIONAL PROTECTION ☒

~~Article 12~~

~~Blocking of data~~

~~1. Data relating to an applicant for asylum which have been recorded pursuant to Article 4(2) shall be blocked in the central database if that person is recognised and admitted as a refugee in a Member State. Such blocking shall be carried out by the Central Unit on the instructions of the Member State of origin.~~

~~As long as a decision pursuant to paragraph 2 has not been adopted, hits concerning persons who have been recognised and admitted as refugees in a Member State shall not be transmitted. The Central Unit shall return a negative result to the requesting Member State.~~

~~2. Five years after Eurodac starts operations, and on the basis of reliable statistics compiled by the Central Unit on persons who have lodged an application for asylum in a Member State after having been recognised and admitted as refugees in another Member State, a decision shall be taken in accordance with the relevant provisions of the Treaty, as to whether the data relating to persons who have been recognised and admitted as refugees in a Member State should:~~

~~(a) be stored in accordance with Article 6 for the purpose of the comparison provided for in Article 4(3); or~~

~~(b) be erased in advance once a person has been recognised and admitted as a refugee.~~

~~3. In the case referred to in paragraph 2(a), the data blocked pursuant to paragraph 1 shall be unblocked and the procedure referred to in paragraph 1 shall no longer apply.~~

~~4. In the case referred to in paragraph 2(b):~~

~~(a) data which have been blocked in accordance with paragraph 1 shall be erased immediately by the Central Unit; and~~

~~(b) data relating to persons who are subsequently recognised and admitted as refugees shall be erased in accordance with Article 15(3), as soon as the Member State of origin becomes aware that the person has been recognised and admitted as a refugee in a Member State.~~

~~5. The implementing rules concerning the procedure for the blocking of data referred to in paragraph 1 and the compilation of statistics referred to in paragraph 2 shall be adopted in accordance with the procedure laid down in Article 22(1).~~

*Article 18***Marking of data**

1. The Member State of origin which granted international protection to an applicant for international protection whose data were previously recorded pursuant to Article 11 in the Central System shall mark the relevant data in conformity with the requirements for electronic communication with the Central System established by the Agency. This mark shall be stored in the Central System in accordance with Article 12 for the purpose of transmission under Article 9(5).
2. The Member State of origin shall unmark data concerning a third country national or stateless person whose data were previously marked in accordance with paragraph 1 if his or her status is revoked or ended or renewal of his status is refused under Article 14 or 19 of Council Directive 2004/83/EC.⁶⁶

⁶⁶ **SK:** This reference to the Qualification Directive shall be updated as to cite amended Directive 2011/95/EU.

CHAPTER VI

PROCEDURE FOR COMPARISON AND DATA TRANSMISSION FOR LAW ENFORCEMENT PURPOSES⁶⁷

Article 19

Procedure for comparison of fingerprint data with EURODAC data

1. The designated authorities referred to in Article 5(1) and Europol may submit a reasoned electronic request to the verifying authority for the transmission for comparison of fingerprint data to the EURODAC Central System via the National Access Point.⁶⁸ Upon receipt of such a request, the verifying authority shall verify whether the conditions for requesting a comparison referred to in Article 20 or Article 21, as appropriate, are fulfilled.

⁶⁷ **DE, FI:** a provision along the lines of Arts 9(3)&(5) or 17(4) shall be inserted in this Chapter in order to provide for the transmission of data to designated authorities, for the purpose of law enforcement access. **RO** suggested adding language regarding the transmission of information for the person, who has been the subject of a hit (within the scope of this paragraph) and linking it with the corresponding category (1 or 2) to which he/she belongs. **IT** also suggested specifying whether the relevant marks for the above persons should constitute a special category or not.

LT pointed out that the definitions used in respect of the law enforcement access to EURODAC, as well as the conditions / purposes for this access, should reflect as closely as possible the relevant provisions of the Council Decision 2008/633/JHA concerning access for consultation to the VIS.

⁶⁸ **EL:** scrutiny reservation on the technical ramification of the procedure described in this provision. **Cion** pointed out that the transmission of data for law enforcement purposes shall be done in the same way as for the other objectives of the EURODAC Regulation and this should be clarified.

2. Where all the conditions for requesting a comparison are fulfilled, the verifying authority shall transmit the request for comparison to the National Access Point which will process it to the EURODAC Central System for the purpose of comparison with all the EURODAC data.⁶⁹
3. In exceptional cases of urgency, the verifying authority may transmit the fingerprint data to the National Access Point for comparison immediately upon receipt of a request by a designated authority and only verify ex-post whether all the conditions of Article 20 or Article 21 are fulfilled, including whether an exceptional case of urgency actually existed. The ex-post verification shall take place without undue delay after the processing of the request.
4. Where the ex-post verification determines that the access was not justified, the information communicated from EURODAC shall be destroyed by all authorities that have accessed it and they shall inform the verifying authority of such destruction.

⁶⁹ **FR:** it should be clarified that the request should not contain the reasons justifying it. **Cion** agreed that it would not be necessary to include the reasons for the request made to the Central System. **Cion** pointed out that the transmission shall be carried out in accordance with Arts 9(3) and (5).

Article 20

Conditions for access to EURODAC data by designated authorities

- 1.⁷⁰ Designated authorities may request the comparison of fingerprint data with those stored in the EURODAC central database within the scope of their powers only if comparisons of national fingerprint databases and of the Automated Fingerprint Databases of other Member States under Decision 2008/615/JHA return negative results⁷¹ and where:
- (a) the comparison is necessary for the purpose of the prevention, detection or investigation of terrorist offences or other serious criminal offences;⁷²

⁷⁰ **AT:** reservation on the provision; **DE:** the meaning of the wording “comparisons that return negative results”, under Council Decision 2008/615/JHA, should be clearly defined; in this context, it queried whether negative results should be returned from a request to all MS, or requests to individual MS would be sufficient. **CZ:** it may not be possible to have clear negative results as long as the Prüm check cannot give all the necessary information. Thus, the access to EURODAC should be given after the national data comparison is done. **Cion** will further reflect on this issue.

⁷¹ **FI, AT:** oppose the obligation to have national and Prüm comparisons as a precondition for the EURODAC comparison. **FI** recalled that such a precondition does not apply in the case of access to the VIS data base. **NL, DE** queried about the nature of a hit which does not allow identification of the TCN and whether such a hit would entitle MS to have access to EURODAC. In the same vein, **HU** questioned the added value of Prüm in the EURODAC legal framework. **Cion** recalled that this precondition is met, even if the Prüm procedure is in force with only one other MS. **HU** also suggested that as regards the Prüm-related questions a coordination with the DAPIX WP could be helpful.

⁷² **FR:** this obligation for the designated authorities could be excessive.

(b) the comparison is necessary in a specific case; systematic comparisons shall not be carried out; and

(c) there are reasonable grounds⁷³ to consider that such comparison with EURODAC data will contribute to the prevention, detection or investigation of any of the criminal offences in question.⁷⁴

2. Requests for comparison with EURODAC data shall be limited to searching with fingerprint data.⁷⁵

⁷³ **FR** deems as counterproductive the obligation for the designated authorities to prove that there are reasonable grounds to consider that the comparison with the EURODAC data would contribute to prevention, etc. of the offences in question. **ES:** point (c) should be deleted.

⁷⁴ **SI** queried whether the conditions laid down in points (a) - (c) are cumulative or not and asked for a clearer wording. **BE:** these conditions / guarantees are cumulative; the one in (c) is too widely drafted. **Cion:** all conditions set out in Art. 20 shall be met in order to have access to EURODAC.

⁷⁵ **FR** considers that other comparison based on the civil status of the person concerned or on external borders checks could be taken into account. **Cion:** the EURODAC comparison is done only through fingerprint data comparison. **CZ** considers this provision superfluous. **ES:** the scope of this paragraph should be broadened.

Article 21

Conditions for access to EURODAC data by Europol⁷⁶

1. Requests for comparison with EURODAC data by Europol shall take place within the limits of its mandate and where necessary for the performance of its tasks pursuant to the Europol Decision and for the purposes of a specific analysis or an analysis of a general nature and of a strategic type.
2. Requests for comparison with EURODAC data shall be limited to comparisons of fingerprint data.
3. Processing of information obtained by Europol from comparison with EURODAC shall be subject to the authorisation of the Member State of origin. Such authorisation shall be obtained via the Europol national unit of that Member State.

⁷⁶ **CZ:** the conditions for access to EURODAC by EUROPOL should take into account the particular duties of EUROPOL. **FR:** reservation, **BE** scrutiny reservation on the Article; **FR:** granting direct access to EUROPOL does not tally with its role; one MS linked with the case, pursuant to Art. 20 should be making the comparison. **Cion:** this issue will be further reflected; at any rate EUROPOL has a limited mandate, within which is entitled to act. **BE:** the conditions for law enforcement authorities' access to EURODAC do not seem to apply to EUROPOL's access to EURODAC. **Cion:** it can be clarified that the same strict conditions apply to EUROPOL's access.
EE: queried about the scope of the analysis on the basis of the fingerprints (specific or general) and the relevant added value of EUROPOL's intervention. **Cion:** EUROPOL has a mandate to process finger prints and other data in order to fulfill its objectives; in this sense, it can, if it turns out to be useful, request access to the EURODAC data.

Article 22

Communication between the verifying authorities and the National Access Points⁷⁷

1. EURODAC Communication Infrastructure shall be used for the data transmission by the verifying authorities of Member States and Europol to the National Access Points and vice versa. All communications shall take place electronically.
2. Fingerprints shall be digitally processed by the Member State and transmitted in the data format referred to in Annex I, in order to ensure that the comparison can be carried out by means of the computerised fingerprint recognition system.

↓ 2725/2000/EC (adapted)

⇒ new

CHAPTER ~~VI~~ VII

**DATA PROCESSING ~~USE~~, DATA PROTECTION⁷⁸ AND
LIABILITY**

Article 23 ~~13~~

Responsibility for data processing ~~use~~

1. The Member State of origin shall be responsible for ensuring that:

⁷⁷ **CZ:** reservation on the Article. In reply to the **UK**, **Cion** confirmed that Recital defined the EURODAC Communication Infrastructure.

⁷⁸ **ES:** general scrutiny reservation on all data protection provisions.

- (a) fingerprints are taken lawfully;
 - (b) fingerprint data and the other data referred to in Article ~~5(1)~~ 11, Article ~~8(2)~~ 14(2) and Article ~~11(2)~~ 17(2) are lawfully transmitted to the Central ~~Unit~~ ⇒ System ⇐;
 - (c) data are accurate and up-to-date when they are transmitted to the Central ~~Unit~~ ⇒ System ⇐;
 - (d) without prejudice to the responsibilities of the ~~Commission~~ ⇒ Agency ⇐, data in the ~~central database~~ ⇒ Central System ⇐ are lawfully recorded, stored, corrected and erased;
 - (e) the results of fingerprint data comparisons transmitted by the Central ~~Unit~~ ⇒ System ⇐ are lawfully processed ~~used~~.
2. In accordance with Article ~~14~~ 34, the Member State of origin shall ensure the security of the data referred to in paragraph 1 before and during transmission to the Central ~~Unit~~ ⇒ System ⇐ as well as the security of the data it receives from the Central ~~Unit~~ ⇒ System ⇐.
 3. The Member State of origin shall be responsible for the final identification of the data pursuant to Article ~~4(6)~~ 25(4).
 4. The ~~Commission~~ ⇒ Agency ⇐ shall ensure that the Central ~~Unit~~ ⇒ System ⇐ is operated in accordance with the provisions of this Regulation ~~and its implementing rules~~. In particular, the ~~Commission~~ ⇒ Agency ⇐ shall:

(a) adopt measures ensuring that persons working ~~in~~ with ~~in~~ the Central ~~Unit~~
~~System~~ ~~process~~ use the data recorded ~~in~~ therein ~~in the central database~~
only in accordance with the purpose of ~~Eurodac~~EURODAC as laid down in Article
1(1);

~~(b) ensure that persons working in the Central System comply with all requests from
Member States made pursuant to this Regulation in relation to recording,
comparison, correction and erasure of data for which they are responsible;~~

~~(b)~~ (e) take the necessary measures to ensure the security of the Central ~~Unit~~
~~System~~ in accordance with Article ~~14~~ 34;

~~(c)~~ (d) ensure that only persons authorised to work ~~in~~ with ~~in~~ the Central ~~Unit~~
~~System~~ have access ~~to~~ thereto ~~to data recorded in the central database,~~
without prejudice to ~~Article 20 and the powers of the independent supervisory body
which will be established under Article 286(2) of the Treaty~~ ~~to~~ the competences of
the European Data Protection Supervisor ~~to~~.

The ~~Commission~~ ~~Agency~~ shall inform the European Parliament and the Council ~~as~~
well as the European Data Protection Supervisor ~~of~~ of the measures it takes pursuant to the
first subparagraph.

Article ~~24~~ 2

Transmission

1. Fingerprints shall be digitally processed and transmitted in the data format referred to in Annex I. As far as it is necessary for the efficient operation of the Central ~~Unit~~ ⇒ System ⇐, the ~~Central Unit~~ ⇔ Agency ⇔ shall establish the technical requirements for transmission of the data format by Member States to the Central ~~Unit~~ ⇒ System ⇐ and vice versa. The ~~Central Unit~~ ⇔ Agency ⇔ shall ensure that the fingerprint data transmitted by the Member States can be compared by the computerised fingerprint recognition system.
2. Member States ~~should~~ ⇔ shall ⇔ transmit the data referred to in Article ~~5(1)~~ 11(1), ~~Article 14(2) and Article 17(2) of the Eurodac Regulation~~ electronically. ⇒ The data referred to in Article 11(1) and Article 14(2) shall be automatically recorded in the Central System. ⇐ As far as it is necessary for the efficient operation of the Central ~~Unit~~ ⇒ System ⇐, the ~~Central Unit~~ ⇒ Agency ⇐ shall establish the technical requirements to ensure that data can be properly electronically transmitted from the Member States to the Central ~~Unit~~ ⇒ System ⇐ and vice versa. ~~Transmission of data in paper form using the form set out in Annex II or by other means of data support (diskettes, CD-ROM or other means of data support which may be developed and generally used in future) should be limited to situations in which there are continuous technical problems.~~

- ⁷⁹3. The reference number referred to in Article ~~5(1)(d)~~ 11(d) and Article 14(2)(d) and 17(1) ~~of the Eurodac Regulation~~ shall make it possible to relate data unambiguously to one particular person and to the Member State which is transmitting the data. In addition, it shall make it possible to tell whether such data relate to ~~an asylum seeker or~~ a person referred to in Article ~~8 or Article 11 of the Eurodac Regulation~~9, Article 14 or Article 17.
4. The reference number shall begin with the identification letter or letters by which, in accordance with the norm referred to in Annex I, the Member State transmitting the data is identified. The identification letter or letters shall be followed by the identification of the category of person. "1" refers to data relating to ~~asylum seekers~~ persons referred to in Article 9(1) , "2" to persons referred to in Article ~~8~~ 14(1) ~~of the Eurodac Regulation~~ and "3" to persons referred to in Article ~~11~~ 17 ~~of the Eurodac Regulation~~.
5. The ~~Central Unit~~ Agency shall establish the technical procedures necessary for Member States to ensure receipt of unambiguous data by the Central ~~Unit~~ System .
- 6~~4.~~ The Central ~~Unit~~ System shall confirm receipt of the transmitted data as soon as possible. To this end the ~~Central Unit~~ Agency shall establish the necessary technical requirements to ensure that Member States receive the confirmation receipt if requested.

⁷⁹ **FI:** pointed out that technical provisions on the comparison of fingerprints for the purposes set out in Art. 1(2) should be added in paras (3) and (4) (obligation to use a reference number, letters identifying the requesting MS, identification of the category of the person concerned). These suggestions would serve statistical, logging and documentation purposes.

Carrying out comparisons and transmitting results

1. Member States shall ensure the transmission of fingerprint data in an appropriate quality for the purpose of comparison by means of the computerised fingerprint recognition system. As far as it is necessary to ensure that the results of the comparison by the Central ~~Unit~~ ⇒ System ⇐ reach a very high level of accuracy, the ~~Central Unit~~ ⇒ Agency ⇐ shall define the appropriate quality of transmitted fingerprint data. The Central ~~Unit~~ ⇒ System ⇐ shall, as soon as possible, check the quality of the fingerprint data transmitted. If fingerprint data do not lend themselves to comparison using the computerised fingerprint recognition system, the Central ~~Unit~~ ⇒ System ⇐ shall, ~~as soon as possible,~~ ⇒ inform ⇐ the Member State. ⇒ The Member State concerned shall ⇐ transmit fingerprint data of the appropriate quality ⇒ using the same reference number of the previous set of fingerprint data ⇐.
2. The Central ~~Unit~~ ⇒ System ⇐ shall carry out comparisons in the order of arrival of requests. Each request must be dealt with within 24 hours. ~~In the case of data which are transmitted electronically, a~~ A Member State may for reasons connected with national law require particularly urgent comparisons to be carried out within one hour. Where these times cannot be respected owing to circumstances which are outside the ~~Central Unit~~ ⇒ Agency's ⇐ responsibility, the Central ~~Unit~~ ⇒ System ⇐ shall process the request as a matter of priority as soon as those circumstances no longer prevail. In such cases, as far as it is necessary for the efficient operation of the Central ~~Unit~~ ⇒ System ⇐, the ~~Central Unit~~ ⇒ Agency ⇐ shall establish criteria to ensure the priority handling of requests.
3. As far as it is necessary for the efficient operation of the Central ~~Unit~~ ⇒ System ⇐, the ~~Central Unit~~ ⇒ Agency ⇐ shall establish the operational procedures for the processing of the data received and for transmitting the result of the comparison.

↓ 2725/2000/EC Article 4(6) (adapted)

⇒ new

4. The results of the comparison shall be immediately checked in the Member State of origin ⇒ by a fingerprint expert ⇐⁸⁰. Final identification shall be made by the Member State of origin in cooperation with the Member States concerned, pursuant to Article ~~15~~ 32 of the Dublin ~~Convention~~ ⊗ Regulation ⊗⁸¹.

Information received from the Central ~~Unit~~ ⇒ System ⇐ relating to other data found to be unreliable shall be erased ~~or destroyed~~ as soon as the unreliability of the data is established.

↓ new

5. Where final identification in accordance with paragraph 4 reveal that the result of the comparison received from the Central System is inaccurate, Member States shall communicate this fact to the Commission and to the Agency.

⁸⁰ **CZ, FI** (suggesting deletion of the point) **FR** (querying about the profile of the "fingerprint expert"), **SI**: reservations on the term.
SI opposes the strict obligation to compare fingerprints manually with a fingerprint expert at MS level, as it would require administrative burden for the MS and suggested maintaining the current Regulation's provision. **UK**: the fingerprint expert's role is useful, as the very limited number of false hits in the EURODAC Annual Report proves; he/she will be very important for the latent fingerprints taking. **Cion**: pointed out that the fingerprint expert should be someone able to verify whether there is a match between fingerprints, as MS do on national basis. **Cion** also recalled the EP position on this issue, in view of the future negotiations within the ordinary procedure.

⁸¹ **RO**: has concerns that the information exchange, which should be made in accordance with Art. 32 of the draft Dublin Regulation, shall have a clear legal basis in the said instrument. However, the Dublin text does not provide for cases under Chapter VI of the EURODAC proposal. **Cion**: this provision is not linked with law enforcement access purposes.

↓ 407/2002/EC (adapted)

⇒ new

Article ~~26~~ 4

Communication between Member States and the Central ~~Unit~~ ⇒ System ⇐

Data transmitted from the Member States to the Central ~~Unit~~ ⇒ System ⇐ and vice versa shall use ~~IDA generic services referred to in Decision No 1719/1999/EC of the European Parliament and of the Council of 12 July 1999 on a series of guidelines, including the identification of projects of common interest, for trans-European networks for the electronic interchange of data between administrations (IDA)~~ ⇒ the EURODAC Communication Infrastructure ⇐. As far as it is necessary for the efficient operation of the Central ~~Unit~~ ⇒ System ⇐, the ~~Central Unit~~ ⊗ Agency ⊗ shall establish the technical procedures necessary for the use of ~~IDA generic services~~ ⇒ the Communication ⇐.

~~Article 14~~

~~Security~~

~~1. The Member State of origin shall take the necessary measures to:~~

- ~~(a) prevent any unauthorised person from having access to national installations in which the Member State carries out operations in accordance with the aim of Eurodac (checks at the entrance to the installation);~~

~~(b) prevent data and data media in Eurodac from being read, copied, modified or erased by unauthorised persons (control of data media);~~

~~(c) guarantee that it is possible to check and establish a posteriori what data have been recorded in Eurodac when and by whom (control of data recording);~~

~~(d) prevent the unauthorised recording of data in Eurodac and any unauthorised modification or erasure of data recorded in Eurodac (control of data entry);~~

~~(e) guarantee that, in using Eurodac, authorised persons have access only to data which are within their competence (control of access);~~

~~(f) guarantee that it is possible to check and establish to which authorities data recorded in Eurodac may be transmitted by data transmission equipment (control of transmission);~~

~~(g) prevent the unauthorised reading, copying, modification or erasure of data during both the direct transmission of data to or from the central database and the transport of data media to or from the Central Unit (control of transport);~~

~~2. As regards the operation of the Central Unit, the Commission shall be responsible for applying the measures mentioned under paragraph 1.~~

↓ 2725/2000/EC

⇒ new

Article 27 ~~15~~

Access to, and correction or erasure of, data recorded in ~~Eurodac~~ EURODAC

1. The Member State of origin shall have access to data which it has transmitted and which are recorded in the ~~central database~~ ⇒ Central System ⇐ in accordance with the provisions of this Regulation.

No Member State may conduct searches in the data transmitted by another Member State, nor may it receive such data apart from data resulting from the comparison referred to in Article ~~4(5)~~ 9(5).⁸²

⁸² **LU** queried if this provision contradicts para. 4 of this Article whereby a MS may advise against the proper recording of certain data, done by another MS. **Cion** pointed out that since this is not in the recast part of the proposal, therefore it could be considered to be amended following a future evaluation of the EURODAC function. **RO:** in relation to the comparison made on the basis of Art 9(5) reference should also be made to Arts 17(3), 20(1) and 21(1). **Cion:** will check this issue out.

↓ 2725/2000/EC (adapted)

⇒ new

2. The authorities of Member States which, pursuant to paragraph 1, have access to data recorded in the ~~central database~~ ⇒ Central System ⇐ shall be those designated by each Member State ⇒ for the purpose of Article 1(1). This designation shall specify the exact unit responsible for carrying out tasks related to the application of this Regulation. ⇐ Each Member State shall without delay communicate to the Commission ⇒ and the Agency ⇐ a list of those authorities ⇒ and any amendments thereto. The Agency shall publish the consolidated list in the Official Journal of the European Union. Where there are amendments thereto, the Agency shall publish once a year an updated consolidated list. ⇐
3. Only the Member State of origin shall have the right to amend the data which it has transmitted to the Central Unit ⇒ System ⇐ by correcting or supplementing such data, or to erase them, without prejudice to erasure carried out in pursuance of Article ~~6, Article 10(1) or Article 12(4)(a)~~ 12 or Article 16(1).

~~Where the Member State of origin records data directly in the central database, it may amend or erase the data directly.~~

~~Where the Member State of origin does not record data directly in the central database, the Central Unit shall amend or erase the data at the request of that Member State.~~

4. If a Member State or the ~~Central Unit~~ ⇒ Agency ⇐ has evidence to suggest that data recorded in the ~~central database~~ ⇒ Central System ⇐ are factually inaccurate, it shall advise the Member State of origin as soon as possible.

If a Member State has evidence to suggest that data were recorded in the ~~central database~~ ⇒ Central System ⇐ contrary to this Regulation, it shall ~~similarly~~ advise ⇒ the Agency, the Commission and ⇐ the Member State of origin as soon as possible. The latter shall check the data concerned and, if necessary, amend or erase them without delay.

5. The ~~Central Unit~~ ⇒ Agency ⇐ shall not transfer or make available to the authorities of any third country data recorded in the ~~central database~~ ⇒ Central System ⇐, unless it is specifically authorised to do so in the framework of a Community agreement on the criteria and mechanisms for determining the State responsible for examining an application for ~~asylum~~ ⇒ international protection ⇐.⁸³

~~Article 22~~

~~Implementing rules~~

- ~~1. The Council shall adopt, acting by the majority laid down in Article 205(2) of the Treaty, the implementing provisions necessary for~~
- ~~laying down the procedure referred to in Article 4(7),~~
- ~~laying down the procedure for the blocking of the data referred to in Article 12(1),~~
- ~~drawing up the statistics referred to in Article 12(2).~~

⁸³ **FR:** asked the **Cion** to provide clarification about the relation of this provision with Art. 35. **Cion** confirmed that this provision is focusing on Dublin associate countries.

~~In cases where these implementing provisions have implications for the operational expenses to be borne by the Member States, the Council shall act unanimously.~~

~~2. The measures referred to in Article 3(4) shall be adopted in accordance with the procedure referred to in Article 23(2).~~

Article 28 ~~16~~

Keeping of records ~~by the Central Unit~~⁸⁴

1. The ~~Central Unit~~ ⇒ Agency ⇐ shall keep records of all data processing operations within the Central ~~Unit~~ ⇒ System ⇐. These records shall show the purpose of access, the date and time, the data transmitted, the data used for interrogation and the name of both the unit ~~putting~~ ⊗ entering ⊗ in or retrieving the data and the persons responsible.
2. Such records may be used only for the data-protection monitoring of the admissibility of data processing as well as to ensure data security pursuant to Article ~~14~~ 34. The records must be protected by appropriate measures against unauthorised access and erased after a period of one year ⇒ after the retention period referred to in Article 12 and in Article 16(1) ~~has expired~~ ⇐, if they are not required for monitoring procedures which have already begun.

↓ new

3. Each Member State shall take the necessary measures in order to achieve the objectives set out in paragraph 1 and 2 in relation to its national system. In addition, each Member State shall keep records of the staff duly authorised to enter or retrieve the data.

⁸⁴ DE: pointed out that Article 36 covers only data processing operations for law enforcement purposes, while Article 28 applies to all other operations. However, the relationship between the two provisions should be clarified in order to confirm the requirements which must be fulfilled in each case.

↓ 2725/2000/EC (adapted)

⇒ new

~~Article 23~~

~~Committee~~

~~1. The Commission shall be assisted by a committee.~~

~~2. In the cases where reference is made to this paragraph, Articles 5 and 7 of Decision 1999/468/EC shall apply.~~

~~The period laid down in Article 5(6) of Decision 1999/468/EC shall be set at three months.~~

~~3. The committee shall adopt its rules of procedure.~~

Article 29 ~~18~~

Rights of the data subject

1. A person covered by this Regulation shall be informed by the Member State of origin ⇒ in writing, and where appropriate, orally, in a language which he or she understands or may reasonably be presumed to understand ⇐ of the following:

(a) the identity of the controller and of his representative, if any;

- (b) ~~the~~ regarding ~~the~~ the purpose for which ~~the~~ his or her ~~the~~ data will be processed within ~~Eurodac~~EURODAC ~~⇒~~ including a description of the aims of the Dublin Regulation, in accordance with Article 4 of that Regulation ~~⇐~~.
- (c) the recipients of the data;
- (d) in relation to a person covered by Article ~~4 9~~ or Article ~~8 14~~, the obligation to have his/her fingerprints taken;
- (e) the existence of the right of access to, ~~and the right to rectify,~~ the data ~~relating to~~ him/her ~~concerning him/her~~ , and the right to request that inaccurate data relating to him/her be corrected ~~⇐~~ ~~⇒~~ or that unlawfully processed data relating to them⁸⁵ be erased, as well as the right to receive information on the procedures for exercising those rights including the contact details of the controller and the National Supervisory Authorities referred to in Article 31(1) ~~⇐~~.

In relation to a person covered by Article ~~4 9~~ or Article ~~8 14~~, the information referred to in the first subparagraph shall be provided when his/her fingerprints are taken.

In relation to a person covered by Article ~~11 17~~, the information referred to in the first subparagraph shall be provided no later than the time when the data relating to the person are transmitted to the Central ~~Unit~~ ~~⇒~~ System ~~⇐~~. This obligation shall not apply where the provision of such information proves impossible or would involve a disproportionate effort.

⁸⁵ **RO:** the word "them" should be replaced by "him/her".

↓ new

A common leaflet, containing at least the information referred to in paragraph 1 of this Article and the information referred to in Article 4(1) of the Dublin Regulation shall be drawn up in accordance with the procedure referred to in Article 40(2) of the Dublin Regulation. The leaflet should be "clear and simple, drafted in a language that the person understands or may reasonably be presumed to understand."⁸⁶

Where a person covered by this Regulation is a minor, Member States shall provide the information in an age-appropriate manner.

↓ 2725/2000/EC

⇒ new

2. In each Member State any data subject may, in accordance with the laws, regulations and procedures of that State, exercise the rights provided for in Article 12 of Directive 95/46/EC.⁸⁷

⁸⁶ **SI:** scrutiny reservation in relation to the obligation of providing a leaflet to persons who are not applicants for international protection. **Cion** clarified that the scope of this proposal covers all TCN whose fingerprints are in the EURODAC data base. It also clarified that Art. 29 applies only to asylum-related purposes.

NL: the folder should be in the most pertinent languages for its purposes. **Pres:** the language should be adapted to Art. 4 of the draft Dublin Regulation relevant provision. **UK** recalled that a leaflet is used for the EURODAC purposes and the only essential addition would be the information about the law-enforcement access. **Cion:** it would not be reasonable to ask the TCN to give fingerprints, without clearly explaining the reasons, in particular for law-enforcement purposes; a common leaflet among MS would cut the costs and could enhance practical co-operation. **Cion** also indicated that AMF might be used for financing the leaflet.

⁸⁷ **HU** pointed out this provision, as well as para. 10 of this Article, should also refer to the relevant provisions of the Framework Decision 2008/977/JHA (Arts. 17, 18, 25(3)), because Directive 95/46/EC does not apply to data processing for law enforcement purposes and Recital 31 of this proposal is not sufficient. **Cion** stressed that Art. 29 applies only to asylum-related elements of the proposal. **DE** suggested that this should be explicitly mentioned.

Without prejudice to the obligation to provide other information in accordance with point (a) of Article 12 of Directive 95/46/EC, the data subject shall have the right to obtain communication of the data relating to him/her recorded in the ~~central database~~ ⇒ Central System ⇐ and of the Member State which transmitted them to the Central ~~Unit~~ ⇒ System ⇐. Such access to data may be granted only by a Member State.

3. In each Member State, any person may request that data which are factually inaccurate be corrected or that data recorded unlawfully be erased. The correction and erasure shall be carried out without excessive delay by the Member State which transmitted the data, in accordance with its laws, regulations and procedures.
4. If the rights of correction and erasure are exercised in a Member State, other than that, or those, which transmitted the data, the authorities of that Member State shall contact the authorities of the Member State, or States, in question so that the latter may check the accuracy of the data and the lawfulness of their transmission and recording in the ~~central database~~ ⇒ Central System ⇐.
5. If it emerges that data recorded in the ~~central database~~ ⇒ Central System ⇐ are factually inaccurate or have been recorded unlawfully, the Member State which transmitted them shall correct or erase the data in accordance with Article ~~15(3)~~ 27(3). That Member State shall confirm in writing to the data subject without excessive delay that it has taken action to correct or erase data relating to him/her.

6. If the Member State which transmitted the data does not agree that data recorded in the ~~central database~~ ⇒ Central System ⇐ are factually inaccurate or have been recorded unlawfully, it shall explain in writing to the data subject without excessive delay why it is not prepared to correct or erase the data.

That Member State shall also provide the data subject with information explaining the steps which he/she can take if he/she does not accept the explanation provided. This shall include information on how to bring an action or, if appropriate, a complaint before the competent authorities or courts of that Member State and any financial or other assistance that is available in accordance with the laws, regulations and procedures of that Member State.

7. Any request under paragraphs 2 and 3 shall contain all the necessary particulars to identify the data subject, including fingerprints. Such data shall be used exclusively to permit the exercise of the rights referred to in paragraphs 2 and 3 and shall be destroyed immediately afterwards.
8. The competent authorities of the Member States shall cooperate actively to enforce promptly the rights laid down in paragraphs 3, 4 and 5.

↓ new

9. Whenever a person requests data relating to him or her in accordance with paragraph 2, the competent authority shall keep a record in the form of a written document that such a request was made, and shall make this document available to the National Supervisory Authorities without delay, upon their request.

↓ 2725/2000/EC (adapted)

⇒ new

~~9.~~ 10. In each Member State, the national supervisory authority shall ⇒ on the basis of his/her request, ⇐ assist the data subject in accordance with Article 28(4) of Directive 95/46/EC in exercising his/her rights.

~~10.~~ 11. The national supervisory authority of the Member State which transmitted the data and the national supervisory authority of the Member State in which the data subject is present shall assist and, where requested, advise him/her in exercising his/her right to correct or erase data. Both national supervisory authorities shall cooperate to this end. Requests for such assistance may be made to the national supervisory authority of the Member State in which the data subject is present, which shall transmit the requests to the authority of the Member State which transmitted the data. ~~The data subject may also apply for assistance and advice to the joint supervisory authority set up by Article 20.~~

~~11.~~ 12. In each Member State any person may, in accordance with the laws, regulations and procedures of that State, bring an action or, if appropriate, a complaint before the competent authorities or courts of the State if he/she is refused the right of access provided for in paragraph 2.

~~12.~~ 13. Any person may, in accordance with the laws, regulations and procedures of the Member State which transmitted the data, bring an action or, if appropriate, a complaint before the competent authorities or courts of that State concerning the data relating to him/her recorded in the ~~central database~~ ⇒ Central System ⇐, in order to exercise his/her rights under paragraph 3. The obligation of the national supervisory authorities to assist and, where requested, advise the data subject, in accordance with paragraph ~~10~~ 13, shall subsist throughout the proceedings.

Article 30 ~~19~~

⊗ Supervision by the ⊗ National Supervisory Authority

1. Each Member State shall provide that the national supervisory authority or authorities designated pursuant to Article 28(1) of Directive 95/46/EC shall monitor independently, in accordance with its respective national law, the lawfulness of the processing, in accordance with this Regulation, of personal data by the Member State in question, including their transmission to the Central ~~Unit~~ ⇨ System ⇐.
 2. Each Member State shall ensure that its national supervisory authority has access to advice from persons with sufficient knowledge of fingerprint data.
-

↓ new

Article 31

Supervision by the European Data Protection Supervisor⁸⁸

1. The European Data Protection Supervisor shall ensure that all the personal data processing activities concerning EURODAC, in particular by the Agency are carried out in accordance with Regulation (EC) No 45/2001 and this Regulation.

⁸⁸ **FR:** scrutiny reservation on Arts 31-37.

2. The European Data Protection Supervisor shall ensure that an audit of the Agency's personal data processing activities is carried out in accordance with international auditing standards⁸⁹ at least every four years. A report of such audit shall be sent to the European Parliament, the Council, the Agency, the Commission and the National Supervisory Authorities. The Agency shall be given an opportunity to make comments before the report is adopted.

Article 32

Cooperation between National Supervisory Authorities and the European Data Protection Supervisor

1. The National Supervisory Authorities and the European Data Protection Supervisor, each acting within the scope of its respective competences, shall cooperate actively in the framework of their responsibilities and shall ensure coordinated supervision of EURODAC.
2. They shall, each acting within the scope of its respective competences, exchange relevant information, assist each other in carrying out audits and inspections, examine difficulties of interpretation or application of this Regulation, study problems with the exercise of independent supervision or in the exercise of the rights of data subjects, draw up harmonised proposals for joint solutions to any problems and promote awareness of data protection rights, as necessary.

⁸⁹ DE queried about the concept of the term "international auditing standards".

3. The National Supervisory Authorities and the European Data Protection Supervisor shall meet for that purpose at least twice a year. The costs and servicing of these meetings shall be for the account of the European Data Protection Supervisor. Rules of procedure shall be adopted at the first meeting. Further working methods shall be developed jointly as necessary. A joint report of activities shall be sent to the European Parliament, the Council, the Commission and the Agency every two years.

Article 33

Protection of personal data for the purposes of the prevention, detection and investigation of terrorist offences or of other serious criminal offences

1. The Framework Decision 2008/977/JHA is applicable to the processing of relevant personal data for law enforcement purposes under this Regulation.⁹⁰
2. The processing of personal data by Europol pursuant to this Regulation shall be in accordance with Decision 2009/371/JHA.⁹¹

⁹⁰ **DE:** it should be clarified that this provision applies to all fields covered under Art. 1(2), because it is considered that for, example, the notion "law enforcement purposes" covers only repressive measures, but not the "prevention" of offences" as referred to in Art. 1(2). In general, **DE** asked for a clearer wording on when to apply the Framework Decision 2008/977/JHA and when other provisions of this proposal should be taken into account - in addition or as an alternative to the Framework Decision. **Cion** welcomed this suggestion.

⁹¹ **DE:** the supervision of personal data-processing by EUROPOL should be addressed along the lines of Art 10(2) of the 2009 proposal for a Council Decision on requesting comparisons with EURODAC data by MS law enforcement authorities; to this effect, **DE** suggested the following wording: "and shall be supervised by the independent joint supervisory body established by Art.34 of that Decision". **Cion** expressed concerns about this suggestion and indicated that the EURODAC Regulation should not enter into such detail.

3. Personal data obtained pursuant to this Regulation from EURODAC shall only be processed for the purposes of the prevention, detection and investigation of terrorist offences or of other serious criminal offences.
4. Personal data obtained by a Member State or Europol pursuant to this Regulation from EURODAC shall be erased in national and Europol files after a period of one month, if the data are not required for a specific ongoing criminal investigation by that Member State, or Europol.⁹²
5. The monitoring of the lawfulness of the processing of personal data under this Regulation by the Member States, including their transmission to and from EURODAC shall be carried out by the national competent authorities⁹³ designated pursuant to Framework Decision 2008/977/JHA.

⁹² **DE** pointed out that the one-month period for the deletion of the personal data is too short, given that the proceedings are usually long and complex. Moreover these data, once deleted, will not be available for the purpose of subsequent analysis, or data protection control. **Cion** stressed that if certain data are not required for a specific investigation it should be deleted as soon as possible.

⁹³ **DE:** the term “national supervisory authorities” should be used instead of “national competent authorities” for consistency with Art.25 of the Framework Decision 2008/977/JHA. **Cion** welcomed this suggestion.

Article 34

Data security⁹⁴

1. The Member State of origin shall ensure the security of the data before and during transmission to the Central System.⁹⁵
2. Each Member State shall, in relation to its national system, adopt the necessary measures, including a security plan, in order to:
 - (a) physically protect data, including by making contingency plans for the protection of critical infrastructure;⁹⁶
 - (b) deny unauthorised persons access to national installations in which the Member State carries out operations in accordance with the purpose of EURODAC (checks at entrance to the installation);
 - (c) prevent the unauthorised reading, copying, modification or removal of data media (data media control);
 - (d) prevent the unauthorised input of data and the unauthorised inspection, modification or erasure of stored personal data (storage control);

⁹⁴ **SK:** reservation on the Article, pointing out that MS should not be responsible for transferring data at national access points in the network sTesta.

⁹⁵ **DE:** this provision should also include the obligation to ensure data security for the reception of data from the Central System database and from other MS. **Cion:** every data from the Central System is covered by the data protection legislation.

⁹⁶ **CZ:** considers that this point is redundant because it is covered by point (b).

- (e) prevent the unauthorised processing of data in EURODAC and any unauthorised modification or erasure of data processed in EURODAC (control of data entry);
- (f) ensure that persons authorised to access EURODAC have access only to the data covered by their access authorisation, by means of individual and unique user identities and confidential access modes only (data access control);
- (g) ensure that all authorities with a right of access to EURODAC create profiles describing the functions and responsibilities of persons who are authorised to access, enter, update, erase and search the data and make these profiles available to the National Supervisory Authorities referred to in Article 25 of Framework Decision 2008/977/JHA without delay at their request (personnel profiles);⁹⁷
- (h) ensure that it is possible to verify and establish to which bodies personal data may be transmitted using data communication equipment (communication control);
- (i) ensure that it is possible to verify and establish what data have been processed in EURODAC, when, by whom and for what purpose (control of data recording);
- (j) prevent the unauthorised reading, copying, modification or erasure of personal data during the transmission of personal data to or from EURODAC or during the transport of data media, in particular by means of appropriate⁹⁸ encryption techniques (transport control);

⁹⁷ **CZ:** considers that this point is creating disproportionate administrative burden.

⁹⁸ **DE:** the following wording shall be added : « and state-of-the-art »

(k) monitor the effectiveness of the security measures referred to in this paragraph and take the necessary organisational measures related to internal monitoring to ensure compliance with this Regulation (self-auditing).⁹⁹

3. The Agency shall take the necessary measures in order to achieve the objectives set out in paragraph 2 as regards the operation of EURODAC, including the adoption of a security plan.

Article 35

Prohibition of transfers of data to third countries or to international bodies or to private parties¹⁰⁰

Personal data obtained by a Member State or Europol pursuant to this Regulation from the EURODAC central database shall not be transferred or made available to any third country or international organisation or a private entity established in or outside the European Union. This prohibition shall be without prejudice to the right of Member States to transfer such data to third countries to which the Dublin Regulation applies.¹⁰¹

⁹⁹ **CZ:** considers that this point is redundant.

¹⁰⁰ **BE:** scrutiny reservation on the Article, in relation to its concerns for the transfer of personal data to third countries. **BE** agreed with the **Cion**, which pointed out that the prohibition of transfer is related to data received from the Central System and it is an absolute prohibition.

¹⁰¹ **DE:** the following wording should be added: “provided that the requirements of Art. 13 of the Framework Decision 2008/977/JHA are fulfilled and it is guaranteed that the receiving country ensures compliance with the requirements under the first sentence (thereof)”. **FR, AT:** reservation on this Article; **AT** considers it limiting the added value of the proposal. **FR, AT** suggested, alternatively, a ban of transfer of data to the countries of origin, or to provide that data from an asylum procedure cannot be passed. **Cion:** invoked Recital 33 and pointed out that third countries might transmit the data to the countries of origin. **CZ:** scrutiny reservation on the provision, asking for a more flexible wording. **BE:** scrutiny reservation on the Article, in relation to its concerns for the transfer of personal data to third countries.

Article 36

Logging and documentation

1. Each Member State and Europol shall ensure that all data processing operations resulting from requests for comparison with EURODAC data pursuant to this Regulation are logged or documented for the purposes of checking the admissibility of the request monitoring the lawfulness of the data processing and data integrity and security and for self-monitoring.
- ¹⁰²2. The log or documentation shall show in all cases:
 - (a) the exact purpose of the request for comparison, including the concerned form of a terrorist offence or other serious criminal offence and for Europol, the exact purpose of the request for comparison;
 - (b) the respective national file reference;
 - (c) the date and exact time of the request for comparison by the National Access Point to the EURODAC Central System;
 - (d) the name of the authority having requested access for comparison, and the person responsible who has made the request and processed the data;

¹⁰² **CZ:** scrutiny reservation on this paragraph, as it would place disproportionate administrative burden on MS.

(e) where applicable the use of the urgent procedure referred to in Article 19(3) and the decision taken with regard to the ex-post verification;

(f) the data used for comparison;

(g) according to national rules or the rules of the Europol decision the identifying mark of the official who carried out the search and of the official who ordered the search or supply.

3. Such logs or documentation shall be used only for the data protection monitoring of the lawfulness of data processing as well as to ensure data security. Only logs containing non-personal data may be used for the monitoring and evaluation referred to in Article 38. The competent national supervisory authorities responsible for checking the admissibility of the request and monitoring the lawfulness of the data processing and data integrity and security, shall have access to these logs at their request for the purpose of fulfilling their duties.

↓ 2725/2000/EC

⇒ new

Article 37 ~~47~~

Liability

1. Any person who, or Member State which, has suffered damage as a result of an unlawful processing operation or any act incompatible with the provisions laid down in this Regulation shall be entitled to receive compensation from the Member State responsible for the damage suffered. That State shall be exempted from its liability, in whole or in part, if it proves that it is not responsible for the event giving rise to the damage.

2. If failure of a Member State to comply with its obligations under this Regulation causes damage to the ~~central database~~ ⇒ Central System ⇐, that Member State shall be held liable for such damage, unless and insofar as the ~~Commission~~ ⇒ Agency or another Member State ⇐ failed to take reasonable steps to prevent the damage from occurring or to minimise its impact.
 3. Claims for compensation against a Member State for the damage referred to in paragraphs 1 and 2 shall be governed by the provisions of national law of the defendant Member State.
-

↓ new

CHAPTER VIII

AMENDMENTS TO THE REGULATION (EU) No 1077/2011

Article 38

Provisions amending Regulation (EU) No 1077/2011

1. Article 5 is replaced by the following:

“Article 5

Tasks relating to EURODAC

In relation to EURODAC, the Agency shall perform :

- (a) the tasks conferred on the Agency by Regulation (EU) No .../... *[of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No {.../...}]*.
- (b) tasks relating to training on the technical use of EURODAC.”

2. Article 12(1) is amended as follows:

- (a) points (t), (u) and (v) are replaced by the following:

“(t) to adopt the reports on the technical functioning of SIS II pursuant to Article 50(4) of Regulation (EC) No 1987/2006 and Article 66(4) of Decision 2007/533/JHA respectively, of VIS pursuant to Article 50(3) of Regulation (EC) No 767/2008 and Article 17(3) of Decision 2008/633/JHA; and of EURODAC pursuant to Article 40(4) of Regulation (EU) No .../... *[of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No {.../...}]* establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third country national or a stateless person] and to request comparisons with EURODAC data by Member States' law enforcement authorities for law enforcement purposes;

(u) to adopt the annual report on the activities of the Central System of EURODAC pursuant to Article 40(1) of Regulation (EU) No .../... [of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No .../...];

(v) to make comments on the European Data Protection Supervisor's reports on the audits pursuant to Article 45 of Regulation (EC) 1987/2006 , Article 42(2) of Regulation (EC) No 767/2008 and Article 31 (2) of Regulation (EU) No .../... [of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No .../...] and ensure appropriate follow-up of the audit;”

(b) point (x) is replaced by the following:

“(x) to compile statistics on the work of the Central System of EURODAC pursuant to Article 8(2) of Regulation (EU) No .../... [of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No {.../...}]”

(c) point (z) is replaced by the following:

“(z) to ensure annual publication of the list of authorities designated pursuant to Article 27(2) of Regulation (EU) No .../... [of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No .../...]”

3. In Article 15 paragraph (4) is replaced by the following:

“4. Europol and Eurojust may attend the meetings of the Management Board as observers when a question concerning SIS II, in relation to the application of Decision 2007/533/JHA, is on the agenda. Europol may also attend the meetings of the Management Board as observer when a question concerning VIS, in relation to the application of Decision 2008/633/JHA, is on the agenda or when a question concerning EURODAC, in relation with the application of Regulation (EU) No .../... [of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No .../...] is on the agenda.”

4. Article 17 is amended as follows:

(a) in paragraph 5 point (g) is replaced by the following:

“(g) without prejudice to Article 17 of the Staff Regulations, establish confidentiality requirements in order to comply with Article 17 of Regulation (EC) No 1987/2006, Article 17 of Decision 2007/533/JHA and Article 26(9) of Regulation (EC) No 767/2008 respectively and Article 4(6) of Regulation (EU) No .../... [of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No .../...];”

(b) in paragraph 6 point (i) is replaced by the following:

“(i) reports on the technical functioning of each large-scale IT system referred to in point (t) of Article 12(1) and the annual report on the activities of the Central System of EURODAC referred to in point (u) of Article 12(1), on the basis of the results of monitoring and evaluation.”

5. In Article 19 paragraph 3 is replaced by the following:

"3. Europol and Eurojust may each appoint a representative to the SIS II Advisory Group. Europol may also appoint a representative to the VIS and to the EURODAC Advisory Groups." ¹⁰³

↓ 2725/2000/EC (adapted)

⇒ new

CHAPTER ~~VII~~ IX

FINAL PROVISIONS

Article ~~39~~ ~~21~~

Costs

1. The costs incurred in connection with the establishment and operation of the ~~Central Unit~~ ⇒ Central System and the Communication Infrastructure ⇐ shall be borne by the general budget of the European Union.

¹⁰³ SE has concerns for the participation of EUROPOL in the EURODAC Advisory Group and in this sense, the possible influence of EUROPOL on the Dublin Regulation system. **Cion:** the advisory role of the EUROPOL will be limited to law enforcement access' checks.

2. The costs incurred by national ~~access points~~ ~~units~~ and the costs for connection to the ~~central database~~ ~~Central System~~ shall be borne by each Member State.

3. Each Member State and Europol shall set up and maintain at their expense the technical infrastructure necessary to implement this Regulation, and be responsible for bearing its costs resulting from requests for comparison with EURODAC data for the purposes of the prevention, detection or investigation of any of the criminal offences defined in this Regulation.¹⁰⁴

~~3. The costs of transmission of data from the Member State of origin and of the findings of the comparison to that State shall be borne by the State in question.~~

Article ~~40~~ 24

Annual report: ~~m~~Monitoring and evaluation

1. The ~~Commission~~ ~~Agency~~ shall submit to the European Parliament and the Council an annual report on the activities of the Central ~~Unit~~ ~~System~~. The annual report shall include information on the management and performance of ~~Eurodac~~ EURODAC against pre-defined quantitative indicators for the objectives referred to in paragraph 2.

¹⁰⁴ **DE:** reference should also be made to the costs of EUROPOL activities pursuant to Art. 21 of this proposal. Currently, Article 39 (3) provides for the costs incurred in connection with the necessary infrastructure and for “costs resulting from requests for comparison with EURODAC data for the purposes of the prevention, detection or investigation of any of the criminal offences defined in this Regulation”. This provision also expressly covers Europol. However, **DE** considers that there is a loophole caused by the access rights granted to Europol in Article 21. According to this provision, EUROPOL may file requests for comparison with EURODAC data within the limits of its mandate for the purposes of a specific analysis or general and strategic analyses. This also covers cases where comparison does not serve the purposes of prevention, detection or investigation of specific criminal offences. Such cases would not be covered by Article 39 (3).

2. The Commission ⇨ Agency ⇩ shall ensure that ☒ procedures ☒ systems are in place to monitor the functioning of the Central Unit ⇨ System ⇩ against objectives ☒ relating to ☒ in terms of outputs, cost-effectiveness and quality of service.

3. ~~The Commission shall regularly evaluate the operation of the Central Unit in order to establish whether its objectives have been attained cost-effectively and with a view to providing guidelines for improving the efficiency of future operations.~~

4. ~~One year after Eurodac starts operations, the Commission shall produce an evaluation report on the Central Unit, focusing on the level of demand compared with expectation and on operational and management issues in the light of experience, with a view to identifying possible short-term improvements to operational practice.~~

↓ new

3. For the purposes of technical maintenance, reporting and statistics, the Agency shall have access to the necessary information relating to the processing operations performed in the Central System.

4. Every two years, the Agency shall submit to the European Parliament, the Council, the Commission and the European Data Protection Supervisor a report on the technical functioning of the Central System, including the security thereof.

↓ 2725/2000/EC

⇒ new

5. Three years after ~~Eurodac starts operations~~ ⇒ the start of application of this Regulation as provided for in Article 46(2) ⇐ and every ~~six~~ ⇒ four ⇐ years thereafter, the Commission shall produce an overall evaluation of ~~Eurodac~~EURODAC, examining results achieved against objectives and assessing the continuing validity of the underlying rationale, and any implications for future operations ⇒ , as well as make any necessary recommendations ⇐ . ⇒ The Commission shall transmit the evaluation to the European Parliament and the Council. ⇐

↓ new

6. Member States shall provide the Agency and the Commission with the information necessary to draft the reports referred to in paragraph 4 and 5.
7. The Agency shall provide the Commission with the information necessary to produce the overall evaluations referred to in paragraph 5. ¹⁰⁵

¹⁰⁵ **DE:** Para. 7 is redundant, as long as its contents are repeated in para. 9, therefore it should be deleted. **Cion** agreed with this remark.

8. Each Member State and Europol shall prepare annual reports on the effectiveness of the comparison of fingerprint data with EURODAC data for law enforcement access purposes, containing information and statistics on the exact purpose of the comparison, including the type of a terrorist offence or a serious criminal offence, number of requests for comparison, the number and type of cases which have ended in successful identifications and on the need and use made of the exceptional case of urgency as well as on those cases where that urgency was not accepted by the ex post verification carried out by the verifying authority. Such reports shall be transmitted to the Commission.

9. The Agency, Member States and Europol shall provide the Commission the information necessary to draft the evaluation reports referred to in paragraph 5. This information shall not jeopardise working methods nor include information that reveals sources, staff members or investigations of the designated authorities.

↓ 2725/2000/EC (adapted)

⇒ new

Article ~~41~~ 25

Penalties¹⁰⁶

Member States shall ~~take~~ the necessary measures to ensure that any ~~processing use~~ of data recorded ~~entered~~ in the ~~central database~~ Central System ~~contrary to the purpose of Eurodac~~ EURODAC as laid down in Article 1(1)¹⁰⁷ shall be ~~subject to appropriate penalties~~ is punishable by penalties, including administrative and/or criminal penalties in accordance with national law, that are effective, proportionate and dissuasive.

Article ~~42~~ 26

Territorial scope

The provisions of this Regulation shall not be applicable to any territory to which the Dublin ~~Convention~~ Regulation does not apply.

¹⁰⁶ **DE** suggested modifying the wording of the provision as follows: "The MS shall lay down the rules on penalties applicable to infringement of the provisions of this Regulation and shall take all measures necessary to ensure that they are implemented. The penalties provided for must be effective, proportionate and dissuasive"; **DE** pointed out that the current wording penalises any use of data stored in the Central System that is contrary to the purpose of this database, which it considered it too broad and imprecise. **DE** stressed that it cannot agree with the obligation to punish (even with fines and administrative penalties) every infringement of the Regulation (principle of discretionary prosecution).

¹⁰⁷ **FI:** reference should be made also to Art. 1(2), in order to cover the entire scope of the proposal and be in line with the 2009 Commission proposal for a Council Decision on requesting comparisons with EURODAC data by MS law enforcement authorities. **Cion** will check it out.

Article 43

Notification of designated authorities and verifying authorities¹⁰⁸

1. By [three months after the date of entry into force of this Regulation] at the latest each Member State shall notify the Commission of its designated authorities and shall notify without delay any amendment thereto.
2. By [three months after the date of entry into force of this Regulation] at the latest each Member State shall notify the Commission of its verifying authority and shall notify without delay any amendment thereto.
3. By [three months after the date of entry into force of this Regulation] at the latest Europol shall notify the Commission of its verifying authority and the National Access Point which it has designated and shall notify without delay any amendment thereto.
4. The Commission shall publish information referred to in paragraphs 1, 2 and 3 in the *Official Journal of the European Union* on an annual basis.

¹⁰⁸ SE suggested the following modifications to this Article (in relation to those it proposed for Arts 5 and 6):

1. "**Without prejudice to Art. 27(2), each MS shall at the latest... communicate to the Commission its designated authorities for the purpose of law enforcement access and shall communicate... any amendments thereto.**"
2. "**... each MS shall communicate to the Commission its ... for the purpose of law enforcement access and shall communicate... any amendments thereto.**"
3. "**... Europol shall communicate to the Commission its ... and shall communicate... any amendments thereto.**"

Article 44

Transitional provision

Data blocked in the Central System in accordance with Article 12 of Council Regulation (EC) No 2725/2000/EC shall be unblocked and marked in accordance with Article 18(1) of this Regulation on the date provided for in Article 46 of this Regulation.

Article 45

Repeal

Council Regulation (EC) No 2725/2000 of 11 December 2000 and Council Regulation (EC) No 407/2002 are repealed with effect from the date referred to in Article 46(2).

References to the repealed Regulations shall be read in accordance with the correlation table in Annex III.

Article ~~46~~ 27

Entry into force and applicability¹⁰⁹

1. This Regulation shall enter into force on the ☒ twentieth ☒ day ☒ following that ☒ of its publication in the Official Journal of the European ~~Communities~~ ☒ Union ☒.
2. This Regulation shall apply ⇒ two years from the date of the entry into force of this Regulation. ⇐ ~~and Eurodac shall start operations from the date which the Commission shall publish in the Official Journal of the European Communities, when the following conditions met:~~
 - ~~(a) each Member State has notified the Commission that it has made the necessary technical arrangements to transmit data to the Central Unit in accordance with the implementing rules adopted under Article 4(7) and to comply with the implementing rules adopted under Article 12(5); and~~
 - ~~(b) the Commission has made the necessary technical arrangements for the Central Unit to begin operations in accordance with the implementing rules adopted under Article 4(7) and Article 12(5).~~

¹⁰⁹ **FI:** suggested providing for an earlier entry into force of this provision if all requirements are met before. **Cion:** the IT Agency has to be ready in order to have the necessary tests carried out.

↓ new

3. Member States shall notify the Commission and the Agency as soon as they have made the technical arrangements to transmit data to the Central System, and in any event no later than two years from the date of the entry into force of this Regulation.
4. This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaties.

↓ 2725/2000/EC

Done at Brussels,

For the European Parliament
The President

For the Council
The President

↓ 407/2002/EC

⇒ new

ANNEX I

Data format for the exchange of fingerprint data

The following format is prescribed for the exchange of fingerprint data:

~~ANSI/NIST-CSL-1-1993~~ ⇒ ANSI/NIST-ITL 1a-1997, Ver.3, June 2001 (INT-1) ⇐ and any future further developments of this standard.

Norm for Member State identification letters

The following ISO norm will apply: ISO 3166 - 2 letters code.

Annex II

EURODAC – Fingerprint form

1.	Reference number			
2.	Place of the application for asylum or place where the third country national or stateless person was apprehended			
3.	Date of the application for asylum or date on which the third country national or stateless person was apprehended			
4.	Sex			
5.	Date on which the fingerprints were taken			
6.	Date on which the data were transmitted to the Central System			

105 mm from top of form
195 mm from top of form
205 mm from top of form

ROLLED IMPRESSIONS

1. Right thumb	2. Right forefinger	3. Right middle finger	4. Right ring finger	5. Right little finger
6. Left thumb	7. Left forefinger	8. Left middle finger	9. Left ring finger	10. Left little finger

PLAIN IMPRESSIONS

LEFT HAND Four fingers taken simultaneously 	TWO THUMBS Impressions taken simultaneously <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; text-align: center;">LEFT</td> <td style="width: 50%; text-align: center;">RIGHT</td> </tr> <tr> <td style="text-align: center;">30 mm</td> <td style="text-align: center;">30 mm</td> </tr> </table>		LEFT	RIGHT	30 mm	30 mm	RIGHT HAND Four fingers taken simultaneously
	LEFT	RIGHT					
	30 mm	30 mm					



ANNEX II

Repealed Regulations
(referred to in Article 45)

Council Regulation (EC) No 2725/2000/EC (OJ L 316, 15.12.2000, p. 1.)

Council Regulation (EC) No 407/2002/EC (OJ L 062, 05.03.2002 p. 1.)

ANNEX III

Correlation table

Regulation 2725/2000/EC	This Regulation
Article 1(1)	Article 1(1)
Article 1(2), first subparagraph	Article 3(1)
Article 1(2), second subparagraph	Deleted
Article 1(2), third subparagraph	Article 3(4)
Article 1(3)	Article 1(3)
Article 2	Article 2
Article 3(1)	deleted
Article 3(2)	Article 3(3)
Article 3(3)	Article 8
Article 3(4)	Deleted
Article 4(1)	Article 9(1), 3(5)
Article 4(2)	Deleted
Article 4(3)	Article 9(3)
Article 4(4)	Article 9(4)
Article 4(5)	Article 9(5)
Article 4(6)	Article 25(4)
Article 5	Article 11
Article 6	Article 12

Article 7	Article 13
Article 8	Article 14
Article 9	Article 15
Article 10	Article 16
Article 11(1)-(4)	Article 17(1)-(4)
Article 11(5)	Deleted
Article 12	Article 18
Article 13	Article 23
Article 14	Deleted
Article 15	Article 27
Article 16	Article 28
Article 17	Article 37
Article 18	Article 29
Article 19	Article 30
Article 20	Deleted
Article 21	Article 39
Article 22	Deleted
Article 23	Deleted
Article 24	Article 40
Article 25	Article 24
Article 26	Article 42
Article 27	Article 46

Regulation 407/2002/EC

This Regulation

Article 2

Article 24

Article 3

Article 25

Article 4

Article 26

Article 5(1)

Article 3(3)

Annex I

Annex I

Annex II

Deleted



Anlage 4



**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 18 October 2012

14847/12

**Interinstitutional File:
2008/0242 (COD)**



LIMITE

**EURODAC 32
CODEC 2366
ENFOPOL 325**

OUTCOME OF PROCEEDINGS

of::	Permanent Representatives Committee (Part II)
on:	10 October 2012
No. prev. doc.:	14519/12 EURODAC 28 CODEC 2293 ENFOPOL 310
No. Cion prop.:	10638/12 EURODAC 3 ENFOPOL 157 CODEC 1503
Subject:	Amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No [.../...] (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person) and to request comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (Recast version)

On 10 October 2012 the Permanent Representatives Committee endorsed the text which appears in the Annex , as a mandate for the Presidency to engage in a first informal trilogue on the recast of the aforementioned Regulation. The remaining comments of delegations on certain provisions of this draft Regulation are reflected in the footnotes.

New text to the Commission proposal is indicated by underlining the insertion and including it within Council tags: ; deleted text is indicated within underlined square brackets as follows: .

ANNEX

↓ 2725/2000/EC (adapted)

⇒ new

2008/0242 (COD)

Amended proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No [.../...] (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person) and to request comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice¹

(Recast version)

¹ **DE, FI:** general scrutiny reservations on the proposal.

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union ~~establishing the European Community~~, and in particular Article 78 point (2)(e) ~~63 point (1)(a)~~ ⇒ , Article 87 point (2)(a) and Article 88 point (2)(a) ⇐ thereof,

Having regard to the proposal from the Commission²,

Having regard to the opinion of the European Data Protection Supervisor³,

~~Having regard to the opinion of the European Parliament⁴~~

⊗ Acting in accordance with the ordinary legislative procedure, ⊗

Whereas:

² COM(2012) XXX.

³ OJ L 92 10.04.2010, p. 1

⁴ ~~OJ C 189, 7.7.2000, p. 105 and p. 227 and opinion delivered on 21 September 2000 (not yet published in the Official Journal).~~

↓ new

- (1) A number of substantive changes are to be made to Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention⁵ and Council Regulation (EC) No 407/2002 of 28 February 2002 laying down certain rules to implement Regulation (EC) No 2725/2000 concerning the establishment of "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention⁶. In the interest of clarity, those Regulations should be recast.

↓ 2725/2000/EC recital 1

- ~~(1) Member States have ratified the Geneva Convention of 28 July 1951, as amended by the New York Protocol of 31 January 1967, relating to the Status of Refugees.~~

↓ 2725/2000/EC recital 2 (adapted)

- ~~(2) Member States have concluded the Convention determining the State responsible for examining applications for asylum lodged in one of the Member States of the European Communities, signed in Dublin on 15 June 1990 (hereinafter referred to as "the Dublin Convention").~~

⁵ OJ L 316, 15.12.2000, p. 1.

⁶ OJ L 62, 5.3.2002, p. 1.

↓ new

- (2) A common policy on asylum, including a Common European Asylum System, is a constituent part of the European Union's objective of progressively establishing an area of freedom, security and justice open to those who, forced by circumstances, legitimately seek international protection in the Union.
- (3) The European Council of 4 November 2004 adopted The Hague Programme which sets the objectives to be implemented in the area of freedom, security and justice in the period 2005-2010. The European Pact on Immigration and Asylum endorsed by the European Council of 15-16 October 2008 called for the completion of the establishment of a Common European Asylum System by creating a single asylum procedure comprising common guarantees and a uniform status for refugees and the beneficiaries of subsidiary protection.

↓ 2725/2000/EC recital 3 (adapted)

⇒ new

↻ Council

- (4) For the purposes of applying ~~the Dublin Convention~~ Council Regulation (EU) No [...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person]⁷ , it is necessary to establish the identity of applicants for ~~asylum~~ international protection and of persons apprehended in connection with the unlawful crossing of the external borders of the [...] Union⁸ . It is also desirable, in order effectively to apply the ~~Dublin Convention~~ Council Regulation (EU) No [...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] , and in particular points ~~(c) and (e)~~ (b) and (d) of Article ~~10(1)~~18(1) thereof, to allow each Member State to check whether an ~~alien~~ third country national or stateless person found illegally ~~present~~ staying on its territory has applied for ~~asylum~~ international protection in another Member State.

↓ 2725/2000/EC recital 4

- (5) Fingerprints constitute an important element in establishing the exact identity of such persons. It is necessary to set up a system for the comparison of their fingerprint data.

⁷ COM(2008)XXX.

⁸ **Pres** invites the **Cion** to consider agreeing to this change to the wording of the underlying Regulation that had not been originally included in the **Cion's** recast on the basis of the need for consistency within the Regulation.

↓ 2725/2000/EC recital 5

⇒ new

- (6) To this end, it is necessary to set up a system known as "~~Eurodac~~EURODAC", consisting of a Central ~~Unit~~ ⇒ System ⇐, ~~to be established within the Commission and~~ which will operate a computerised central database of fingerprint data, as well as of the electronic means of transmission between the Member States and the ~~central database~~ ⇒ Central System, hereinafter the "Communication Infrastructure". ⇐

↓ new

➡ Council

- (7) The Hague Programme called for the improvement of access to existing data filing systems in the European Union. In addition, The Stockholm Programme called for well targeted data collection and a development of information exchange and its tools that is driven by law enforcement needs.
- (8) It is essential in the fight against terrorist offences and other serious criminal offences for the law enforcement authorities to have the fullest and most up-to-date information if they are to perform their tasks. The information contained in EURODAC is necessary for the purposes of the prevention, detection and investigation of terrorist offences and ➡ of ➡ other serious criminal offences. Therefore, the data in EURODAC should be available, subject to the conditions set out in this Regulation, for comparison by the designated authorities of Member States and Europol.

(9) The Commission outlined in its Communication to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European data bases in the area of Justice and Home Affairs⁹ of 24 November 2005 that authorities responsible for internal security could have access to EURODAC in well defined cases, when there would be a substantiated suspicion that the perpetrator of a terrorist or other serious criminal offence has applied for asylum. In this Communication the Commission also found that the proportionality principle requires that EURODAC be queried for these purposes only once there is an overriding public security concern, that is, if the act committed by the criminal or terrorist to be identified is so reprehensible that it justifies querying a database that registers persons with a clean criminal record and it concluded that the threshold for authorities responsible for internal security to query EURODAC must therefore always be significantly higher than the threshold for querying criminal databases.

(10) Moreover, Europol has a key role with respect to cooperation between Member States' authorities in the field of cross-border crime investigation in supporting Union-wide crime prevention, analyses and investigation. Consequently, Europol should also have access to EURODAC data within the framework of its tasks and in accordance with the Decision establishing the European Police Office (Europol) No (2009/371/JHA).¹⁰

⁹ COM(2005) 597, 24.11.2005.

¹⁰ OJ L 121, 15.5.2009, p. 37

(11) Since EURODAC has been established to facilitate the application of Council Regulation (EU) No [...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], access to EURODAC for the purposes of preventing, detecting [...] and [...] investigating terrorist offences and [...] of [...] other serious criminal offences constitutes a change of the original purpose of EURODAC, which interferes with the right to respect the private life of individuals whose personal data are processed in EURODAC. Any such interference must be in accordance with the law, which must be formulated with sufficient precision to allow individuals to adjust their conduct and it must protect individuals against arbitrariness and indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise. Any interference must be necessary in a democratic society to attain a legitimate and proportionate interest and proportionate to the legitimate objective it aims to achieve.

(12) Even though the original purpose for the establishment of EURODAC did not require the facility of requesting comparisons of data with the database on the basis of a latent which is the dactyloscopic trace which may be found at a crime scene, such a facility is a fundamental one in the field of police cooperation. The possibility to compare a latent with the fingerprint data which is stored in EURODAC will provide the designated authorities of the Member States with a very valuable tool in preventing, detecting and investigating terrorist offences and other serious criminal offences, when for example the only evidence available at a crime scene are latents.

~~(13) Since the Member States alone are responsible for identifying and classifying the results of comparisons transmitted by the Central Unit as well as for the blocking of data relating to persons admitted and recognised as refugees and since this responsibility concerns the particularly sensitive area of the processing of personal data and could affect the exercise of individual freedoms, there are specific grounds for the Council reserving for itself the exercise of certain implementing powers, relating in particular to the adoption of measures ensuring the safety and reliability of such data.~~

(13) This Regulation also lays down the conditions under which requests for comparison of fingerprint data with EURODAC data for the purposes of preventing, detecting or investigating terrorist offences and other serious criminal offences should be allowed and the necessary safeguards to ensure the protection of the fundamental right to respect for the private life of individuals whose personal data are processed in EURODAC.=

~~(14) The measures necessary for the implementation of other measures of this Regulation should be adopted in accordance with Council Decision 1999/468/EC of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission(3).~~

(14) In view of ensuring equal treatment for all applicants and beneficiaries of international protection, as well as in order to ensure consistency with current Union asylum acquis, in particular with Council Directive 2004/83/EC of 29 April 2004 on minimum standards for the qualification and status of third country nationals or stateless persons as refugees or as persons who otherwise need international protection and the content of the protection granted¹¹ and Regulation (EU) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], it is appropriate to extend the scope of this Regulation to order to include applicants for subsidiary protection and persons enjoying subsidiary protection.

¹¹ OJ L 304, 30.9.2004, p. 12.

↓ 2725/2000/EC recital 6 (adapted)

⇒ new

- (15) It is also necessary to require the Member States promptly to take ⇒ and transmit ⇐ fingerprints ⇒ data ⇐ of every applicant for ~~asylum~~ ⇒ international protection ⇐ and of every ~~alien~~ ⊗ third country national or stateless person ⊗ who is apprehended in connection with the irregular crossing of an external border of a Member State, if they are at least 14 years of age.

↓ 2725/2000/EC recital 7 (adapted)

⇒ new

- (16) It is necessary to lay down precise rules on the transmission of such fingerprint data to the Central ~~Unit~~ ⇒ System ⇐, the recording of such fingerprint data and other relevant data in the Central ~~Unit~~ ⇒ System ⇐, their storage, their comparison with other fingerprint data, the transmission of the results of such comparison and the ~~blocking~~ ⇒ marking ⇐ and erasure of the recorded data. Such rules may be different for, and should be specifically adapted to, the situation of different categories of ~~aliens~~ ⊗ third country nationals or stateless persons ⊗.

↓ new

↻ Council

- (17) Hits obtained from EURODAC should be verified by a fingerprint expert in order to ensure the accurate determination of responsibility under Regulation (EU) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] ↻ and the exact identification of the criminal suspect or victim of crime whose data might be stored in EURODAC ↻ .
-

↓ 2725/2000/EC recital 8 (adapted)

⇒ new

- (18) ~~Aliens~~ ⊗ Third country nationals or stateless persons ⊗ who have requested ~~asylum~~ ⇒ international protection ⇐ in one Member State may have the option of requesting ~~asylum~~ ⇒ international protection ⇐ in another Member State for many years to come. Therefore, the maximum period during which fingerprint data should be kept by the Central ~~Unit~~ ⇒ System ⇐ should be of considerable length. Given that most ~~aliens~~ ⊗ third country nationals or stateless persons ⊗ who have stayed in the ~~Community~~ ⊗ European Union ⊗ for several years will have obtained a settled status or even citizenship of a Member State after that period, a period of ten years should be considered a reasonable period for the conservation of fingerprint data.

↓ 2725/2000/EC recital 9 (adapted)

- (19) The conservation period should be shorter in certain special situations where there is no need to keep fingerprint data for that length of time. Fingerprint data should be erased immediately once ~~aliens~~ ☒ third country nationals or stateless persons ☒ obtain citizenship of a Member State.
-

↓ new

↻ Council

- (20) It is appropriate to store data relating to those data subjects whose fingerprints were initially recorded in EURODAC upon lodging their applications for international protection and who have been granted international protection in a Member State in order to allow data recorded upon lodging an application for international protection to be compared against them.

- ~~(20) The United Kingdom and Ireland, in accordance with Article 3 of the Protocol on the position of the United Kingdom and Ireland annexed to the Treaty on European Union and the Treaty establishing the European Community, have given notice of their wish to take part in the adoption and application of this Regulation.~~

(21) The European Agency for the operational management of large-scale information systems in the area of freedom, security and justice established by Regulation (EU) n° 1077/2011 of the European Parliament and of the Council of 25 October 2011¹² (the "Agency") has been entrusted with the Commission's tasks relating to the operational management of EURODAC in accordance with this Regulation and with certain tasks relating to the communication infrastructure as from the date on which the Agency takes up its responsibilities as of 1 December 2012. The Agency should take up the tasks entrusted to it under this Regulation and the relevant provisions of Regulation (EU) No 1077/2011 should be amended accordingly. In addition, Europol should have observer status at the meetings of the Management Board of the Agency, when a question in relation to the application of this Regulation concerning access for consultation of Eurodac by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences is on the agenda. Europol should be able to appoint a representative to the Eurodac Advisory Group of the Agency.

(22) The Staff Regulations of Officials of the European Union (Staff Regulations of Officials) and the Conditions of Employment of Other Servants of the European Union (Conditions of Employment), laid down in Regulation (EEC, Euratom, ECSC) No 259/68 (15) (together referred to as the 'Staff Regulations'), should apply to all staff working in the Agency on matters pertaining to this Regulation.

~~(23) This Regulation should serve as legal basis for the implementing rules which, with a view to its rapid application, are required for the establishment of the necessary technical arrangements by the Member States and the Commission. The Commission should be charged with verifying that those conditions are fulfilled.~~

¹² OJ L 286, 1.11.2011, p. 1.

↓ 2725/2000/EC recital 10 (adapted)

⇒ new

- (23) It is necessary to lay down clearly the respective responsibilities of the Commission ⇒ and the Agency ⇐, in respect of the Central-Unit ⇐ System ⇐ ⇐ and the Communication Infrastructure ⇐, and of the Member States, as regards data ~~use~~ processing, data security, access to, and correction of, recorded data.

↓ new

⇒ Council

- (24) It is necessary to designate the competent Member States' authorities as well as the National Central Access Point through which the requests for comparison with EURODAC data are ⇒ [...] ⇐ ⇒ made ⇐ and to keep a list of the operating units within the designated authorities that are authorised to request such comparison for the specific purposes of the prevention, detection and investigation of terrorist offences as referred to in the Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism¹³ and of other serious criminal offences as referred to in the Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States¹⁴.

¹³ OJ L 164, 22.6.2002, p. 3.

¹⁴ OJ L 190, 18.7.2002, p. 1.

(25) Requests for comparison with data stored in the EURODAC central database shall be made by the operating units within the designated authorities to the National Access Point, through the verifying authority and shall be reasoned. The operating units within the designated authorities that are authorised to request comparisons with EURODAC data shall not act as a verifying authority. The verifying authorities should be responsible for ensuring ~~☐~~, in an independent manner, ~~☐~~ strict compliance with the conditions for access as established in this Regulation. The verifying authorities should then forward the request ~~☐~~ without forwarding the reasons for it, ~~☐~~ for comparison through the National Access Point to the EURODAC Central System following verification of whether all conditions for access are fulfilled. In the exceptional case of urgency ~~☐~~, ~~☐~~ where early access is necessary to respond to a specific and actual threat related to terrorist offences or serious crime, the verifying authority should process the request immediately and only do the verification afterwards.¹⁵

¹⁵ **CZ:** reservation on this Recital, in relation with its concerns about the concept of verifying authorities.

(26) For the purposes of protection of personal data, and to exclude systematic comparisons which should be forbidden, the processing of EURODAC data should only take place on a case-by-case basis and when it is necessary for the purposes of preventing, detecting and investigating terrorist offences and other serious criminal offences. In addition access should only be allowed when comparisons with the national databases of the Member State and with the Automated Fingerprint Databases of other Member States under the Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime¹⁶ did not lead to the establishment of the identity of the data subject. This condition requires the Member State to conduct a comparison with the Automated Fingerprint Database of another Member State under Council Decision 2008/615/JHA and all further comparisons with other Member States under the Council Decision that are necessary and technically available. The comparison with the Automated Fingerprint Databases of another Member State is **not** necessary in a specific case if there are **no** reasonable grounds to consider that this comparison will contribute to the prevention, detection or investigation of any of the criminal offences in question. This condition requires prior legal and technical implementation of the Council Decision by the Member State in the area of fingerprint data, as it shall not be permitted to conduct a EURODAC check for law enforcement purposes where these above steps have not been first undertaken. A specific case exists in particular when the request for comparison is connected to a specific and concrete situation or to a specific and concrete danger associated with a terrorist or other serious criminal offence, or to specific persons in respect of whom there are serious grounds for believing that the persons will commit or have committed terrorist offences or other serious criminal offences. A specific case also exists when the request for comparison is connected to a person who is a victim of a terrorist or other serious criminal offence. The designated authorities and Europol should thus only request a comparison with EURODAC when they have reasonable grounds to believe that such a comparison will provide information that will substantially assist them in preventing, detecting or investigating a terrorist or other serious criminal offence.

¹⁶ OJ L 210, 6.8.2008, p. 1.

(27) In case the requesting Member State establishes that EURODAC data pertains to a minor, these data may only be used for law enforcement purposes by the requesting Member State in accordance with that State's laws for minors and in accordance with the obligation to give primary consideration to the child's best interest.

↓ 2725/2000/EC recital 11

↻ Council

(28) While the non-contractual liability of the ↻ [...] ↻ ↻ Union¹⁷ ↻ in connection with the operation of the ~~Eurodac~~EURODAC system will be governed by the relevant provisions of the Treaty, it is necessary to lay down specific rules for the non-contractual liability of the Member States in connection with the operation of the system.

↓ 2725/2000/EC recital 12

↻ Council

(29) In accordance with the principle of subsidiarity as set out in Article 5 of the Treaty ↻ on the European Union ↻, the objective of the proposed measures, namely the creation ~~within the Commission~~ of a system for the comparison of fingerprint data to assist the implementation of the ↻ [...] ↻ ↻ Union's¹⁸ ↻ asylum policy, cannot, by its very nature, be sufficiently achieved by the Member States and can therefore be better achieved by the ↻ [...] ↻ ↻ Union ↻. In accordance with the principle of proportionality as set out in the said Article, this Regulation does not go beyond what is necessary to achieve ~~that~~ those objectives.

¹⁷ Pres invites the Cion to consider agreeing to this change to the wording of the underlying Regulation that had not been originally included in the Cion's recast on the basis of the need for consistency within the Regulation.

¹⁸ Pres invites the Cion to consider agreeing to this change to the wording of the underlying Regulation that had not been originally included in the Cion's recast on the basis of the need for consistency within the Regulation.

↓ 2725/2000/EC recital 15 (adapted)

⇒ new

↻ Council

- (30) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data¹⁹ applies to the processing of personal data by the Member States ~~carried out in application of this Regulation within the framework of the Eurodac system~~ ⇒ unless such processing takes place by Member States' ⇒ [...] authorities for the purposes of the prevention, detection and investigation of terrorist offences and ⇒ of other serious criminal offences ⇐.

↓ new

↻ Council

- (31) ⇒ [...] The processing of personal data by Member States' ⇒ [...] authorities for the purposes of the prevention, detection and investigation of terrorist offences and ⇒ of other serious criminal offences pursuant to this Regulation ⇒ should be subject to a standard of protection of personal data under their national law which is in line with Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters. ⇐ .

¹⁹ OJ L 281, 23.11.1995, p. 31.

↓ 2725/2000/EC recital 16

~~(16) By virtue of Article 286 of the Treaty, Directive 95/46/EC also applies to Community institutions and bodies. Since the Central Unit will be established within the Commission, that Directive will apply to the processing of personal data by that Unit.~~

↓ 2725/2000/EC recital 17

(32) The principles set out in Directive 95/46/EC regarding the protection of the rights and freedoms of individuals, notably their right to privacy, with regard to the processing of personal data should be supplemented or clarified, in particular as far as certain sectors are concerned.

↓ new

☞ Council

(33) Transfers of data obtained pursuant to this ☞ [...] ☞ ☞ Regulation ☞ to third countries or international organisations or private entities should be prohibited, in order to ensure the right to asylum and to safeguard applicants for international protection from having their data disclosed to any third country. This prohibition shall be without prejudice to the right of Member States to transfer such data to third countries to which Regulation (EU) No [...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] applies, in order to ensure that Member States have the possibility of cooperating with such third countries for the purposes of this Regulation.

- (34) National [...] supervisory authorities [...] should monitor the lawfulness of the processing of personal data by the Member States, and the supervisory authority set up by the Europol Decision should monitor the lawfulness of data processing activities performed by Europol.
- (35) Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data²⁰ and in particular Articles 21 and 22 thereof concerning confidentiality and security of processing apply to the processing of personal data by Union institutions, bodies, offices and agencies carried out in application of this Regulation. However, certain points should be clarified in respect of the responsibility for the processing of data and of the supervision of data protection.
- (36) It is appropriate that national supervisory authorities monitor the lawfulness of the processing of personal data by the Member States, whilst the European Data Protection Supervisor, as referred to in Article 41 of Regulation (EC) No 45/2001, should monitor the activities of the Union institutions, bodies, offices and agencies in relation to the processing of personal data carried out in application of this Regulation.

²⁰ OJ L 8, 12.1.2001, p. 1.

↓ 2725/2000/EC recital 18

⇒ new

- (37) It is appropriate to monitor and evaluate the performance of ~~Eurodac~~EURODAC ⇒ at regular intervals ⇐.²¹
-

↓ 2725/2000/EC recital 19 (adapted)

⇒ new

- (38) Member States should provide for a system of effective, proportionate and dissuasive penalties to sanction the processing use of data entered in the ~~central database~~ ⇒ Central System ⇐ contrary to the purpose of ~~Eurodac~~EURODAC.
-

↓ new

- (39) It is necessary that Member States are informed of the status of particular asylum procedures, with a view to facilitating the adequate application of Regulation (EU) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person].

²¹ **BE:** suggested the following amendment in order to ensure that due attention is paid to the evaluation of whether or not the operation of the search functionality for law enforcement purposes will lead to the stigmatisation of persons seeking international protection or not; the evaluation should also look at the effect of the access to Eurodac for law enforcement purposes on the protection of personal data.
It is appropriate to monitor and evaluate at regular intervals the performance **and results** of EURODAC. **This should also include an evaluation of the effect of the search functionality for law enforcement purposes on data protection and whether it has led to the stigmatization of asylum seekers.**

- (40) This Regulation respects and has to be applied in accordance with fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union. In particular, this Regulation fully respects the individual's right to protection of his or her personal data and the right to asylum.
- (41) In accordance with Articles 1 and 2 of the Protocol on the position of Denmark annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application. As regards Denmark, this Regulation, with the exception of the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43, constitutes amendment to the EURODAC Regulation within the meaning of the Agreement between the European Community and the Kingdom of Denmark on the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in Denmark or any other Member State of the European Union and 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention²². Consequently, in accordance with Article 3 thereof, Denmark is to notify the Commission whether it will implement the contents of this Regulation and when it does so, this Regulation creates mutual obligations under international law between Denmark and the European Union. Once this Recast Regulation is adopted and subject to a Commission recommendation for a Council Decision authorising the opening of negotiations, Denmark will be consulted as to whether it wishes to enter into negotiations on complementary agreements also covering the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43.

²² OJ L 66, 8.3.2006, p. 38.

- (42) In accordance with Article 3 of the Protocol on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, and without prejudice to Article 4 of that Protocol, the United Kingdom *[is not taking part in the adoption of this Regulation and is not bound by it or subject to its application / has notified its wish to take part in the adoption and application of this Regulation]*.
- (43) In accordance with Article 3 of the Protocol on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, and without prejudice to Article 4 of that Protocol, Ireland *[is not taking part in the adoption of this Regulation and is not bound by it or subject to its application / has notified its wish to take part in the adoption and application of this Regulation]*.
- (44) As regards the Republic of Iceland and the Kingdom of Norway, this Regulation, with the exception of the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43, constitutes a new measure related to EURODAC within the meaning of the Agreement between the European Community and the Republic of Iceland and the Kingdom of Norway concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Iceland or Norway²³. Consequently, subject to their decision to implement it in their internal legal order, this Regulation shall be applied between the Republic of Iceland and the Kingdom of Norway in their mutual relations and in their relations with the Member States of the European Union. Once this Recast Regulation is adopted and subject to a Commission recommendation for a Council Decision authorising the opening of negotiations, the Republic of Iceland and the Kingdom of Norway will be consulted as to whether they wish to enter into negotiations on complementary agreements also covering the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43.

²³ OJ L 93, 3.4.2001, p. 40.

(45) As regards the Swiss Confederation, this Regulation, with the exception of the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43, constitutes a new measure related to EURODAC within the meaning of the Agreement between the European Community and the Swiss Confederation concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Switzerland²⁴. Consequently, subject to its decision to implement it in its internal legal order, this Regulation shall be applied between the Swiss Confederation and the Member States of the European Union. Once this Recast Regulation is adopted and subject to a Commission recommendation for a Council Decision authorising the opening of negotiations, the Swiss Confederation will be consulted as to whether it wishes to enter into negotiations on complementary agreements also covering the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43, subject to a separate agreement on the application of relevant provisions of Council Decision 2008/615/JHA on the stepping up of cross-border cooperation.

²⁴ OJ L 53, 27.2.2008, p. 5

(46) As regards the Principality of Liechtenstein, this Regulation, with the exception of the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43, constitutes a new measure related to EURODAC within the meaning of the Protocol between the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Community and the Swiss Confederation concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Switzerland²⁵. Consequently, subject to its decision to implement it in its internal legal order, this Regulation shall be applied between the Principality of Liechtenstein, the Swiss Confederation and the Member States of the European Union. Once this Recast Regulation is adopted and subject to a Commission recommendation for a Council Decision authorising the opening of negotiations, the Principality of Liechtenstein will be consulted as to whether it wishes to enter into negotiations on complementary agreements also covering the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43, subject to a separate agreement on their application of relevant provisions of Council Decision 2008/615/JHA on the stepping up of cross-border cooperation.

↓ 2725/2000/EC recital 22 (adapted)

(47) It is appropriate to restrict the territorial scope of this Regulation so as to align it on the territorial scope of ~~the Dublin Convention~~ Regulation (EU) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] .

²⁵ OJ L 160, 18.6.2011, p. 39.

↓ 2725/2000/EC (adapted)

⇒ new

↻ Council

HAVE ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS

Article 1

Purpose of "~~Eurodac~~EURODAC"

1. A system known as "~~Eurodac~~EURODAC" is hereby established, the purpose of which shall be to assist in determining which Member State is to be responsible pursuant to ~~the Dublin Convention~~ Regulation (EU) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] for examining an application for ~~asylum~~ international protection lodged in a Member State by a third country national or a stateless person , and otherwise to facilitate the application of the Dublin ~~Convention~~ Regulation under the conditions set out in this Regulation.

~~For the purposes of this Regulation:~~

~~(a) "Central Unit" shall mean the unit referred to in Article 1(2)(a) of the Eurodac Regulation;~~

~~(b) "database" shall mean the computerised central database referred to in Article 1(2)(b) of the Eurodac Regulation;~~

~~(c) "comparison" shall mean the procedure of checking whether fingerprint data recorded in the database match those transmitted by a Member State.~~

~~2. Eurodac shall consist of:~~

~~(a) the Central Unit referred to in Article 3;~~

~~(b) a computerised central database in which the data referred to in Article 5(1), Article 8(2) and Article 11(2) are processed for the purpose of comparing the fingerprint data of applicants for asylum and of the categories of aliens referred to in Article 8(1) and Article 11(1);~~

~~(c) means of data transmission between the Member States and the central database.~~

2. This Regulation also lays down the conditions under which Member States' designated authorities and the European Police Office (Europol) may request the comparison of fingerprint data with those stored in the EURODAC central database for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences (“law enforcement purposes”).²⁶

²⁶ **DE** suggested adding at the end of the text: “... including averting individual dangers”. **BE**, considering that the terms “prevention, detection and investigation” are not defined in the proposal and in order to better demarcate the scope of the access to EURODAC for law enforcement authorities and avoid abuses, suggested amending the end of the sentence as follows: “... for the purposes of **conducting criminal investigations or criminal intelligence operations into terrorist offences and other serious criminal offences**”, thus drawing on the Framework Decision 2006/960 JHA. In this vein, **BE** suggested defining “criminal investigation” and “criminal intelligence operation”- see under Art. 2(1) - and adapting accordingly the relevant wording throughout the proposal. **Pres**: recalled that Recital 24 contains references to the definitions of terrorist offences (Council Framework Decision 2002/475/JHA) and of serious criminal offences (Council Framework Decision 2002/584/JHA). **EL, ES, HU, PT, SI, SK, UK** (these delegations preferred the **Pres** text), as well as **CZ, SE**: scrutiny reservations on this **BE** suggestion and the ensuing new definitions under Art. 2(1)(m) and (n). These delegations stressed, mainly, that the current wording does not define loosely the scope and hence, there is no aggravated risk of abuse of the access to law enforcement authorities. **FR** could live with both the **Pres** and the **BE** options. **Cion**, supported its own proposal and could not agree with the **BE** suggestion, pointing out (along with **CZ, HU**) that the Framework Decision 2006/960 provides for a different legal context, which does not tally with the hit/no-hit basis of EURODAC. **Cion** also recalled that the safeguard provided for under draft Art. 20(1)(b), preventing systematic search, counters effectively the risk of extended abuse through the “prevention” element of the scope. **BE** underlined that its main objective is to avoid linking at a premature stage an all too widely interpreted concept of prevention with a possible offence and thought that despite the Art. 20(1) safeguard this could still end up happening.

↓ 2725/2000/EC (adapted)

⇒ new

3. Without prejudice to the processing use of data intended for ~~Eurodac~~ EURODAC by the Member State of origin in databases set up under the latter's national law, fingerprint data and other personal data may be processed in ~~Eurodac~~ EURODAC only for the purposes set out in ⇒ this Regulation and ⇐ Article ~~15(1)~~ 32(1) of the Dublin ~~Convention~~ Regulation ⇔ .
-

↓ 2725/2000/EC (adapted)

⇒ new

⇒ Council

Article 2

Definitions

1. For the purposes of this Regulation:
- (a) "the Dublin ~~Convention~~ ⇔ Regulation ⇔ " means the ~~Convention determining the State responsible for examining applications for asylum lodged in one of the Member States of the European Communities, signed at Dublin on 15 June 1990~~ ⇔ Regulation (EU) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] ⇔;

(b) an "applicant for ~~asylum~~ ⇒ international protection ⇐" means an ~~alien~~ ⊗ third-country national or a stateless person ⊗ who has made an application for ~~asylum or on whose behalf such an application has been made~~ ⇒ international protection as defined in Article 2(g) of Council Directive 2004/83/EC in respect of which a final decision has not yet been taken ⇐;

²⁷(c) "Member State of origin" means:

- (i) in relation to an ~~applicant for asylum~~ ⊗ person covered by Article 9 9 9 [...] 9 ⊗, the Member State which transmits the personal data to the Central ~~Unit~~ ⇒ System ⇐ and receives the results of the comparison;
- (ii) in relation to a person covered by Article 8 9 [...] 9 9 14 9, the Member State which transmits the personal data to the Central ~~Unit~~ ⇒ System ⇐;
- (iii) in relation to a person covered by Article 11 9 [...] 9 9 17 9, the Member State which transmits such data to the Central ~~Unit~~ ⇒ System ⇐ and receives the results of the comparison;

↓ 2725/2000/EC (adapted)

⇒ new

↻ Council

(d) ~~"refugee"~~ ⇒ "person granted international protection" ⇐ means a ⊗ third country national or a stateless ⊗ person ~~who has been~~ recognised as ~~a refugee in accordance with the Geneva Convention on Refugees of 28 July 1951, as amended by the New York Protocol of 31 January 1967~~ ⇒ entitled to international protection as defined in point (a) of Article 2 of Council Directive 2004/83/EC ⇐;

²⁷

In relation to the corrections on this provision, **Pres** invites the **Cion** to consider agreeing to this change to the wording of the underlying Regulation that had not been originally included in the **Cion's** recast on the basis of the need for consistency within the Regulation.

- (e) "hit" shall mean the existence of a match or matches established by the Central ~~Unit~~
⇒ System ⇐ by comparison between fingerprint data recorded in the ~~database~~
⊗ central database ⊗ and those transmitted by a Member State with regard to a
person, without prejudice to the requirement that Member States shall immediately
check the results of the comparison pursuant to Article ~~4(6)~~ ⇒ [...] ⇐ ⇒ 25 ⇐ (4);²⁸

↓ new

⇒ Council

- (f) "National ⇒ [...] ⇐ ⇒ Access ⇐ Point" means the designated national system which
communicates with the Central System;
- (g) "Agency" means the Agency established by Regulation (EU) No 1077/2011;
- (h) 'Europol' means the European Police Office as established by Decision
2009/371/JHA;
- (i) 'EURODAC data' means all ⇒ [...] ⇐ data stored in the central database in
accordance with Article 11 and Article ⇒ [...] ⇐ ⇒ 14 ⇐ (2);
- (j) 'terrorist ⇒ -related ⇐ offences' means the offences under national law which
correspond or are equivalent to the offences referred to in Articles 1 to 4 of
Framework Decision 2002/475/JHA;
- (k) 'serious criminal offences' means the forms of crime which correspond or are
equivalent to those referred to in Article 2(2) of Framework Decision 2002/584/JHA
if they are punishable by a custodial sentence or a detention order for a maximum
period of at least three years under national law;

²⁸ Pres invites the Cion to consider agreeing to this change to the wording of the underlying Regulation that had not been originally included in the Cion's recast on the basis of the need for consistency within the Regulation.

- (l) 'fingerprint data' means the data relating to fingerprints of all or at least the index fingers, and if those are missing, the prints of all other fingers of a person, or a latent.

↓ 2725/2000/EC (adapted)

⇒ new

⇒ Council

29

2. The terms defined in Article 2 of Directive 95/46/EC shall have the same meaning in this Regulation ⇒ unless the processing of personal data takes place by Member States' ⇒ [...] authorities for the purposes of the prevention, detection and investigation of terrorist offences and ⇒ of other serious criminal offences ⇐.
3. Unless stated otherwise, the terms defined in Article 1 2 of the Dublin ~~Convention~~ Regulation ⊗ shall have the same meaning in this Regulation.

29 BE in accordance with its suggestions on Art. 1(2), suggested the following additional definitions:

(m) "Criminal Investigation" means a procedural stage within which measures are taken by competent law enforcement or judicial authorities, including public prosecutors, with a view to establishing and identifying facts, suspects and circumstances regarding one or several concrete criminal acts.

(n) "Criminal intelligence operation" means a procedural stage, not yet having reached the stage of a criminal investigation, within which a competent law enforcement authority is entitled by national law, to collect, process and analyse information about crime or criminal activities with a view to establishing whether concrete criminal acts have been committed or may be committed in the future. (see relevant comments from delegations under footnote 26).

↓ new

☞ Council

4. The terms defined in Article 2 of the Framework Decision 2008/977/JHA shall have the same meaning in this Regulation in so far as personal data are processed by Member States' [...] authorities for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences pursuant to this Regulation.

↓ 2725/2000/EC (adapted)

Article 3

~~Central Unit~~ ☒ System architecture and basic principles ☒

~~1. A Central Unit shall be established within the Commission which shall be responsible for operating the central database referred to in Article 1(2)(b) on behalf of the Member States. The Central Unit shall be equipped with a computerised fingerprint recognition system.~~

↓ new

1. EURODAC shall consist of:

(a) a computerised central fingerprint database (Central System) composed of

– a Central Unit,

– a Business Continuity System.

(b) a communication infrastructure between the Central System and Member States that provides an encrypted virtual network dedicated to EURODAC data (Communication Infrastructure).

2. Each Member State shall have a single National Access Point.

↓ 2725/2000/EC (adapted)

⇒ new

2.3. Data on ~~applicants for asylum~~, persons covered by Articles ~~8~~ and persons covered by ~~Article 14~~ 9, 14 and 17 which are processed in the Central ~~Unit~~ ⇒ System ⇐ shall be processed on behalf of the Member State of origin under the conditions set out in this Regulation ☒ and separated by appropriate technical means ☒.

↓ 2725/2000/EC Article 1(2) third subparagraph

⇒ new

4. The rules governing ~~Eurodac~~ EURODAC shall also apply to operations effected by the Member States as from the transmission of data to the Central ~~Unit~~ ⇒ System ⇐ until use is made of the results of the comparison.

↓ 2725/2000/EC Article 4(1) second sentence

⇒ new

5. The procedure for taking fingerprints shall be determined ⇒ and applied ⇐ in accordance with the national practice of the Member State concerned and in accordance with the safeguards laid down in ⇒ the Charter of Fundamental Rights of the European Union, in the Convention for the Protection of Human Rights and Fundamental Freedoms and ⇐ ~~the European Convention on Human Rights and~~ in the United Nations Convention on the Rights of the Child.
-

↓ new

Article 4

Operational management

1. The Agency, shall be responsible for the operational management of EURODAC. The Agency shall ensure, in cooperation with the Member States, that at all times the best available technology, subject to a cost-benefit analysis, is used for the Central System.
2. The Agency shall also be responsible for the following tasks relating to the Communication Infrastructure:
 - (a) supervision;
 - (b) security;
 - (c) the coordination of relations between the Member States and the provider.

3. The Commission shall be responsible for all other tasks relating to the Communication Infrastructure, in particular:
 - (a) tasks relating to implementation of the budget;
 - (b) acquisition and renewal;
 - (c) contractual matters.
4. Before the Agency takes up its responsibilities, the Commission shall be responsible for all tasks attributed to the Agency by this Regulation.
5. Operational management of EURODAC shall consist of all the tasks necessary to keep EURODAC functioning 24 hours a day, 7 days a week in accordance with this Regulation, in particular the maintenance work and technical developments necessary to ensure that the system functions at a satisfactory level of operational quality, in particular as regards the time required for interrogation of the Central System.
6. Without prejudice to Article 17 of Regulation No 31 (EEC), 11 (EAEC)³⁰, the Agency shall apply appropriate rules of professional secrecy or other equivalent duties of confidentiality to all its staff required to work with EURODAC data. This obligation shall also apply after such staff leave office or employment or after the termination of their activities.

³⁰ OJ 45, 14.6.1962, p. 1385.

~~Article 5~~

~~Other tasks of the Central Unit~~

- ~~1. The Central Unit shall separate the data on asylum applicants and the data on persons referred to in Article 8 of the Eurodac Regulation which are stored in the database, by appropriate technical means.~~
- ~~2. On the basis of a communication from a Member State, the Central Unit shall give an appropriate distinguishing mark to data on persons who have been recognised and admitted as refugees and shall separate them, by appropriate technical means, from other data recorded in the database. If a decision has been taken in accordance with Article 12(2)(a) of the Eurodac Regulation, the first sentence shall no longer apply. The Central Unit shall remove the existing distinguishing marks and cancel separation of the data.~~
- ~~3. Four years and six months after Eurodac begins its activities, the Central Unit shall draw up statistics in order to indicate:
 - ~~(a) the number of persons who, having been recognised and admitted as refugees in a Member State, have lodged a further application for asylum in another Member State;~~
 - ~~(b) the number of persons who have been recognised and admitted as refugees in more than one Member State;~~
 - ~~(c) the Member States in which the refugees have lodged a further application for asylum, with:~~~~

~~per Member State, the number of applicants for asylum who, having the status of refugee in that State, have applied for asylum in another Member State, and the number of such persons for each of the latter Member States,~~

~~per Member State, the number of applicants for asylum who already have the status of refugee in another Member State, and the number of such persons for each of the latter Member States.~~

~~4. The Central Unit shall ensure that, pursuant to Article 4(4) of the Eurodac Regulation, comparisons carried out at the request of a Member State can also cover the data transmitted by that particular Member State at an earlier time.~~

↓ new

☞ Council

Article 5

Designated Authorities for the purpose of law enforcement access

1. ☞ For the purposes as laid down in Article 1(2) ☹ Member States shall designate the authorities which are authorised to access EURODAC data pursuant to this Regulation. Designated authorities shall be authorities of the Member States which are ☞ [...] ☹ ☞ competent ☹ for the prevention, detection ☞ [...] ☹ ☞ and ☹ investigation of terrorist offences ☞ [...] ☹ ☞ or ☹ other serious criminal offences.³¹
2. Every Member State shall keep a list of the designated authorities.
3. At national level, each Member State shall keep a list of the operating units within the designated authorities that are authorised to request comparisons with EURODAC data through the National Access Point.

³¹ **BE:** the scope of the term “competent authorities” should not be expanded.
DE: the following sentence, which was included in Art. 3(1) of the 2009 proposal for a Council Decision on requesting comparisons with EURODAC data by MS law enforcement authorities - and was agreed during those negotiations among delegations, should be added in this provision: “Designated authorities shall not include agencies or units dealing especially with national security issues”. **NL, Cion** could agree with this suggestion. **BG, EE, EL, ES, FR, IE, AT, PT, RO, SE, SI, UK:** reservations or concerns on the **DE** suggestion, mainly about the exclusion of national security services. **RO** pointed out that MS should be entitled to appoint the designated authorities of their choice; **SI:** such a suggestion would have an additional administrative burden. **DE** stressed that intelligence services should not be given access to EURODAC expressly, although acknowledging that in certain national administrations intelligence services are also responsible for threat prevention. **HU** suggested focusing on the task to be accomplished rather than the organisation which would be responsible for it. The above commentary from delegations is also relevant to the similar suggestion made by **DE** under Art. 6(1).

Article 6

Verifying Authorities for the purposes of law enforcement access

1. For the purposes as laid down in Article 1(2) each Member State shall designate a single national authority or a branch of such an authority to act as its verifying authority. The verifying authority shall be an authority of the Member State which is competent for the prevention, detection or investigation of terrorist offences or other serious criminal offences.³²
2. The verifying authority shall ensure that the conditions for requesting comparisons of fingerprints with EURODAC data are fulfilled.

Only the verifying authority shall be authorised to forward requests for comparison of fingerprints to the National Access Point which communicates with the Central System.

³² **CZ:** reservation on the concept of verifying authority; **DE:** scrutiny reservation on this paragraph, pointing out that MS should be entitled to designate more than one verifying authority, insofar as this corresponds with its national structures. **DE** also suggested the following sentence, included in Art. 4(1) of the 2009 proposal for a Council Decision on requesting comparisons with EURODAC data by MS law enforcement authorities and agreed then among delegations, should be added in this provision: “Verifying authorities shall not include agencies or units dealing especially with national security issues” (see comments under footnote 39).

Article 7

Europol

1. ➔ For the purposes as laid down in Article 1(2) ☹ Europol shall designate a specialised unit with duly empowered Europol officials to act as its verifying authority ➔. The verifying authority shall be a unit of Europol which acts independently. The unit shall ensure that the conditions for requesting comparisons of fingerprints with EURODAC data are fulfilled. Europol ☹ and shall designate in agreement with any Member State the National Access Point of that Member State which shall communicate its requests for comparison of fingerprint data to the Central System.
2. Europol shall designate an operating unit that is authorised to request comparisons with EURODAC data through its designated National Access Point. ➔ The designated authority shall be an operating unit of Europol which is competent to collect, store, process, analyse and exchange information to support and strengthen action by Member States in preventing, detecting and investigating terrorist offences or other serious criminal offences falling under Europol's mandate. ☹

↓ 2725/2000/EC (adapted)

⇒ new

Article ~~8~~ ³

⊗ Statistics ⊗

~~3.1.~~ The ~~Central Unit~~ ⊗ Agency ⊗ shall draw up statistics on ~~its~~ ⊗ the ⊗ work ⊗ of the Central System ⊗ every ~~quarter~~ ⇒ month ⇐, indicating ⇒ in particular ⇐ :

- (a) the number of data sets transmitted on ~~applicants for asylum and the~~ persons referred to in Articles 9(1), ~~8(1) and 11(1)~~ 14(1) and 17(1) ;
- (b) the number of hits for applicants for ~~asylum~~ ⇒ international protection ⇐ who have lodged an application for ~~asylum~~ ⇒ international protection ⇐ in another Member State;
- (c) the number of hits for persons referred to in Article ~~8(1)~~ 14(1) who have subsequently lodged an application for ~~asylum~~ ⇒ international protection ⇐;
- (d) the number of hits for persons referred to in Article ~~11(1)~~ 17(1) who had previously lodged an application for ~~asylum~~ ⇒ international protection ⇐ in another Member State;
- (e) the number of fingerprint data which the Central ~~Unit~~ ⇒ System ⇐ had to ⇒ repeatedly ⇐ request ~~a second time~~ from the Member States of origin because the fingerprint data originally transmitted did not lend themselves to comparison using the computerised fingerprint recognition system;=

↓ new

↻ Council

(f) the number of requests for marking and unmarking transmitted in accordance with Article 18(1) and (2).

(g) the number of hits for persons referred to in Article 18(1) for whom hits have been recorded under points (b) and (d) of this Article.

↻ (h) the number of requests referred to in Article 20 (1) ↻³³

↻ (i) the number of hits referred to in Article 20 (1) ↻

↻ (j) the number of requests referred to in Article 21 (1) ↻

↻ (k) the number of hits referred to in Article 21 (1) ↻

↓ 2725/2000/EC

⇒ new

2. At the end of each year, statistical data shall be established in the form of a compilation of the ⇒ monthly ⇐ ~~quarterly~~ statistics ~~drawn up since the beginning of Eurodac's activities~~ ⇒ for that year ⇐, including an indication of the number of persons for whom hits have been recorded under ⇒ points ⇐ (b), (c), and (d). ⇒ The statistics shall contain a breakdown of data for each Member State. ⇐

³³ In relation to added points (h) to (k), **Pres** invites the **Cion** to consider agreeing to this change to the wording of the underlying Regulation that had not been originally included in the **Cion's** recast on the basis of the need for consistency within the Regulation.

~~4. Pursuant to the procedure laid down in Article 23(2), the Central Unit may be charged with carrying out certain other statistical tasks on the basis of the data processed at the Central Unit.~~

↓ 2725/2000/EC (adapted)

⇒ new

CHAPTER II

APPLICANTS FOR ~~ASYLUM~~ ⊗ INTERNATIONAL PROTECTION ⊗

Article 9 ~~4~~

Collection, transmission and comparison of fingerprints

1. Each Member State shall promptly take the fingerprints of all fingers of every applicant for ~~asylum~~ ⇒ international protection ⇐ of at least 14 years of age and shall promptly ⇒ as soon as possible and no later than 72 hours after the lodging of that application for international protection as defined by Article 20(2) of the Dublin Regulation ⇐ transmit ⊗ them together with ⊗ the data referred to in points ~~(a)~~ (b) to ~~(f)~~ (g) of Article ~~5(1)~~ 11 to the Central Unit ⇒ System ⇐.

↓ new

⇒ Non compliance with the 72 hours time limit does not relieve Member States of the obligation to take and transmit the fingerprints to the Central System. Where the condition of the fingertips does not allow to take the fingerprints in a quality ensuring appropriate comparison under Article 25 of this Regulation, the Member State of origin shall retake the fingerprints of the applicant and resend them as soon as possible and no later than 48 hours after they have been successfully taken. ⇐

↓ 2725/2000/EC

~~(2) The data referred to in Article 5(1) shall be immediately recorded in the central database by the Central Unit, or, provided that the technical conditions for such purposes are met, directly by the Member State of origin.~~

↓ new

2. By way of derogation from paragraph 1, where it is not possible to take the fingerprints of an applicant on account of measures taken to ensure the health of the applicant or the protection of public health, Member States shall take and send the fingerprints of the applicant as soon as possible and no later than 48 hours after these grounds no longer prevail.

↓ 2725/2000/EC (adapted)

⇒ new

⇒ Council

3. Fingerprint data within the meaning of point ~~(b)~~ (a) of Article ~~5(1)~~ 11, transmitted by any Member State, ~~with~~ with exception to those transmitted in accordance with Article 10 point (b) ~~shall be compared by the Central Unit~~ ⇒ automatically ⇐ with the fingerprint data transmitted by other Member States and already stored in the ~~Central database~~ ⇒ System ⇐.
4. The Central ~~Unit~~ ⇒ System ⇐ shall ensure, on the request of a Member State, that the comparison referred to in paragraph 3 covers the fingerprint data previously transmitted by that Member State, in addition to the data from other Member States.
5. The Central ~~Unit~~ ⇒ System ⇐ shall ~~forthwith~~ ⇒ automatically ⇐ transmit the hit or the negative result of the comparison to the Member State of origin. Where there is a hit, it shall transmit for all data sets corresponding to the hit, the data referred to in ~~Articles 5(1) and 11(a) to (k)~~ ⇒ [...] ⇐, ~~although in the case of the data referred to in Article 5(1)(b), only insofar as they were the basis for the hit~~ ⇒ along with, where appropriate, the mark referred to in Article 18(1) ⇐.
- ~~Direct transmission to the Member State of origin of the result of the comparison shall be permissible where the technical conditions for such purpose are met.~~
- ~~7. The implementing rules setting out the procedures necessary for the application of paragraphs 1 to 6 shall be adopted in accordance with the procedure laid down in Article 22(1).~~

↓ new

→ Council

Article 10

Information on the status of the data subject

The following information shall be sent to the Central System in order to be stored in accordance with Article 12 [...] for the purpose of transmission under Article 9(5):

- (a) When an applicant for international protection or another person as referred to in point (d) of Article 18(1) of the Dublin Regulation arrives in the responsible Member State following a transfer pursuant to a decision acceding to a request to take him/her back as referred to in Article 24 of the Dublin Regulation, the responsible Member State shall update its dataset recorded in conformity with Article [...] of this Regulation relating to the person concerned by adding their date of arrival .
- (b) When an applicant for international protection arrives in the responsible Member State following a transfer pursuant to a decision acceding to a request to take charge of [...] him/her as referred to in Article 22 of the Dublin Regulation, the responsible Member State shall send a dataset in conformity with Article 11 of this Regulation relating to the person concerned and include their date of arrival.

- (c) As soon as the Member State of origin can establish that the person concerned whose data was recorded in EURODAC in accordance with Article 11 of this Regulation has left the territory of the Member States, it shall update its dataset recorded in conformity with Article 11 of this Regulation relating to the person concerned by adding the date when the person left the territory, in order to facilitate the application of Articles 19(2) and 20(5) of the Dublin Regulation.
- (d) As soon as the Member State of origin ensures that the person concerned whose data was recorded in EURODAC in accordance with Article 11 has left the territory of the Member States in compliance with a return decision or removal order it issued following the withdrawal or rejection of the application as provided for in Article 19(3) of the Dublin Regulation, it shall update its dataset recorded in conformity with Article 11 relating to the person concerned by adding the date of his/her removal or when the person left the territory.
- (e) The Member State which assumes responsibility in accordance with Article 17(1) of the Dublin Regulation shall update its dataset recorded in conformity with Article 11 of this Regulation relating to that applicant by adding the date when the decision to examine the application was taken.

↓ 2725/2000/EC

⇒ new

Article 11 ~~5~~

Recording of data

~~1.~~ Only the following data shall be recorded in the eCentral database ⇒ System ⇐ :

(~~a~~) fingerprint data;

(~~b~~) Member State of origin, place and date of the application for asylum ⇒ international protection; in the cases referred to in point (b) of Article 10, the date of application shall be the one entered by the Member State who transferred the applicant ⇐;

(c) sex;

(d) reference number used by the Member State of origin;

(e) date on which the fingerprints were taken;

(f) date on which the data were transmitted to the Central Unit ⇒ System ⇐;

~~(g) date on which the data were entered in the central database;~~

↓ new

(g) operator user ID.

↓ 2725/2000/EC

⇒ new

~~(h) details in respect of the recipient(s) of the data transmitted and the date(s) of transmission(s).~~

(h) where applicable in accordance with Article 10 point (a) or point (b), the date of the arrival of the person concerned after a successful transfer;

(i) where applicable in accordance with Article 10 point (c), the date when the person concerned left the territory of the Member States;

(j) where applicable in accordance with Article 10 point (d), the date when the person concerned left or was removed from the territory of the Member States;

(k) where applicable in accordance with Article 10 point (e), the date when the decision to examine the application was taken.

~~2. After recording the data in the central database, the Central Unit shall destroy the media used for transmitting the data, unless the Member State of origin has requested their return.~~

Article ~~12~~ 6

Data storage

Each set of data, as referred to in Article ~~5(1)~~ 11, shall be stored in the ~~Central~~ ⇒ System ⇐ database for ten years from the date on which the fingerprints were taken.

Upon expiry of this period, the Central ~~Unit~~ ⇒ System ⇐ shall automatically erase the data from the ~~Central~~ database ⇒ System ⇐.

Article ~~13~~ 7

Advance data erasure

1. Data relating to a person who has acquired citizenship of any Member State before expiry of the period referred to in Article ~~6~~ 12 shall be erased from the Central ~~Unit~~ ⇒ System ⇐, in accordance with Article ~~15(3)~~ 27(4) as soon as the Member State of origin becomes aware that the person has acquired such citizenship.

↓ new

2. The Central System shall inform all Member States of origin about the erasure of data for the reason specified in paragraph 1 by another Member State of origin having produced a hit with data which they transmitted relating to persons referred to in Article 9(1) or Article 14(1).

↓ 2725/2000/EC (adapted)

⇒ new

CHAPTER III

~~ALIENS~~ ☒ **THIRD COUNTRY NATIONALS OR STATELESS PERSONS** ☒ **APPREHENDED IN CONNECTION WITH THE IRREGULAR CROSSING OF AN EXTERNAL BORDER**

Article 14 §

Collection and transmission of fingerprint data

1. Each Member State shall, ~~in accordance with the safeguards laid down in the European Convention on Human Rights and in the United Nations Convention on the Rights of the Child~~ promptly take the fingerprints of all fingers of every ~~alien~~ ☒ third country national or stateless person ☒ of at least 14 years of age who is apprehended by the competent control authorities in connection with the irregular crossing by land, sea or air of the border of that Member State having come from a third country and who is not turned back ⇒ or who remains physically on the territory of the Member States and who is not kept in custody, confinement or detention during the entirety of the period between apprehension and removal on the basis of the decision to turn them back ⇐ .

2. The Member State concerned shall promptly ⇒ as soon as possible and no later than 72 hours from the date of apprehension ⇐ transmit to the Central Unit ⇐ System ⇐ the following data in relation to any alien ⊗ third country national or stateless person ⊗, as referred to in paragraph 1, who is not turned back:

(a) fingerprint data;

(b) Member State of origin, place and date of the apprehension;

(c) sex;

(d) reference number used by the Member State of origin;

(e) date on which the fingerprints were taken;

(f) date on which the data were transmitted to the Central Unit ⇐ System ⇐;

↓ new

(g) operator user ID.

3. By way of derogation from paragraph 2, as regards persons apprehended in the manner described in paragraph 1 who remain physically on the territory of the Member States but are kept in custody, confinement or detention upon their apprehension for a period exceeding 72 hours, the transmission of the data specified in paragraph 2 relating to those persons shall take place before their release from custody, confinement or detention.

4. Non compliance with the 72 hours time limit referred to in paragraph 2 does not relieve Member States of the obligation to take and transmit the fingerprints to the Central System. Where the condition of the fingertips does not allow to take the fingerprints in a quality ensuring appropriate comparison under Article 25, the Member State of origin shall retake the fingerprints of such person and resend them as soon as possible and no later than 48 hours after they have been successfully taken.

5. By way of derogation from paragraph 1, where it is not possible to take the fingerprints of such person on account of measures taken to ensure the health of the person or the protection of public health, the Member State concerned shall take and send the fingerprints of the person, in accordance with the deadline set out in paragraph 2, once these grounds no longer prevail.

↓ 2725/2000/EC (adapted)

⇒ new

⇒ Council

Article 15 ~~9~~

Recording of data

1. The data referred to ~~in Article 5(1)(g) and~~ in Article ~~8(2)~~ 14(2) shall be recorded in the ~~central database~~ ⇒ Central System ⇐.

Without prejudice to Article ~~3(3)~~8, data transmitted to the Central ~~Unit~~ ⇒ System ⇐ pursuant to Article ~~8(2)~~ 14(2) shall be recorded for the sole purpose of comparison with data on applicants for ~~asylum~~ ⇒ international protection ⇐ transmitted subsequently to the Central ~~Unit~~ ⇒ System ⇐ and for the purposes as laid down in Article 1(2) ~~c~~.³⁴

The Central ~~Unit~~ ⇒ System ⇐ shall not compare data transmitted to it pursuant to Article ~~8(2)~~ 14(2) with any data previously recorded in the ~~central database~~ ⇒ Central System ⇐, nor with data subsequently transmitted to the Central ~~Unit~~ ⇒ System ⇐ pursuant to Article ~~8(2)~~ 14(2).

³⁴ Pres invites the Cion to consider agreeing to this change to the wording of the underlying Regulation that had not been originally included in the Cion's recast on the basis of the need for consistency within the Regulation.

2. ~~The procedures provided for in Article 4(1), second sentence, Article 4(2) and Article 5(2) as well as the provisions laid down pursuant to Article 4(7) shall apply.~~ As regards the comparison of data on applicants for ~~asylum~~ ⇒ international protection ⇐ subsequently transmitted to the Central ~~Unit~~ ⇒ System ⇐ with the data referred to in paragraph 1, the procedures provided for in Article ~~4(3), (5) and (6)~~ 9(3) and (5) and in Article 25(4) shall apply.

Article ~~16~~ 10

Storage of data

1. Each set of data relating to an ~~alien~~ ☒ third country national or stateless person ☒ as referred to in Article ~~8(1)~~ 14(1) shall be stored in the ~~central database~~ ⇒ Central System ⇐ for ⇒ ~~[...]~~ ⇐ two years ³⁵ ⇐ ~~two years~~ from the date on which the fingerprints of the ~~alien~~ ☒ third country national or stateless person ☒ were taken. Upon expiry of this period, the Central ~~Unit~~ ⇒ System ⇐ shall automatically erase the data from the ~~central database~~ ⇒ Central System ⇐.
2. The data relating to an ~~alien~~ ☒ third country national or stateless person ☒ as referred to in Article ~~8(1)~~ 14(1) shall be erased from the ~~central database~~ ⇒ Central System ⇐ in accordance with Article ~~15(3)~~ ~~[...]~~ ⇐ 27 ⇐ (3) ☒³⁶ as soon as ☒ the Member State of origin becomes aware of one of the following circumstances before the ~~two~~ ⇒ ~~two~~ ⇐ ~~[...]~~ ⇐ -year period mentioned in paragraph 1 has expired:

³⁵ **EL, IT:** reservations, preferring a one-year storage period as a stronger guarantee for the applicants. **Cion** cannot accept the compromise; for asylum-linked (the main objective of the EURODAC Regulation is to facilitate the functioning of the Dublin Regulation), as well as for data-protection purposes; it would prefer the one-year period storage. **Cion** also recalled the EP position on this issue, in view of the future negotiations within the ordinary procedure.

³⁶ **Pres** invites the **Cion** to consider agreeing to this change to the wording of the underlying Regulation that had not been originally included in the **Cion's** recast on the basis of the need for consistency within the Regulation.

- (a) the ~~alien~~ third country national or stateless person has been issued with a residence ~~permit~~ document ;
 - (b) the ~~alien~~ third country national or stateless person has left the territory of the Member States;
 - (c) the ~~alien~~ third country national or stateless person has acquired the citizenship of any Member State.
-

- 3. The Central System shall inform all Member States of origin about the erasure of data for the reason specified in point (a) or (b) of paragraph 2 or by another Member State of origin having produced a hit with data which they transmitted relating to persons referred to in Article 14(1).
- 4. The Central System shall inform all Member States of origin about the erasure of data for the reason specified in point (c) of paragraph 2 by another Member State of origin having produced a hit with data which they transmitted relating to persons referred to in Article 9(1) or Article 14(1).

↓ 2725/2000/EC (adapted)

⇒ new

↻ Council

CHAPTER IV

~~ALIENS~~ ⊗ THIRD COUNTRY NATIONALS OR STATELESS PERSONS ⊗ FOUND ILLEGALLY ~~PRESENT~~ ⊗ STAYING ⊗ IN A MEMBER STATE

Article ~~17~~

Comparison of fingerprint data

1. With a view to checking whether an ~~alien~~ ⊗ third country national or a stateless person ⊗ found illegally ~~present~~ ⊗ staying ⊗ within its territory has previously lodged an application for ~~asylum~~ ⇒ international protection ⇐ in another Member State, each Member State may transmit to the Central ~~Unit~~ ⇒ System ⇐ any fingerprint data relating to fingerprints which it may have taken of any such ~~alien~~ ⊗ third country national or stateless person ⊗ of at least 14 years of age together with the reference number used by that Member State.

As a general rule there are grounds for checking whether the ~~alien~~ ☒ third country national or stateless person ☒ has previously lodged an application for ~~asylum~~ ⇒ international protection ⇐ in another Member State where:

- (a) the ~~alien~~ ☒ third country national or stateless person ☒ declares that he/she has lodged an application for ~~asylum~~ ⇒ international protection ⇐ but without indicating the Member State in which he/she made the application;
- (b) the ~~alien~~ ☒ third country national or stateless person ☒ does not request ~~asylum~~ ⇒ international protection ⇐ but objects to being returned to his/her country of origin by claiming that he/she would be in danger, or
- (c) the ~~alien~~ ☒ third country national or stateless person ☒ otherwise seeks to prevent his/her removal by refusing to cooperate in establishing his/her identity, in particular by showing no, or false, identity papers.

2. Where Member States take part in the procedure referred to in paragraph 1, they shall transmit to the Central ~~Unit~~ ⇒ System ⇐ the fingerprint data relating to all or at least the index fingers, and, if those are missing, the prints of all other fingers, of ~~aliens~~ ☒ third country nationals or stateless persons ☒ referred to in paragraph 1.

3. The fingerprint data of an ~~alien~~ ☒ third country national or a stateless person ☒ as referred to in paragraph 1 shall be transmitted to the Central ~~Unit~~ ⇒ System ⇐ solely for the purpose of comparison with the fingerprint data of applicants for ~~asylum~~ ⇒ international protection ⇐ transmitted by other Member States and already recorded in the ~~central database~~ ⇒ Central System ⇐.

The fingerprint data of such ~~an alien~~ third country national or a stateless person shall not be recorded in the ~~central database~~ Central System , nor shall they be compared with the data transmitted to the Central ~~Unit~~ System pursuant to Article ~~8(2)~~ 14(2).

4. As regards the comparison of fingerprint data transmitted under this Article with the fingerprint data of applicants for ~~asylum~~ international protection transmitted by other Member States which have already been stored in the Central ~~Unit~~ System , the procedures provided for in Article ~~4(3) (5) and (6)~~ 9(3) and (5) as well as the provisions pursuant to Article 25 (4)³⁷ ~~as well as the provisions laid down pursuant to Article 4(7)~~ shall apply.

~~5. Once the results of the comparison have been transmitted to the Member State of origin, the Central Unit shall forthwith:~~

~~(a) erase the fingerprint data and other data transmitted to it under paragraph 1; and~~

~~(b) destroy the media used by the Member State of origin for transmitting the data to the Central Unit, unless the Member State of origin has requested their return.~~

³⁷ **Pres** invites the **Cion** to consider agreeing to this change to the wording of the underlying Regulation that had not been originally included in the **Cion's** recast on the basis of the need for consistency within the Regulation.

CHAPTER V

~~RECOGNISED REFUGEES~~ ☒ PERSONS GRANTED INTERNATIONAL PROTECTION ☒

~~Article 12~~

~~Blocking of data~~

~~1. Data relating to an applicant for asylum which have been recorded pursuant to Article 4(2) shall be blocked in the central database if that person is recognised and admitted as a refugee in a Member State. Such blocking shall be carried out by the Central Unit on the instructions of the Member State of origin.~~

~~As long as a decision pursuant to paragraph 2 has not been adopted, hits concerning persons who have been recognised and admitted as refugees in a Member State shall not be transmitted. The Central Unit shall return a negative result to the requesting Member State.~~

~~2. Five years after Eurodac starts operations, and on the basis of reliable statistics compiled by the Central Unit on persons who have lodged an application for asylum in a Member State after having been recognised and admitted as refugees in another Member State, a decision shall be taken in accordance with the relevant provisions of the Treaty, as to whether the data relating to persons who have been recognised and admitted as refugees in a Member State should:~~

~~(a) be stored in accordance with Article 6 for the purpose of the comparison provided for in Article 4(3); or~~

~~(b) be erased in advance once a person has been recognised and admitted as a refugee.~~

~~3. In the case referred to in paragraph 2(a), the data blocked pursuant to paragraph 1 shall be unblocked and the procedure referred to in paragraph 1 shall no longer apply.~~

~~4. In the case referred to in paragraph 2(b):~~

~~(a) data which have been blocked in accordance with paragraph 1 shall be erased immediately by the Central Unit; and~~

~~(b) data relating to persons who are subsequently recognised and admitted as refugees shall be erased in accordance with Article 15(3), as soon as the Member State of origin becomes aware that the person has been recognised and admitted as a refugee in a Member State.~~

~~5. The implementing rules concerning the procedure for the blocking of data referred to in paragraph 1 and the compilation of statistics referred to in paragraph 2 shall be adopted in accordance with the procedure laid down in Article 22(1).~~

Article 18

Marking of data

1. The Member State of origin which granted international protection to an applicant for international protection whose data were previously recorded pursuant to Article 11 in the Central System shall mark the relevant data in conformity with the requirements for electronic communication with the Central System established by the Agency. This mark shall be stored in the Central System in accordance with Article 12 for the purpose of transmission under Article 9(5).
2. The Member State of origin shall unmark data concerning a third country national or stateless person whose data were previously marked in accordance with paragraph 1 if his or her status is revoked or ended or renewal of his status is refused under Article 14 or 19 of Council Directive 2004/83/EC.

↓ new

↻ Council

CHAPTER VI

PROCEDURE FOR COMPARISON AND DATA TRANSMISSION FOR LAW ENFORCEMENT PURPOSES

Article 19

Procedure for comparison of fingerprint data with EURODAC data³⁸

1. ↻ For the purposes as laid down in Article 1 (2) the ↻ [...] ↻ designated authorities referred to in Article 5(1) and ↻ the designated authority of ↻ Europol ↻ referred to in Article 7(2)³⁹ ↻ may submit a reasoned electronic request ↻ together with the reference number used by that authority's Member State or Europol, ↻ to the verifying authority for the transmission for comparison of fingerprint data to the EURODAC Central System via the National Access Point. Upon receipt of such a request, the verifying authority shall verify whether the conditions for requesting a comparison referred to in Article 20 or Article 21, as appropriate, are fulfilled.

³⁸ CZ: reservation in relation to its concerns about the notion of Verifying Authority.

³⁹ DE suggested the using the wording of Art. 7(2): "operating unit of EUROPOL".

2. Where all the conditions for requesting a comparison are fulfilled, the verifying authority shall transmit the request for comparison to the National Access Point which will process it to the EURODAC Central System according to the procedures laid down in Article 9 (3) and (5) for the purpose of comparison with the data transmitted to the Central System pursuant to Article 9(1) and 14 (2) .
3. In exceptional cases of urgency, the verifying authority may transmit the fingerprint data to the National Access Point for comparison immediately upon receipt of a request by a designated authority and only verify ex-post whether all the conditions of Article 20 or Article 21 are fulfilled, including whether an exceptional case of urgency actually existed. The ex-post verification shall take place without undue delay after the processing of the request.
4. Where the ex-post verification determines that the access was not justified, the information communicated from EURODAC shall be destroyed by all authorities that have accessed it and they shall inform the verifying authority of such destruction.

Article 20

Joint supervisory authority

- ~~1. An independent joint supervisory authority shall be set up, consisting of a maximum of two representatives from the supervisory authorities of each Member State. Each delegation shall have one vote.~~
- ~~2. The joint supervisory authority shall have the task of monitoring the activities of the Central Unit to ensure that the rights of data subjects are not violated by the processing or use of the data held by the Central Unit. In addition, it shall monitor the lawfulness of the transmission of personal data to the Member States by the Central Unit.~~
- ~~3. The joint supervisory authority shall be responsible for the examination of implementation problems in connection with the operation of Eurodac, for the examination of possible difficulties during checks by the national supervisory authorities and for drawing up recommendations for common solutions to existing problems.~~
- ~~4. In the performance of its duties, the joint supervisory authority shall, if necessary, be actively supported by the national supervisory authorities.~~
- ~~5. The joint supervisory authority shall have access to advice from persons with sufficient knowledge of fingerprint data.~~
- ~~6. The Commission shall assist the joint supervisory authority in the performance of its tasks. In particular, it shall supply information requested by the joint supervisory body, give it access to all documents and paper files as well as access to the data stored in the system and allow it access to all its premises, at all times.~~

- ~~7. The joint supervisory authority shall unanimously adopt its rules of procedure. It shall be assisted by a secretariat, the tasks of which shall be defined in the rules of procedure.~~
- ~~8. Reports drawn up by the joint supervisory authority shall be made public and shall be forwarded to the bodies to which the national supervisory authorities submit their reports, as well as to the European Parliament, the Council and the Commission for information. In addition, the joint supervisory authority may submit comments or proposals for improvement regarding its remit to the European Parliament, the Council and the Commission at any time.~~
- ~~9. In the performance of their duties, the members of the joint supervisory authority shall not receive instructions from any government or body.~~
- ~~10. The joint supervisory authority shall be consulted on that part of the draft operating budget of the Eurodac Central Unit which concerns it. Its opinion shall be annexed to the draft budget in question.~~
- ~~11. The joint supervisory authority shall be disbanded upon the establishment of the independent supervisory body referred to in Article 286(2) of the Treaty. The independent supervisory body shall replace the joint supervisory authority and shall exercise all the powers conferred on it by virtue of the act under which that body is established.~~

Article 20

Conditions for access to EURODAC data by designated authorities⁴⁰

1. **For the purposes as laid down in Article 1 (2) designated authorities may request the comparison of fingerprint data with those stored in the EURODAC central database within the scope of their powers only if comparisons of national fingerprint databases and of the Automated Fingerprint Databases of other Member States under Decision 2008/615/JHA did not lead to the establishment of the identity of the data subject and where:**
 - (a) the comparison is necessary for the purpose of the prevention, detection or investigation of terrorist offences or other serious criminal offences;
 - (b) the comparison is necessary in a specific case; systematic comparisons shall not be carried out; and
 - (c) there are reasonable grounds to consider that such comparison with EURODAC data will contribute to the prevention, detection or investigation of any of the criminal offences in question.⁴¹
2. Requests for comparison with EURODAC data shall be limited to searching with fingerprint data.

⁴⁰ RO pointed out that although the access to the Prüm functionality is voluntary, it constitutes a precondition of access to EURODAC for law enforcement purposes.

⁴¹ BE: reasonable grounds to consider that there is a link between the person concerned and the criminal act under investigation should exist, in order to avoid excessive use of the search functionality. To this effect points (a) and (b) should read as follows:

- (a) the comparison is necessary for the purpose of **conducting criminal investigations or criminal intelligence operations into** terrorist offences or other serious criminal offences;
- (b) the comparison is necessary in a specific case; systematic comparisons shall not be carried out; and
- (c) there are reasonable grounds to **suspect the data subject to commit or to have committed** any of the criminal offences in question.

Article 21

Conditions for access to EURODAC data by Europol

1.

For the purposes as laid down in Article 1 (2) the designated authority of Europol may request the comparison of fingerprint data with those stored in the EURODAC central database within the limits of the mandate of Europol and where necessary for the performance of tasks of Europol only if comparisons with fingerprint data stored in any information processing system established at Europol did not lead to the establishment of the identity of the data subject and where

 - (a) the comparison is necessary to support and strengthen action by Member States in preventing, detecting and investigating terrorist offences or other serious criminal offences falling under Europol's mandate;
 - (b) the comparison is necessary in a specific case; systematic comparisons shall not be carried out; and
 - (c) there are reasonable grounds to consider that such comparison with EURODAC data will contribute to the prevention, detection or investigation of any of the criminal offences in question.
2. Requests for comparison with EURODAC data shall be limited to comparisons of fingerprint data.
3. Processing of information obtained by Europol from comparison with EURODAC shall be subject to the authorisation of the Member State of origin. Such authorisation shall be obtained via the Europol national unit of that Member State.

Article 22

Communication between the ~~the~~ designated authorities, the ~~the~~ verifying authorities and the National Access Points⁴²

1. ~~the~~ [...] ~~the~~ In accordance with Article 26, all communication between the designated authorities, the verifying authorities and the National Access points shall be secure and ~~the~~ take place electronically.
2. ~~the~~ For the purposes as laid down in Article 1 (2) fingerprints ~~the~~ [...] ~~the~~ shall be digitally processed by the Member State and transmitted in the data format referred to in Annex I, in order to ensure that the comparison can be carried out by means of the computerised fingerprint recognition system.

↓ 2725/2000/EC (adapted)

⇒ new

CHAPTER ~~VI~~ VII

DATA PROCESSING ~~USE~~, DATA PROTECTION AND LIABILITY

Article ~~23~~ ~~13~~

Responsibility for data processing ~~use~~

1. The Member State of origin shall be responsible for ensuring that:
 - (a) fingerprints are taken lawfully;

⁴² CZ: reservation on this Article.

- (b) fingerprint data and the other data referred to in Article ~~5(1)~~ 11, Article ~~8(2)~~ 14(2) and Article ~~11(2)~~ 17(2) are lawfully transmitted to the Central ~~Unit~~ ⇒ System ⇐;
- (c) data are accurate and up-to-date when they are transmitted to the Central ~~Unit~~ ⇒ System ⇐;
- (d) without prejudice to the responsibilities of the ~~Commission~~ ⇒ Agency ⇐, data in the ~~central database~~ ⇒ Central System ⇐ are lawfully recorded, stored, corrected and erased;
- (e) the results of fingerprint data comparisons transmitted by the Central ~~Unit~~ ⇒ System ⇐ are lawfully processed ~~used~~.
2. In accordance with Article ~~14~~ 34, the Member State of origin shall ensure the security of the data referred to in paragraph 1 before and during transmission to the Central ~~Unit~~ ⇒ System ⇐ as well as the security of the data it receives from the Central ~~Unit~~ ⇒ System ⇐.
3. The Member State of origin shall be responsible for the final identification of the data pursuant to Article ~~4(6)~~ 25(4).
4. The ~~Commission~~ ⇒ Agency ⇐ shall ensure that the Central ~~Unit~~ ⇒ System ⇐ is operated in accordance with the provisions of this Regulation ~~and its implementing rules~~. In particular, the ~~Commission~~ ⇒ Agency ⇐ shall:
- (a) adopt measures ensuring that persons working ⇒ with ⇐ ~~in~~ the Central ~~Unit~~ ⇒ System ⇐ process ~~use~~ the data recorded ⊗ therein ⊗ ~~in the central database~~ only in accordance with the purpose of ~~Eurodac~~ EURODAC as laid down in Article 1(1);

~~(b) ensure that persons working in the Central System comply with all requests from Member States made pursuant to this Regulation in relation to recording, comparison, correction and erasure of data for which they are responsible;~~

~~(b) (e)~~ take the necessary measures to ensure the security of the Central ~~Unit~~
⇒ System ⇐ in accordance with Article ~~14~~ 34;

~~(c) (d)~~ ensure that only persons authorised to work ⇒ with ⇐ in the Central ~~Unit~~
⇒ System ⇐ have access ⊗ thereto ⊗ ~~to data recorded in the central database,~~
without prejudice to ~~Article 20 and the powers of the independent supervisory body~~
~~which will be established under Article 286(2) of the Treaty~~ ⊗ the competences of
the European Data Protection Supervisor ⊗.

The ~~Commission~~ ⇒ Agency ⇐ shall inform the European Parliament and the Council ⇒ as
well as the European Data Protection Supervisor ⇐ of the measures it takes pursuant to the
first subparagraph.

↓ 407/2002/EC Article 2 (adapted)

⇒ new

↻ Council

Article ~~24~~ 2

Transmission

1. Fingerprints shall be digitally processed and transmitted in the data format referred to in Annex I. As far as it is necessary for the efficient operation of the Central ~~Unit~~
⇒ System ⇐, the ~~Central Unit~~ ⊗ Agency ⊗ shall establish the technical requirements for transmission of the data format by Member States to the Central ~~Unit~~ ⇒ System ⇐ and vice versa. The ~~Central Unit~~ ⊗ Agency ⊗ shall ensure that the fingerprint data transmitted by the Member States can be compared by the computerised fingerprint recognition system.

2. Member States ~~should~~ shall transmit the data referred to in Article ~~5(1)~~ 11(1), Article 14(2) and Article 17(2) of the Eurodac Regulation electronically. The data referred to in Article 11(1) and Article 14(2) shall be automatically recorded in the Central System. As far as it is necessary for the efficient operation of the Central ~~Unit~~ System , the ~~Central Unit~~ Agency shall establish the technical requirements to ensure that data can be properly electronically transmitted from the Member States to the Central ~~Unit~~ System and vice versa. ~~Transmission of data in paper form using the form set out in Annex II or by other means of data support (diskettes, CD-ROM or other means of data support which may be developed and generally used in future) should be limited to situations in which there are continuous technical problems.~~

3.⁴³ The reference number referred to in [...] Articles ~~5(1)(d)~~ 11(d) , [...] 14(2)(d) , [...] 17(1) and 19 (1) ~~of the Eurodac Regulation~~ shall make it possible to relate data unambiguously to one particular person and to the Member State which is transmitting the data. In addition, it shall make it possible to tell whether such data relate to ~~an asylum seeker or~~ a person referred to in Article ~~8 or Article 11 of the Eurodac Regulation~~9, Article 14 or Article 17.

⁴³ In relation to the new cross-references cited in this provision, **Pres** invites the **Cion** to consider agreeing to this change to the wording of the underlying Regulation that had not been originally included in the **Cion's** recast on the basis of the need for consistency within the Regulation.

4. The reference number shall begin with the identification letter or letters by which, in accordance with the norm referred to in Annex I, the Member State transmitting the data is identified. The identification letter or letters shall be followed by the identification of the category of person ~~or request~~ . "1" refers to data relating to ~~asylum seekers~~ ~~persons referred to in Article 9(1)~~, "2" to persons referred to in Article ~~8~~ 14(1) ~~, C of the Eurodac Regulation~~ [...] "3" to persons referred to in Article ~~11~~ 17 , "4" to requests referred to in Article 20, and "5" to requests referred to in Article 21 and "9" to requests referred to in article 29⁴⁴ ~~of the Eurodac Regulation~~.
5. The ~~Central Unit~~ Agency shall establish the technical procedures necessary for Member States to ensure receipt of unambiguous data by the Central ~~Unit~~ System.
6. The Central ~~Unit~~ System shall confirm receipt of the transmitted data as soon as possible. To this end the ~~Central Unit~~ Agency shall establish the necessary technical requirements to ensure that Member States receive the confirmation receipt if requested.

⁴⁴ Pres invites the **Cion** to consider agreeing to this change to the wording of the underlying Regulation that had not been originally included in the **Cion's** recast on the basis of the need for consistency within the Regulation.

Carrying out comparisons and transmitting results

1. Member States shall ensure the transmission of fingerprint data in an appropriate quality for the purpose of comparison by means of the computerised fingerprint recognition system. As far as it is necessary to ensure that the results of the comparison by the Central ~~Unit~~ ⇒ System ⇐ reach a very high level of accuracy, the ~~Central Unit~~ ⇒ Agency ⇐ shall define the appropriate quality of transmitted fingerprint data. The Central ~~Unit~~ ⇒ System ⇐ shall, as soon as possible, check the quality of the fingerprint data transmitted. If fingerprint data do not lend themselves to comparison using the computerised fingerprint recognition system, the Central ~~Unit~~ ⇒ System ⇐ shall, ~~as soon as possible,~~ ⇒ inform ⇐ the Member State. ⇒ The Member State concerned shall ⇐ transmit fingerprint data of the appropriate quality ⇒ using the same reference number of the previous set of fingerprint data ⇐.
2. The Central ~~Unit~~ ⇒ System ⇐ shall carry out comparisons in the order of arrival of requests. Each request must be dealt with within 24 hours. ~~In the case of data which are transmitted electronically,~~ ~~a~~ A Member State may for reasons connected with national law require particularly urgent comparisons to be carried out within one hour. Where these times cannot be respected owing to circumstances which are outside the ~~Central Unit~~ ⇒ Agency's ⇐ responsibility, the Central ~~Unit~~ ⇒ System ⇐ shall process the request as a matter of priority as soon as those circumstances no longer prevail. In such cases, as far as it is necessary for the efficient operation of the Central ~~Unit~~ ⇒ System ⇐, the ~~Central Unit~~ ⇒ Agency ⇐ shall establish criteria to ensure the priority handling of requests.

3. As far as it is necessary for the efficient operation of the Central ~~Unit~~ ⇒ System ⇐ , the ~~Central Unit~~ ⇒ Agency ⇐ shall establish the operational procedures for the processing of the data received and for transmitting the result of the comparison.

↓ 2725/2000/EC Article 4(6) (adapted)
⇒ new
⇒ Council

4. The results of the comparison shall be immediately checked in the ⇒ receiving ⇐ Member State ⇒ [...] ⇐ ⇒ by a fingerprint expert ⇒ as defined in accordance with its national rules, specifically trained in the types of fingerprint comparisons included in this Regulation ⇐ ⇐ . ⇒ For the purposes as laid down in Article 1 (1), final ⁴⁵ ⇐ ⇒ [...] ⇐ identification shall be made by the Member State of origin in cooperation with the Member States concerned, pursuant to Article ~~15~~ 32 of the Dublin ~~Convention~~ ⊗ Regulation ⊗.

Information received from the Central ~~Unit~~ ⇒ System ⇐ relating to other data found to be unreliable shall be erased ~~or destroyed~~ as soon as the unreliability of the data is established.

↓ new

5. Where final identification in accordance with paragraph 4 reveal that the result of the comparison received from the Central System is inaccurate, Member States shall communicate this fact to the Commission and to the Agency.

⁴⁵ **Pres** invites the **Cion** to consider agreeing to this change to the wording of the underlying Regulation that had not been originally included in the **Cion's** recast on the basis of the need for consistency within the Regulation.

↓ 407/2002/EC (adapted)

⇒ new

Article 26 4

Communication between Member States and the Central ~~Unit~~ ⇒ System ⇐

Data transmitted from the Member States to the Central ~~Unit~~ ⇒ System ⇐ and vice versa shall use ~~IDA generic services referred to in Decision No 1719/1999/EC of the European Parliament and of the Council of 12 July 1999 on a series of guidelines, including the identification of projects of common interest, for trans-European networks for the electronic interchange of data between administrations (IDA)~~ ⇒ the EURODAC Communication Infrastructure ⇐. As far as it is necessary for the efficient operation of the Central ~~Unit~~ ⇒ System ⇐, the ~~Central Unit~~ ⊗ Agency ⊗ shall establish the technical procedures necessary for the use of ~~IDA generic services~~ ⇒ the Communication ⇐.

~~Article 14~~

Security

~~1. The Member State of origin shall take the necessary measures to:~~

~~(a) prevent any unauthorised person from having access to national installations in which the Member State carries out operations in accordance with the aim of Eurodac (checks at the entrance to the installation);~~

~~(b) prevent data and data media in Eurodac from being read, copied, modified or erased by unauthorised persons (control of data media);~~

~~(c) guarantee that it is possible to check and establish a posteriori what data have been recorded in Eurodac when and by whom (control of data recording);~~

~~(d) prevent the unauthorised recording of data in Eurodac and any unauthorised modification or erasure of data recorded in Eurodac (control of data entry);~~

~~(e) guarantee that, in using Eurodac, authorised persons have access only to data which are within their competence (control of access);~~

~~(f) guarantee that it is possible to check and establish to which authorities data recorded in Eurodac may be transmitted by data transmission equipment (control of transmission);~~

~~(g) prevent the unauthorised reading, copying, modification or erasure of data during both the direct transmission of data to or from the central database and the transport of data media to or from the Central Unit (control of transport);~~

~~2. As regards the operation of the Central Unit, the Commission shall be responsible for applying the measures mentioned under paragraph 1.~~

↓ 2725/2000/EC

⇒ new

Article 27 ~~15~~

Access to, and correction or erasure of, data recorded in ~~Eurodac~~ EURODAC

1. The Member State of origin shall have access to data which it has transmitted and which are recorded in the ~~central database~~ ⇒ Central System ⇐ in accordance with the provisions of this Regulation.

No Member State may conduct searches in the data transmitted by another Member State, nor may it receive such data apart from data resulting from the comparison referred to in Article ~~4(5)~~ 9(5).

↓ 2725/2000/EC (adapted)

⇒ new

⇒ Council

2. The authorities of Member States which, pursuant to paragraph 1, have access to data recorded in the ~~central database~~ ⇒ Central System ⇐ shall be those designated by each Member State ⇒ for the purpose of Article 1(1). This designation shall specify the exact unit responsible for carrying out tasks related to the application of this Regulation. ⇐ Each Member State shall without delay communicate to the Commission ⇒ and the Agency ⇐ a list of those authorities ⇒ and any amendments thereto. The Agency shall publish the consolidated list in the Official Journal of the European Union. Where there are amendments thereto, the Agency shall publish once a year an updated consolidated list. ⇐
3. Only the Member State of origin shall have the right to amend the data which it has transmitted to the Central ~~Unit~~ ⇒ System ⇐ by correcting or supplementing such data, or to erase them, without prejudice to erasure carried out in pursuance of Article ~~6, Article 10(1) or Article 12(4)(a)~~ 12 or Article 16(1).

~~Where the Member State of origin records data directly in the central database, it may amend or erase the data directly.~~

~~Where the Member State of origin does not record data directly in the central database, the Central Unit shall amend or erase the data at the request of that Member State.~~

4. If a Member State or the ~~Central Unit~~ ⇒ Agency ⇐ has evidence to suggest that data recorded in the ~~central database~~ ⇒ Central System ⇐ are factually inaccurate, it shall advise the Member State of origin as soon as possible.

If a Member State has evidence to suggest that data were recorded in the ~~central database~~ ⇒ Central System ⇐ contrary to this Regulation, it shall ~~similarly~~ advise ⇒ the Agency, the Commission and ⇐ the Member State of origin as soon as possible. The latter shall check the data concerned and, if necessary, amend or erase them without delay.

5. The ~~Central Unit~~ ⇒ Agency ⇐ shall not transfer or make available to the authorities of any third country data recorded in the ~~central database~~ ⇒ Central System ⇐, unless it is specifically authorised to do so in the framework of a ⇨ [...] ⇩ ⇨ Union⁴⁶ ⇩ agreement on the criteria and mechanisms for determining the State responsible for examining an application for ~~asylum~~ ⇒ international protection ⇐ .

~~Article 22~~

~~Implementing rules~~

- ~~1. The Council shall adopt, acting by the majority laid down in Article 205(2) of the Treaty, the implementing provisions necessary for~~

~~laying down the procedure referred to in Article 4(7);~~

~~laying down the procedure for the blocking of the data referred to in Article 12(1);~~

~~drawing up the statistics referred to in Article 12(2).~~

~~In cases where these implementing provisions have implications for the operational expenses to be borne by the Member States, the Council shall act unanimously.~~

- ~~2. The measures referred to in Article 3(4) shall be adopted in accordance with the procedure referred to in Article 23(2).~~

⁴⁶ Pres invites the Cion to consider agreeing to this change to the wording of the underlying Regulation that had not been originally included in the Cion's recast on the basis of the need for consistency within the Regulation.

Article ~~28~~ ~~16~~

Keeping of records ~~by the Central Unit~~

1. The ~~Central Unit~~ ⇒ Agency ⇐ shall keep records of all data processing operations within the Central ~~Unit~~ ⇒ System ⇐. These records shall show the purpose of access, the date and time, the data transmitted, the data used for interrogation and the name of both the unit ~~putting~~ ⊗ entering ⊗ in or retrieving the data and the persons responsible.
2. Such records may be used only for the data-protection monitoring of the admissibility of data processing as well as to ensure data security pursuant to Article ~~14~~ ~~34~~. The records must be protected by appropriate measures against unauthorised access and erased after a period of one year ⇒ after the retention period referred to in Article 12 and in Article 16(1) has expired ⇐, if they are not required for monitoring procedures which have already begun.

↓ new

↻ Council

3. ↻ For the purposes as laid down in Article 1 (1) each ⇐ ↻ [...] ⇐ Member State shall take the necessary measures in order to achieve the objectives set out in paragraph 1 and 2 in relation to its national system. In addition, each Member State shall keep records of the staff duly authorised to enter or retrieve the data.

↓ 2725/2000/EC (adapted)

⇒ new

↻ Council

~~Article 23~~

~~Committee~~

~~1. The Commission shall be assisted by a committee.~~

~~2. In the cases where reference is made to this paragraph, Articles 5 and 7 of Decision 1999/468/EC shall apply.~~

~~The period laid down in Article 5(6) of Decision 1999/468/EC shall be set at three months.~~

~~3. The committee shall adopt its rules of procedure.~~

Article 29 ~~18~~

Rights of the data subject

1. A person covered by ~~☉~~ [...] ~~☉~~ ~~☉~~ Article 9, Article 14 and Article 17⁴⁷ ~~☉~~ shall be informed by the Member State of origin ⇒ in writing, and where appropriate, orally, in a language which he or she understands or may reasonably be presumed to understand ⇐ of the following:

(a) the identity of the controller and of his representative, if any;

⁴⁷ **Pres** invites the **Cion** to consider agreeing to this change to the wording of the underlying Regulation that had not been originally included in the **Cion's** recast on the basis of the need for consistency within the Regulation.

- (b) ~~the~~ regarding ~~the~~ the purpose for which ~~the~~ his or her ~~the~~ data will be processed within ~~Eurodac~~EURODAC ~~⇒~~ including a description of the aims of the Dublin Regulation, in accordance with Article 4 of that Regulation ~~⇐~~.
- (c) the recipients of the data;
- (d) in relation to a person covered by Article ~~4 9~~ or Article ~~8 14~~, the obligation to have his/her fingerprints taken;
- (e) the existence of the right of access to, ~~and the right to rectify,~~ the data ~~relating to~~ relating to him/her ~~concerning him/her~~ , and the right to request that inaccurate data relating to him/her be corrected ~~⇐~~ ~~⇒~~ or that unlawfully processed data relating to ~~...~~ ~~him/her~~ be erased, as well as the right to receive information on the procedures for exercising those rights including the contact details of the controller and the National Supervisory Authorities referred to in Article 31(1) ~~⇐~~.

In relation to a person covered by Article ~~4 9~~ or Article ~~8 14~~, the information referred to in the first subparagraph shall be provided when his/her fingerprints are taken.

In relation to a person covered by Article ~~11 17~~, the information referred to in the first subparagraph shall be provided no later than the time when the data relating to the person are transmitted to the Central ~~Unit~~ ~~⇒~~ System ~~⇐~~. This obligation shall not apply where the provision of such information proves impossible or would involve a disproportionate effort.

↓ new

⇒ Council

A common leaflet, containing [...] the relevant information referred to in paragraph 1 of this Article and the information referred to in Article 4(1 [...]) of the Dublin Regulation shall be drawn up in accordance with the procedure referred to in Article 40(2) of the Dublin Regulation. The leaflet should be [...] clear and simple, drafted in a language that the person understands or may reasonably be presumed to understand.

Where a person covered by Article 9, Article 14 and Article 17 [...] is a minor, Member States shall provide the information in an age-appropriate manner.

↓ 2725/2000/EC

⇒ new

⇒ Council

2. [...] For the purposes as laid down in Article 1 (1) in⁴⁸ each Member State any data subject may, in accordance with the laws, regulations and procedures of that State, exercise the rights provided for in Article 12 of Directive 95/46/EC.

Without prejudice to the obligation to provide other information in accordance with point (a) of Article 12 of Directive 95/46/EC, the data subject shall have the right to obtain communication of the data relating to him/her recorded in the ~~central database~~ ⇒ Central System ⇐ and of the Member State which transmitted them to the Central Unit ⇒ System ⇐. Such access to data may be granted only by a Member State.

⁴⁸ Pres invites the Cion to consider agreeing to this change to the wording of the underlying Regulation that had not been originally included in the Cion's recast on the basis of the need for consistency within the Regulation.

3. ⇒ For the purposes as laid down in Article 1 (1) in⁴⁹ ⇒ [...] ⇒ each Member State, any person may request that data which are factually inaccurate be corrected or that data recorded unlawfully be erased. The correction and erasure shall be carried out without excessive delay by the Member State which transmitted the data, in accordance with its laws, regulations and procedures.
4. ⇒ For the purposes as laid down in Article 1 (1) if⁵⁰ ⇒ [...] ⇒ the rights of correction and erasure are exercised in a Member State, other than that, or those, which transmitted the data, the authorities of that Member State shall contact the authorities of the Member State, or States, in question so that the latter may check the accuracy of the data and the lawfulness of their transmission and recording in the ~~central database~~ ⇒ Central System ⇐.

⁴⁹ **Pres** invites the **Cion** to consider agreeing to this change to the wording of the underlying Regulation that had not been originally included in the **Cion's** recast on the basis of the need for consistency within the Regulation.

⁵⁰ **Pres** invites the **Cion** to consider agreeing to this change to the wording of the underlying Regulation that had not been originally included in the **Cion's** recast on the basis of the need for consistency within the Regulation.

5. ➔ For the purposes as laid down in Article 1 (1) if⁵¹ ➔ [...] ➔ it emerges that data recorded in the ~~central database~~ ⇒ Central System ⇐ are factually inaccurate or have been recorded unlawfully, the Member State which transmitted them shall correct or erase the data in accordance with Article ~~15(3)~~ 27(3). That Member State shall confirm in writing to the data subject without excessive delay that it has taken action to correct or erase data relating to him/her.
6. ➔ For the purposes as laid down in Article 1 (1) if⁵² ➔ [...] ➔ the Member State which transmitted the data does not agree that data recorded in the ~~central database~~ ⇒ Central System ⇐ are factually inaccurate or have been recorded unlawfully, it shall explain in writing to the data subject without excessive delay why it is not prepared to correct or erase the data.

That Member State shall also provide the data subject with information explaining the steps which he/she can take if he/she does not accept the explanation provided. This shall include information on how to bring an action or, if appropriate, a complaint before the competent authorities or courts of that Member State and any financial or other assistance that is available in accordance with the laws, regulations and procedures of that Member State.

⁵¹ **Pres** invites the **Cion** to consider agreeing to this change to the wording of the underlying Regulation that had not been originally included in the **Cion's** recast on the basis of the need for consistency within the Regulation.

⁵² **Pres** invites the **Cion** to consider agreeing to this change to the wording of the underlying Regulation that had not been originally included in the **Cion's** recast on the basis of the need for consistency within the Regulation.

7. Any request under paragraphs 2 and 3 shall contain all the necessary particulars to identify the data subject, including fingerprints. Such data shall be used exclusively to permit the exercise of the rights referred to in paragraphs 2 and 3 and shall be destroyed immediately afterwards.
8. The competent authorities of the Member States shall cooperate actively to enforce promptly the rights laid down in paragraphs 3, 4 and 5.
-

↓ new

9. Whenever a person requests data relating to him or her in accordance with paragraph 2, the competent authority shall keep a record in the form of a written document that such a request was made, and shall make this document available to the National Supervisory Authorities without delay, upon their request.
-

↓ 2725/2000/EC (adapted)

⇒ new

↻ Council

- ~~9.~~ 10. ↻ For the purposes as laid down in Article 1 (1) in⁵³ ↻ [...] ↻ each Member State, the national supervisory authority shall ⇒ on the basis of his/her request, ⇐ assist the data subject in accordance with Article 28(4) of Directive 95/46/EC in exercising his/her rights.

⁵³ Pres invites the Cion to consider agreeing to this change to the wording of the underlying Regulation that had not been originally included in the Cion's recast on the basis of the need for consistency within the Regulation.

~~10.~~ 11. ~~⇒~~ For the purposes as laid down in Article 1 (1) the⁵⁴ ~~☉~~ ~~⇒~~ [...] ~~☉~~ national supervisory authority of the Member State which transmitted the data and the national supervisory authority of the Member State in which the data subject is present shall assist and, where requested, advise him/her in exercising his/her right to correct or erase data. Both national supervisory authorities shall cooperate to this end. Requests for such assistance may be made to the national supervisory authority of the Member State in which the data subject is present, which shall transmit the requests to the authority of the Member State which transmitted the data. ~~The data subject may also apply for assistance and advice to the joint supervisory authority set up by Article 20.~~

~~11.~~ 12. In each Member State any person may, in accordance with the laws, regulations and procedures of that State, bring an action or, if appropriate, a complaint before the competent authorities or courts of the State if he/she is refused the right of access provided for in paragraph 2.

~~12.~~ 13. Any person may, in accordance with the laws, regulations and procedures of the Member State which transmitted the data, bring an action or, if appropriate, a complaint before the competent authorities or courts of that State concerning the data relating to him/her recorded in the ~~central database~~ ⇒ Central System ⇐, in order to exercise his/her rights under paragraph 3. The obligation of the national supervisory authorities to assist and, where requested, advise the data subject, in accordance with paragraph ~~10~~ ⇒ [...] ☉ ⇒ 11 ☉, shall subsist throughout the proceedings.

⁵⁴ **Pres** invites the **Cion** to consider agreeing to this change to the wording of the underlying Regulation that had not been originally included in the **Cion's** recast on the basis of the need for consistency within the Regulation.

Article 30 ~~19~~

⊗ Supervision by the ⊗ National ~~S~~upervisory ~~A~~uthority

1. ➡ For the purposes as laid down in Article 1 (1) each⁵⁵ Ⓞ ➡ [...] Ⓞ Member State shall provide that the national supervisory authority or authorities designated pursuant to Article 28(1) of Directive 95/46/EC shall monitor independently, in accordance with its respective national law, the lawfulness of the processing, in accordance with this Regulation, of personal data by the Member State in question, including their transmission to the Central ~~Unit~~ ⇒ System ⇐.
2. Each Member State shall ensure that its national supervisory authority has access to advice from persons with sufficient knowledge of fingerprint data.

↓ new

Ⓞ Council

Article 31

Supervision by the European Data Protection Supervisor

1. The European Data Protection Supervisor shall ensure that all the personal data processing activities concerning EURODAC, in particular by the Agency are carried out in accordance with Regulation (EC) No 45/2001 and this Regulation.

⁵⁵ Pres invites the Cion to consider agreeing to this change to the wording of the underlying Regulation that had not been originally included in the Cion's recast on the basis of the need for consistency within the Regulation.

2. The European Data Protection Supervisor shall ensure that an audit of the Agency's personal data processing activities is carried out in accordance with international auditing standards⁵⁶ at least every four years. A report of such audit shall be sent to the European Parliament, the Council, the Agency, the Commission and the National Supervisory Authorities. The Agency shall be given an opportunity to make comments before the report is adopted.

Article 32

Cooperation between National Supervisory Authorities and the European Data Protection Supervisor

1. The National Supervisory Authorities and the European Data Protection Supervisor, each acting within the scope of its respective competences, shall cooperate actively in the framework of their responsibilities and shall ensure coordinated supervision of EURODAC.
2. They shall, each acting within the scope of its respective competences, exchange relevant information, assist each other in carrying out audits and inspections, examine difficulties of interpretation or application of this Regulation, study problems with the exercise of independent supervision or in the exercise of the rights of data subjects, draw up harmonised proposals for joint solutions to any problems and promote awareness of data protection rights, as necessary.
3. The National Supervisory Authorities and the European Data Protection Supervisor shall meet for that purpose at least twice a year. The costs and servicing of these meetings shall be for the account of the European Data Protection Supervisor. Rules of procedure shall be adopted at the first meeting. Further working methods shall be developed jointly as necessary. A joint report of activities shall be sent to the European Parliament, the Council, the Commission and the Agency every two years.

⁵⁶ **DE** suggested providing for the term "international auditing standards" in detail in the operative body of the text. **Cion:** these standards do not have to be applied in the context of this Regulation.

Article 33

Protection of personal data for the purposes of the prevention, detection and investigation of terrorist offences [...] and of other serious criminal offences

1. [...] Each Member State shall provide that the provisions adopted under national law implementing Framework Decision 2008/977/JHA [...] are also applicable to the processing of [...] personal data by its national authorities for [...] the purposes as laid down in Article 1 (2) [...].
2. The processing of personal data by Europol pursuant to this Regulation shall be in accordance with Decision 2009/371/JHA and shall be supervised by an independent external data protection supervisor. The provisions of that Decision in Article 30 on the individual's rights of access, Article 31 on the data subject's right to correction and deletion of data and Article 32 on appeals shall therefore be applicable to the processing of personal data by Europol pursuant to this Regulation; the independent external data protection supervisor shall ensure that the rights of the individual are not violated.⁵⁷




⁵⁷ **DE:** the supervision of personal data-processing by EUROPOL should be addressed along the lines of Art 10(2) of the 2009 proposal for a Council Decision on requesting comparisons with EURODAC data by MS law enforcement authorities; to this effect, it suggested the following wording: “and shall be supervised by the independent joint supervisory body established by Art.34 of that Decision”. **Cion** expressed concerns about this suggestion and indicated that the EURODAC Regulation should not enter into such detail. Furthermore, the current wording is within the scope of Art. 34 of Framework Decision 2008/977.

3. Personal data obtained pursuant to this Regulation from EURODAC \Rightarrow for the purposes as laid down in Article 1 (2) \Leftarrow shall only be processed for the purposes of the prevention, detection and investigation of terrorist offences or of other serious criminal offences.
4. Personal data obtained by a Member State or Europol pursuant to this Regulation from EURODAC \Rightarrow for the purposes as laid down in Article 1 (2) \Leftarrow shall be erased in national and Europol files after a period of one month,⁵⁸ if the data are not required for a specific ongoing criminal investigation by that Member State, or Europol.
5. The monitoring of the lawfulness of the processing of personal data under this Regulation by the Member States \Rightarrow for the purposes as laid down in Article 1 (2) \Leftarrow , including their transmission to and from EURODAC shall be carried out by the national \Rightarrow [...] \Leftarrow \Rightarrow supervisory \Leftarrow authorities designated pursuant to Framework Decision 2008/977/JHA.

⁵⁸ **DE** pointed out that the one-month period for the deletion of the personal data is too short, given that the proceedings are usually long and complex. Moreover these data, once deleted, will not be available for the purpose of subsequent analysis, or data protection control. **Cion** stressed that if certain data is not required for a specific investigation it should be deleted as soon as possible.

Article 34

Data security

1. The Member State of origin shall ensure the security of the data before and during transmission to the Central System.
2. Each Member State shall, in relation to  [...]  all data processed by its relevant authorities pursuant to this Regulation,  , adopt the necessary measures, including a security plan, in order to:
 - (a) physically protect data, including by making contingency plans for the protection of critical infrastructure;
 - (b) deny unauthorised persons access to national installations in which the Member State carries out operations in accordance with the purpose of EURODAC (checks at entrance to the installation);
 - (c) prevent the unauthorised reading, copying, modification or removal of data media (data media control);
 - (d) prevent the unauthorised input of data and the unauthorised inspection, modification or erasure of stored personal data (storage control);
 - (e) prevent the unauthorised processing of data in EURODAC and any unauthorised modification or erasure of data processed in EURODAC (control of data entry);
 - (f) ensure that persons authorised to access EURODAC have access only to the data covered by their access authorisation, by means of individual and unique user identities and confidential access modes only (data access control);

- (g) ensure that all authorities with a right of access to EURODAC create profiles describing the functions and responsibilities of persons who are authorised to access, enter, update, erase and search the data and make these profiles available to the National Supervisory Authorities referred to in Article 25 of Framework Decision 2008/977/JHA without delay at their request (personnel profiles);
- (h) ensure that it is possible to verify and establish to which bodies personal data may be transmitted using data communication equipment (communication control);
- (i) ensure that it is possible to verify and establish what data have been processed in EURODAC, when, by whom and for what purpose (control of data recording);
- (j) prevent the unauthorised reading, copying, modification or erasure of personal data during the transmission of personal data to or from EURODAC or during the transport of data media, in particular by means of appropriate⁵⁹ encryption techniques (transport control);
- (k) monitor the effectiveness of the security measures referred to in this paragraph and take the necessary organisational measures related to internal monitoring to ensure compliance with this Regulation (self-auditing).

3. The Agency shall take the necessary measures in order to achieve the objectives set out in paragraph 2 as regards the operation of EURODAC, including the adoption of a security plan.

⁵⁹ **DE:** the following wording shall be added: "and state-of-the-art".

Article 35

Prohibition of transfers of data to third countries or to international bodies or to private parties

Personal data obtained by a Member State or Europol pursuant to this Regulation from the EURODAC central database shall not be transferred or made available to any third country or international organisation or a private entity established in or outside the European Union. This prohibition shall be without prejudice to the right of Member States to transfer such data to third countries to which the Dublin Regulation applies.⁶⁰

Article 36

Logging and documentation

1. Each Member State and Europol shall ensure that all data processing operations resulting from requests for comparison with EURODAC data for the purposes as laid down in Article 1 (2) are logged or documented for the purposes of checking the admissibility of the request monitoring the lawfulness of the data processing and data integrity and security and for self-monitoring.
2. The log or documentation shall show in all cases:
 - (a) the exact purpose of the request for comparison, including the concerned form of a terrorist offence or other serious criminal offence and for Europol, the exact purpose of the request for comparison;
 - (b) the respective national file reference;
 - (c) the date and exact time of the request for comparison by the National Access Point to the EURODAC Central System;

⁶⁰ **DE:** the following wording should be added: “provided that the requirements of Art. 13 of the Framework Decision 2008/977/JHA are fulfilled and it is guaranteed that the receiving country ensures compliance with the requirements under the first sentence (thereof)”.

- (d) the name of the authority having requested access for comparison, and the person responsible who has made the request and processed the data;
- (e) where applicable the use of the urgent procedure referred to in Article 19(3) and the decision taken with regard to the ex-post verification;
- (f) the data used for comparison;
- (g) according to national rules or the rules of the Europol decision the identifying mark of the official who carried out the search and of the official who ordered the search or supply.

3. Such logs or documentation shall be used only for the data protection monitoring of the lawfulness of data processing as well as to ensure data security. Only logs containing non-personal data may be used for the monitoring and evaluation referred to in Article 38. The competent national supervisory authorities responsible for checking the admissibility of the request and monitoring the lawfulness of the data processing and data integrity and security, shall have access to these logs at their request for the purpose of fulfilling their duties.

↓ 2725/2000/EC

⇒ new

Article 37 ~~17~~

Liability

1. Any person who, or Member State which, has suffered damage as a result of an unlawful processing operation or any act incompatible with the provisions laid down in this Regulation shall be entitled to receive compensation from the Member State responsible for the damage suffered. That State shall be exempted from its liability, in whole or in part, if it proves that it is not responsible for the event giving rise to the damage.

2. If failure of a Member State to comply with its obligations under this Regulation causes damage to the ~~central database~~ ⇒ Central System ⇐, that Member State shall be held liable for such damage, unless and insofar as the ~~Commission~~ ⇒ Agency or another Member State ⇐ failed to take reasonable steps to prevent the damage from occurring or to minimise its impact.
 3. Claims for compensation against a Member State for the damage referred to in paragraphs 1 and 2 shall be governed by the provisions of national law of the defendant Member State.
-

↓ new

CHAPTER VIII

AMENDMENTS TO THE REGULATION (EU) No 1077/2011

Article 38

Provisions amending Regulation (EU) No 1077/2011

1. Article 5 is replaced by the following:

“Article 5

Tasks relating to EURODAC

In relation to EURODAC, the Agency shall perform :

- (a) the tasks conferred on the Agency by Regulation (EU) No .../... [of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No {.../...}].

(b) tasks relating to training on the technical use of EURODAC.”

2. Article 12(1) is amended as follows:

(a) points (t), (u) and (v) are replaced by the following:

“(t) to adopt the reports on the technical functioning of SIS II pursuant to Article 50(4) of Regulation (EC) No 1987/2006 and Article 66(4) of Decision 2007/533/JHA respectively, of VIS pursuant to Article 50(3) of Regulation (EC) No 767/2008 and Article 17(3) of Decision 2008/633/JHA; and of EURODAC pursuant to Article 40(4) of Regulation (EU) No .../... [of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No {.../...} establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third country national or a stateless person] and to request comparisons with EURODAC data by Member States' law enforcement authorities for law enforcement purposes;

(u) to adopt the annual report on the activities of the Central System of EURODAC pursuant to Article 40(1) of Regulation (EU) No .../... [of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No .../...];

(v) to make comments on the European Data Protection Supervisor's reports on the audits pursuant to Article 45 of Regulation (EC) 1987/2006 , Article 42(2) of Regulation (EC) No 767/2008 and Article 31 (2) of Regulation (EU) No .../... [of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No .../...] and ensure appropriate follow-up of the audit;”

(b) point (x) is replaced by the following:

“(x) to compile statistics on the work of the Central System of EURODAC pursuant to Article 8(2) of Regulation (EU) No .../... [of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No {.../...}]”

(c) point (z) is replaced by the following:

“(z) to ensure annual publication of the list of authorities designated pursuant to Article 27(2) of Regulation (EU) No .../... [of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No .../...]”

3. In Article 15 paragraph (4) is replaced by the following:

“4. Europol and Eurojust may attend the meetings of the Management Board as observers when a question concerning SIS II, in relation to the application of Decision 2007/533/JHA, is on the agenda. Europol may also attend the meetings of the Management Board as observer when a question concerning VIS, in relation to the application of Decision 2008/633/JHA, is on the agenda or when a question concerning EURODAC, in relation with the application of Regulation (EU) No .../... [of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No .../...] is on the agenda.”

4. Article 17 is amended as follows:

(a) in paragraph 5 point (g) is replaced by the following:

“(g) without prejudice to Article 17 of the Staff Regulations, establish confidentiality requirements in order to comply with Article 17 of Regulation (EC) No 1987/2006, Article 17 of Decision 2007/533/JHA and Article 26(9) of Regulation (EC) No 767/2008 respectively and Article 4(6) of Regulation (EU) No .../... [of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No .../...];”

(b) in paragraph 6 point (i) is replaced by the following:

“(i) reports on the technical functioning of each large-scale IT system referred to in point (t) of Article 12(1) and the annual report on the activities of the Central System of EURODAC referred to in point (u) of Article 12(1), on the basis of the results of monitoring and evaluation.”

5. In Article 19 paragraph 3 is replaced by the following:

"3. Europol and Eurojust may each appoint a representative to the SIS II Advisory Group. Europol may also appoint a representative to the VIS and to the EURODAC Advisory Groups."

↓ 2725/2000/EC (adapted)

⇒ new

CHAPTER ~~VII~~ IX

FINAL PROVISIONS

Article 39 ~~21~~

Costs

1. The costs incurred in connection with the establishment and operation of the ~~Central Unit~~
⇒ Central System and the Communication Infrastructure ⇐ shall be borne by the general budget of the European Union.
2. The costs incurred by national ⇒ access points ⇐ ~~units~~ and the costs for connection to the ~~central database~~ ⇒ Central System ⇐ shall be borne by each Member State.

3. Each Member State and Europol shall set up and maintain at their expense the technical infrastructure necessary to implement this Regulation, and be responsible for bearing its costs resulting from requests for comparison with EURODAC data for the purposes of the prevention, detection or investigation of any of the criminal offences defined in this Regulation.⁶¹

~~3. The costs of transmission of data from the Member State of origin and of the findings of the comparison to that State shall be borne by the State in question.~~

Article ~~40~~ 24

Annual report: ~~m~~Monitoring and evaluation

1. The ~~Commission~~ ⇒ Agency ⇐ shall submit to the European Parliament and the Council an annual report on the activities of the Central ~~Unit~~ ⇒ System ⇐. The annual report shall include information on the management and performance of ~~Eurodac~~EURODAC against pre-defined quantitative indicators for the objectives referred to in paragraph 2.
2. The ~~Commission~~ ⇒ Agency ⇐ shall ensure that ☒ procedures ☒ systems are in place to monitor the functioning of the Central ~~Unit~~ ⇒ System ⇐ against objectives ☒ relating to ☒ ~~in terms of~~ outputs, cost-effectiveness and quality of service.

⁶¹ **DE:** reference should also be made to the costs of EUROPOL activities pursuant to Art. 21 of this proposal. Currently, Article 39 (3) provides for the costs incurred in connection with the necessary infrastructure and for “costs resulting from requests for comparison with EURODAC data for the purposes of the prevention, detection or investigation of any of the criminal offences defined in this Regulation”. This provision also expressly covers Europol. However, **DE** considers that there is a loophole caused by the access rights granted to Europol in Article 21. According to this provision, EUROPOL may file requests for comparison with EURODAC data within the limits of its mandate for the purposes of a specific analysis or general and strategic analyses. This also covers cases where comparison does not serve the purposes of prevention, detection or investigation of specific criminal offences. Such cases would not be covered by Article 39 (3).

3. ~~The Commission shall regularly evaluate the operation of the Central Unit in order to establish whether its objectives have been attained cost-effectively and with a view to providing guidelines for improving the efficiency of future operations.~~
 4. ~~One year after Eurodac starts operations, the Commission shall produce an evaluation report on the Central Unit, focusing on the level of demand compared with expectation and on operational and management issues in the light of experience, with a view to identifying possible short-term improvements to operational practice.~~
-

↓ new

3. For the purposes of technical maintenance, reporting and statistics, the Agency shall have access to the necessary information relating to the processing operations performed in the Central System.
4. Every two years, the Agency shall submit to the European Parliament, the Council, the Commission and the European Data Protection Supervisor a report on the technical functioning of the Central System, including the security thereof.

↓ 2725/2000/EC

⇒ new

5. Three years after ~~Eurodac starts operations~~ ⇒ the start of application of this Regulation as provided for in Article 46(2) ⇐ and every ~~six~~ ⇒ four ⇐ years thereafter, the Commission shall produce an overall evaluation of ~~Eurodac~~EURODAC, examining results achieved against objectives and assessing the continuing validity of the underlying rationale, and any implications for future operations ⇒ , as well as make any necessary recommendations ⇐ . ⇒ The Commission shall transmit the evaluation to the European Parliament and the Council. ⇐
-

↓ new

⇒ Council

6. Member States shall provide the Agency and the Commission with the information necessary to draft the reports referred to in paragraph 4 and 5.

7. ⇒ [...] ⇐

8. Each Member State and Europol shall prepare annual reports on the effectiveness of the comparison of fingerprint data with EURODAC data for law enforcement access purposes, containing information and statistics on the exact purpose of the comparison, including the type of a terrorist offence or a serious criminal offence, number of requests for comparison, the number and type of cases which have ended in successful identifications and on the need and use made of the exceptional case of urgency as well as on those cases where that urgency was not accepted by the ex post verification carried out by the verifying authority. Such reports shall be transmitted to the Commission.

9. The Agency, Member States and Europol shall provide the Commission the information necessary to draft the evaluation reports referred to in paragraph 5. This information shall not jeopardise working methods nor include information that reveals sources, staff members or investigations of the designated authorities.

↓ 2725/2000/EC (adapted)

⇒ new

↻ Council

Article ~~41~~ 25

Penalties⁶²

Member States shall take the necessary measures to ensure that any processing use of data recorded entered in the ~~central database~~ Central System contrary to the purpose of ~~Eurodac~~ EURODAC as laid down in Article 1⁶³ [...] shall be subject to appropriate penalties is punishable by penalties, including administrative and/or criminal penalties in accordance with national law, that are effective, proportionate and dissuasive.

⁶² DE suggested modifying the wording of the provision as follows: "The MS shall lay down the rules on penalties applicable to infringement of the provisions of this Regulation and shall take all measures necessary to ensure that they are implemented. The penalties provided for must be effective, proportionate and dissuasive"; DE pointed out that the current wording penalises any use of data stored in the Central System that is contrary to the purpose of this database, which it considered it too broad and imprecise. DE stressed that it cannot agree with the obligation to punish (even with fines and administrative penalties) every infringement of the Regulation (principle of discretionary prosecution).

⁶³ Pres invites the Cion to consider agreeing to this change to the wording of the underlying Regulation that had not been originally included in the Cion's recast on the basis of the need for consistency within the Regulation.

Article ~~42~~ 26

Territorial scope

The provisions of this Regulation shall not be applicable to any territory to which the Dublin Convention Regulation does not apply.

↓ new

Article 43

Notification of designated authorities and verifying authorities

1. By [three months after the date of entry into force of this Regulation] at the latest each Member State shall notify the Commission of its designated authorities and shall notify without delay any amendment thereto.
2. By [three months after the date of entry into force of this Regulation] at the latest each Member State shall notify the Commission of its verifying authority and shall notify without delay any amendment thereto.
3. By [three months after the date of entry into force of this Regulation] at the latest Europe shall notify the Commission of its verifying authority and the National Access Point which it has designated and shall notify without delay any amendment thereto.
4. The Commission shall publish information referred to in paragraphs 1, 2 and 3 in the *Official Journal of the European Union* on an annual basis.

↓ new

Article 44

Transitional provision

Data blocked in the Central System in accordance with Article 12 of Council Regulation (EC) No 2725/2000/EC shall be unblocked and marked in accordance with Article 18(1) of this Regulation on the date provided for in Article 46 of this Regulation.

Article 45

Repeal

Council Regulation (EC) No 2725/2000 of 11 December 2000 and Council Regulation (EC) No 407/2002 are repealed with effect from the date referred to in Article 46(2).

References to the repealed Regulations shall be read in accordance with the correlation table in Annex III.

↓ 2725/2000/EC Article 27 (adapted)

⇒ new

Article ~~46~~ 27

Entry into force and applicability

1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European ~~Communities~~ Union .

2. This Regulation shall apply \Rightarrow two years from the date of the entry into force of this Regulation. \Leftarrow ~~and Eurodac shall start operations, from the date which the Commission shall publish in the Official Journal of the European Communities, when the following conditions met:~~

~~(a) each Member State has notified the Commission that it has made the necessary technical arrangements to transmit data to the Central Unit in accordance with the implementing rules adopted under Article 4(7) and to comply with the implementing rules adopted under Article 12(5); and~~

~~(b) the Commission has made the necessary technical arrangements for the Central Unit to begin operations in accordance with the implementing rules adopted under Article 4(7) and Article 12(5).~~

3. Member States shall notify the Commission and the Agency as soon as they have made the technical arrangements to transmit data to the Central System, and in any event no later than two years from the date of the entry into force of this Regulation.

4. This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaties.

↓ 2725/2000/EC

Done at Brussels,

For the European Parliament
The President

For the Council
The President

↓ 407/2002/EC

⇒ new

ANNEX I

Data format for the exchange of fingerprint data

The following format is prescribed for the exchange of fingerprint data:

~~ANSI/NIST-CSL-1-1993~~ ⇒ ANSI/NIST-ITL 1a-1997, Ver.3, June 2001 (INT-1) ⇐ and any future further developments of this standard.

Norm for Member State identification letters

The following ISO norm will apply: ISO 3166 - 2 letters code.

Annex II

EURODAC – Fingerprint form

1.	Reference number	
2.	Place of the application for asylum or place where the third country national or stateless person was apprehended	
3.	Date of the application for asylum or date on which the third country national or stateless person was apprehended	
4.	Sex	
5.	Date on which the fingerprints were taken	
6.	Date on which the data were transmitted to the Central System	

ROLLED IMPRESSIONS

1. Right thumb	2. Right forefinger	3. Right middle finger	4. Right ring finger	5. Right little finger
40 mm	50 mm	40 mm	40 mm	40 mm
40 mm	40 mm	40 mm	40 mm	40 mm
6. Left thumb	7. Left forefinger	8. Left middle finger	9. Left ring finger	10. Left little finger
40 mm				

PLAIN IMPRESSIONS

LEFT HAND Four fingers taken simultaneously	TWO THUMBS Impressions taken simultaneously		RIGHT HAND Four fingers taken simultaneously
	LEFT	RIGHT	
75 mm	30 mm	30 mm	75 mm
65 mm	65 mm		



ANNEX II

Repealed Regulations
(referred to in Article 45)

Council Regulation (EC) No 2725/2000/EC (OJ L 316, 15.12.2000, p. 1.)

Council Regulation (EC) No 407/2002/EC (OJ L 062, 05.03.2002 p. 1.)

ANNEX III

Correlation table

Regulation 2725/2000/EC	This Regulation
Article 1(1)	Article 1(1)
Article 1(2), first subparagraph	Article 3(1)
Article 1(2), second subparagraph	Deleted
Article 1(2), third subparagraph	Article 3(4)
Article 1(3)	Article 1(3)
Article 2	Article 2
Article 3(1)	deleted
Article 3(2)	Article 3(3)
Article 3(3)	Article 8
Article 3(4)	Deleted
Article 4(1)	Article 9(1), 3(5)
Article 4(2)	Deleted
Article 4(3)	Article 9(3)
Article 4(4)	Article 9(4)
Article 4(5)	Article 9(5)
Article 4(6)	Article 25(4)
Article 5	Article 11
Article 6	Article 12

Article 7	Article 13
Article 8	Article 14
Article 9	Article 15
Article 10	Article 16
Article 11(1)-(4)	Article 17(1)-(4)
Article 11(5)	Deleted
Article 12	Article 18
Article 13	Article 23
Article 14	Deleted
Article 15	Article 27
Article 16	Article 28
Article 17	Article 37
Article 18	Article 29
Article 19	Article 30
Article 20	Deleted
Article 21	Article 39
Article 22	Deleted
Article 23	Deleted
Article 24	Article 40
Article 25	Article 24
Article 26	Article 42
Article 27	Article 46

Regulation 407/2002/EC

Article 2

Article 3

Article 4

Article 5(1)

Annex I

Annex II

This Regulation

Article 24

Article 25

Article 26

Article 3(3)

Annex I

Deleted

Anlage 5



EUROPEAN PARLIAMENT

2009 - 2014

Committee on Civil Liberties, Justice and Home Affairs

2008/0242(COD)

26.9.2012

*****|**

DRAFT REPORT

on the amended proposal for a regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No [...] (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person) and to request comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast)
(COM(2012)0254 – C7-0148/2012 – 2008/0242(COD))

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Monica Luisa Macovei

PR913490EN.doc

PE450.875v03-00

EN

United in diversity

EN

(Recast – Rule 87 of the Rules of Procedure)

Symbols for procedures

- * Consultation procedure
- *** Consent procedure
- ***I Ordinary legislative procedure (first reading)
- ***II Ordinary legislative procedure (second reading)
- ***III Ordinary legislative procedure (third reading)

(The type of procedure depends on the legal basis proposed by the draft act.)

Amendments to a draft act

In amendments by Parliament, amendments to draft acts are highlighted in ***bold italics***. Highlighting in *normal italics* is an indication for the relevant departments showing parts of the draft act which may require correction when the final text is prepared – for instance, obvious errors or omissions in a language version. Suggested corrections of this kind are subject to the agreement of the departments concerned.

The heading for any amendment to an existing act that the draft act seeks to amend includes a third line identifying the existing act and a fourth line identifying the provision in that act that Parliament wishes to amend. Passages in an existing act that Parliament wishes to amend, but that the draft act has left unchanged, are highlighted in **bold**. Any deletions that Parliament wishes to make in such passages are indicated thus: [...].

CONTENTS

	Page
DRAFT EUROPEAN PARLIAMENT LEGISLATIVE RESOLUTION	6
EXPLANATORY STATEMENT.....	19
ANNEX: LETTER FROM THE COMMITTEE ON LEGAL AFFAIRS.....	22
ANNEX: OPINION OF THE CONSULTATIVE WORKING PARTY OF THE LEGAL SERVICES OF THE EUROPEAN PARLIAMENT, THE COUNCIL AND THE COMMISSION	25

DRAFT EUROPEAN PARLIAMENT LEGISLATIVE RESOLUTION

on the amended proposal for a regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No [...] (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person) and to request comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast)

(COM(2012)0254 – C7-0148/2012 – 2008/0242(COD))

(Ordinary legislative procedure – recast)

The European Parliament,

- having regard to the amended Commission proposal to Parliament and the Council (COM(2012)0254),
 - having regard to Article 294(2), Article 78(2)(e), Article 87(2)(a) and Article 88(2)(a) of the Treaty on the Functioning of the European Union, pursuant to which the Commission submitted the proposal to Parliament (C7-0148/2012),
 - having regard to Article 294(3) of the Treaty on the Functioning of the European Union,
 - having regard to the Interinstitutional Agreement of 28 November 2001 on a more structured use of the recasting technique for legal acts¹,
 - having regard to the letter of 20 September 2012 from the Committee on Legal Affairs to the Committee on Civil Liberties, Justice and Home Affairs in accordance with Rule 87(3) of its Rules of Procedure,
 - having regard to Rules 87 and 55 of its Rules of Procedure,
 - having regard to the report of the Committee on Civil Liberties, Justice and Home Affairs (A7-0000/2012),
- A. whereas, according to the Consultative Working Party of the legal services of the European Parliament, the Council and the Commission, the proposal in question does not include any substantive amendments other than those identified as such in the proposal and whereas, as regards the codification of the unchanged provisions of the earlier acts together with those amendments, the proposal contains a straightforward codification of the existing texts, without any change in their substance;

1. Adopts its position at first reading hereinafter set out, taking into account the

¹ OJ C 77, 28.3.2002, p. 1.

recommendations of the Consultative Working Party of the legal services of the European Parliament, the Council and the Commission;

2. Calls on the Commission to refer the matter to Parliament again if it intends to amend its proposal substantially or replace it with another text;
3. Instructs its President to forward its position to the Council, the Commission and the national parliaments.

Amendment 1

Proposal for a regulation

Recital 4

Text proposed by the Commission

(4) For the purposes of applying **Council** Regulation (EU) No [...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], it is necessary to establish the identity of applicants for international protection and of persons apprehended in connection with the unlawful crossing of the external borders of the **Community**. It is also desirable, in order effectively to apply the **Council** Regulation (EU) No [...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], and in particular points (b) and (d) of Article 18(1) thereof, to allow each Member State to check whether a third country national or stateless person found illegally staying on its territory has applied for international protection in another Member State.

Amendment

(4) For the purposes of applying Regulation (EU) No [...] **of the European Parliament and of the Council** [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], it is necessary to establish the identity of applicants for international protection and of persons apprehended in connection with the unlawful crossing of the external borders of the **Union**. It is also desirable, in order effectively to apply Regulation (EU) No [...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], and in particular points (b) and (d) of Article 18(1) thereof, to allow each Member State to check whether a third country national or stateless person found illegally staying on its territory has applied for international protection in another Member State.

(The replacement of the term 'Community' by 'Union' applies throughout the text.)

Justification

The amendment is technical and aims to align the text to the provisions of the Lisbon Treaty.

Amendment 2**Proposal for a regulation****Recital 14***Text proposed by the Commission*

(14) In view of ensuring equal treatment for all applicants and beneficiaries of international protection, as well as in order to ensure consistency with current Union asylum *acquis*, in particular with **Council Directive 2004/83/EC of 29 April 2004 on minimum standards for the qualification and status of third country nationals or stateless persons as refugees or as persons who otherwise need international protection and the content of the protection granted** and Regulation (EU) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], it is appropriate to extend the scope of this Regulation to order to include applicants for subsidiary protection and persons enjoying subsidiary protection.

Amendment

(14) In view of ensuring equal treatment for all applicants and beneficiaries of international protection, as well as in order to ensure consistency with current Union asylum *acquis*, in particular with **Directive 2011/95/EU of the European Parliament and of the Council of 13 December 2011 on standards for the qualification of third-country nationals or stateless persons as beneficiaries of international protection, for a uniform status for refugees or for persons eligible for subsidiary protection, and for the content of the protection granted**¹ and Regulation (EU) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], it is appropriate to extend the scope of this Regulation to order to include applicants for subsidiary protection and persons enjoying subsidiary protection.

¹ *OJ L 337, 20.12.2011, p. 9.*

Justification

The amendment is technical and aims to align the text to the title of the amended

Amendment 3

**Proposal for a regulation
Recital 16 a (new)**

Text proposed by the Commission

Amendment

(16a) Member States should ensure the transmission of fingerprint data in an appropriate quality for the purpose of comparison by means of the computerised fingerprint recognition system. All authorities with right of access to EURODAC should invest in adequate training and in the necessary technological equipment. The authorities with right of access to EURODAC should inform the Agency of specific difficulties encountered with regard to the quality of data, in order to resolve them.

Or. en

Amendment 4

**Proposal for a regulation
Recital 35**

Text proposed by the Commission

Amendment

(35) Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data and in particular Articles 21 and 22 thereof concerning confidentiality and security of processing apply to the processing of personal data by Union institutions, bodies, offices and agencies carried out in application of this Regulation. However, certain points should

(35) Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data and in particular Articles 21 and 22 thereof concerning confidentiality and security of processing apply to the processing of personal data by Union institutions, bodies, offices and agencies carried out in application of this Regulation. However, certain points should

be clarified in respect of the responsibility for the processing of data and of the supervision of data protection.

be clarified in respect of the responsibility for the processing of data and of the supervision of data protection, ***bearing in mind that data protection is a key factor in the successful operation of EURODAC and that data security, high technical quality and lawfulness of consultations are essential to ensure the smooth and proper functioning of EURODAC as well as to facilitate the application of Regulation (EU) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person].***

Or. en

Amendment 5

Proposal for a regulation Recital 37

Text proposed by the Commission

(37) It is appropriate to monitor and evaluate the performance of EURODAC at regular intervals.

Amendment

(37) It is appropriate to monitor and evaluate the performance of EURODAC at regular intervals. ***The Agency should submit an annual report on the activities of the Central System to the European Parliament and to the Council.***

Or. en

Amendment 6

Proposal for a regulation Article 2 – paragraph 1 – point b

Text proposed by the Commission

(b) ***an*** "applicant for international

Amendment

(b) "applicant for international protection"

protection" means a third-country national or a stateless person who has made an application for international protection as defined in *Article 2(g) of Council Directive 2004/83/EC* in respect of which a final decision has not yet been taken;

means a third-country national or a stateless person who has made an application for international protection as defined in *Article 2(h) of Directive 2011/95/EU* in respect of which a final decision has not yet been taken;

Or. en

Justification

The amendment is technical and aims to align the text to the amended Qualification Directive.

Amendment 7

Proposal for a regulation

Article 2 – paragraph 1 – point c – point iii

Text proposed by the Commission

(iii) in relation to a person covered by Article 14, the Member State which transmits *such* data to the Central System and receives the results of the comparison;

Amendment

(iii) in relation to a person covered by Article 14, the Member State which transmits *the personal* data to the Central System and receives the results of the comparison;

Or. en

Justification

Terminology adaptation.

Amendment 8

Proposal for a regulation

Article 2 – paragraph 1 – point e

Text proposed by the Commission

(e) "hit" *shall mean* the existence of a match or matches established by the Central System by comparison between fingerprint data recorded in the central database and those transmitted by a Member State with regard to a person,

Amendment

(e) "hit" *means* the existence of a match or matches established by the Central System by comparison between fingerprint data recorded in the *computerised* central *fingerprint* database and those transmitted by a Member State with regard to a person,

without prejudice to the requirement that Member States shall immediately check the results of the comparison pursuant to Article 18(4);

without prejudice to the requirement that Member States shall immediately check the results of the comparison pursuant to Article 18(4);

Or. en

Justification

This amendment is technical and aims to align the wording to that present in Article 3(1)(a).

Amendment 9

Proposal for a regulation
Article 3 – paragraph 5

Text proposed by the Commission

5. The procedure for taking fingerprints shall be determined and applied in accordance with the national practice of the Member State concerned and in accordance with the safeguards laid down in the Charter of Fundamental Rights of the European Union, in the Convention for the Protection of Human Rights and Fundamental Freedoms and in the United Nations Convention on the Rights of the Child.

Amendment

5. The procedure for taking fingerprints shall be determined and applied in accordance with the national practice of the Member State concerned and in accordance with the safeguards laid down in the Charter of Fundamental Rights of the European Union, in the Convention for the Protection of Human Rights and Fundamental Freedoms and in the United Nations Convention on the Rights of the Child. ***The best interests of the child shall be a primary consideration of Member States in the application of this Regulation.***

Or. en

Justification

This amendment brings this Regulation in line with the Directive on minimum standards on procedures in Member States for granting and withdrawing international protection which specifies that the best interests of the child should be a primary consideration when implementing the Regulation. Also the EDPS in its 2008-2009 Activity Report highlighted the rights of persons subjected to age evaluations.

Amendment 10

Proposal for a regulation

Article 4 – paragraph 1

Text proposed by the Commission

1. The Agency, shall be responsible for the operational management of EURODAC. The Agency shall ensure, in cooperation with the Member States, that at all times the best available **technology**, subject to a cost-benefit analysis, **is** used for the Central System.

Amendment

1. The Agency shall be responsible for the operational management of EURODAC. The Agency shall ensure, in cooperation with the Member States, that at all times the best available **techniques**, subject to a cost-benefit analysis, **are** used for the Central System.

Or. en

Justification

The reference to "techniques" covers both the technology used and the way the installation is designed, built, maintained and operated as it is also suggested in the opinion of the European Data Protection Supervisor (EDPS) on Eurodac of 18 February 2009.

Amendment 11

Proposal for a regulation

Article 8 – paragraph 1 – introductory part

Text proposed by the Commission

1. The Agency shall draw up statistics on the work of the Central System every **month**, indicating in particular:

Amendment

1. The Agency shall draw up statistics on the work of the Central System every **quarter**, indicating in particular:

Or. en

Justification

Monthly statistics are too frequent and they would only overload the work of the Agency and of the institutions receiving them with the risk of not providing a relevant image of the activities reported on.

Amendment 12

Proposal for a regulation

Article 8 – paragraph 1 – point f

Text proposed by the Commission

(f) the number of **requests for marking and unmarking transmitted** in accordance with Article 18(1) and (2).

Amendment

(f) the number of **data sets marked** in accordance with Article 18(1) and (2);

Or. en

Justification

According to Article 18, it is the Member States which mark and unmark the relevant data. Statistics should contain the number of data sets marked and not the requests for such marking.

Amendment 13

Proposal for a regulation

Article 8 – paragraph 1 – point g

Text proposed by the Commission

(g) the number of hits for persons referred to in Article 18(1) for whom hits have been recorded under **points (b) and (d)** of this Article.

Amendment

(g) the number of hits for persons referred to in Article 18(1) for whom hits have been recorded under **points (b), (c) and (d)** of this Article.

Or. en

Amendment 14

Proposal for a regulation

Article 8 – paragraph 2

Text proposed by the Commission

2. At the end of each year, statistical data shall be established in the form of a compilation of the **monthly** statistics for that year, including an indication of the number of persons for whom hits have

Amendment

2. At the end of each year, statistical data shall be established in the form of a compilation of the **quarterly** statistics for that year, including an indication of the number of persons for whom hits have

been recorded under points (b), (c), and (d). The statistics shall contain a breakdown of data for each Member State.

been recorded under points (b), (c), and (d). The statistics shall contain a breakdown of data for each Member State.

Or. en

Justification

See the justification under Amendment 11.

Amendment 15

Proposal for a regulation

Article 9 – title

Text proposed by the Commission

Amendment

Collection, transmission and comparison of
fingerprints

Collection, transmission and comparison of
fingerprint data

Or. en

Justification

Technical amendment (harmonisation of wording in line with the titles of Articles 14 and 17).

Amendment 16

Proposal for a regulation

Article 9 – paragraph 2

Text proposed by the Commission

Amendment

2. By way of derogation from paragraph 1, where it is not possible to take the fingerprints of an applicant on account of measures taken to ensure the health of the applicant *or* the protection of public health, Member States shall take and send the fingerprints of the applicant as soon as possible and no later than 48 hours after these grounds no longer prevail.

2. By way of derogation from paragraph 1, where it is not possible to take the fingerprints of an applicant on account of measures taken to ensure the health of the applicant, *for* the protection of public health *or for technical reasons*, Member States shall take and send the fingerprints of the applicant as soon as possible and no later than 48 hours after these grounds no longer prevail.

Justification

Technical defects can occur at any time, hence the need for the addition.

Amendment 17

Proposal for a regulation
Article 14 – paragraph 5

Text proposed by the Commission

5. By way of derogation from paragraph 1, where it is not possible to take the fingerprints of such person on account of measures taken to ensure the health of the person *or* the protection of public health, the Member State concerned shall take and send the fingerprints of the person, in accordance with the deadline set out in paragraph 2, once these grounds no longer prevail.

Amendment

5. By way of derogation from paragraph 1, where it is not possible to take the fingerprints of such person on account of measures taken to ensure the health of the person, *for* the protection of public health *or for technical reasons*, the Member State concerned shall take and send the fingerprints of the person, in accordance with the deadline set out in paragraph 2, once these grounds no longer prevail.

Justification

Technical defects can occur at any time, hence the need for the addition.

Amendment 18

Proposal for a regulation
Article 21 – paragraph 1

Text proposed by the Commission

1. Requests for comparison with EURODAC data by Europol shall take place within the limits of its mandate and where necessary for the performance of its tasks pursuant to the Europol Decision *and for the purposes of a specific analysis or an analysis of a general nature and of a strategic type.*

Amendment

1. Requests for comparison with EURODAC data by Europol shall take place within the limits of its mandate and where necessary for the performance of its tasks pursuant to the Europol Decision.

Justification

This amendment is proposed in order to align the text with the conditions set forth in Article 20(1)(b).

Amendment 19**Proposal for a regulation****Article 29 – paragraph 1 – point e***Text proposed by the Commission*

(e) the ***existence of the*** right of access to data relating to him/her, and the right to request that inaccurate data relating to him/her be corrected or that unlawfully processed data relating to them be erased, as well as ***the right to receive information on*** the procedures for exercising those rights including the contact details of the controller and the National Supervisory Authorities referred to in Article 31(1).

Amendment

(e) the right of access to data relating to him/her, and the right to request that inaccurate data relating to him/her be corrected or that unlawfully processed data relating to them be erased, as well as the procedures for exercising those rights including the contact details of the controller and the National Supervisory Authorities referred to in Article 31(1).

Justification

The objective is to clarify that the person covered by the Regulation shall be informed about the "right of access to data relating to him/her" instead of "the existence of the right". In the same line it is clearer to indicate that the person will be informed about "the procedures for exercising the rights" as it has also been suggested by the European Data Protection Supervisor in its opinion.

Amendment 20**Proposal for a regulation****Article 29 – paragraph 1 – subparagraph 5***Text proposed by the Commission*

Where a person covered by this Regulation is a minor, Member States shall provide the information in an age-appropriate manner.

Amendment

Where a person covered by this Regulation is a minor, Member States shall provide the information in an age-appropriate manner.

The best interests of the child shall be a primary consideration of Member States when applying this Article.

Or. en

Justification

This amendment brings this Regulation in line with the Directive on minimum standards on procedures in Member States for granting and withdrawing international protection which specifies that the best interests of the child should be a primary consideration when implementing the Regulation. Also the EDPS in its 2008-2009 Activity Report highlighted the rights of persons subjected to age evaluations.

EXPLANATORY STATEMENT

EURODAC was established by Regulation (EC) No 2725/2000 concerning the establishment of "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention¹. The Commission adopted in December 2008² a recast proposal for the amendment of the EURODAC Regulation with the aim of ensuring a more efficient support to the application of the Dublin Regulation, properly addressing data protection concerns and taking into account developments in the asylum *acquis* and technical progress which took place since the adoption of the Regulation in 2000. It also aligned the IT management framework to that of the SIS II and VIS Regulations by providing for the taking over of the tasks of the operational management for EURODAC by the future Agency for the operational management of large-scale IT systems in the area of freedom, security and justice.³

In May 2009, the European Parliament adopted a legislative resolution⁴ endorsing the Commission proposal subject to a number of amendments.

The Commission adopted an amended proposal in September 2009 in order to, on the one hand, take into account the resolution of the European Parliament and the results of negotiations in the Council, and, on the other hand, introduce the possibility for Member States' law enforcement authorities and Europol to access the EURODAC central database for the purposes of prevention, detection and investigation of terrorist offences and other serious criminal offences.⁵ The proposal introduced a bridging clause to allow access for law enforcement purposes as well as the necessary accompanying provisions and amended the December 2008 proposal. At the same time the Commission put forward the Proposal for a Council Decision on requesting comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes⁶, which indicated the

¹ OJ L 062, 05.03.2002, p. 1.

² Proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No [...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], COM(2008)825 final.

³ The Proposal for a Regulation of the European Parliament and of the Council establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice [COM(2009) 293 final] was adopted on 24 June 2009. An amended proposal was adopted on 19 March 2010: Amended proposal for a Regulation (EU) No .../... of the European Parliament and of the Council on establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, COM(2010)93.

⁴ Establishment of 'Eurodac' for the comparison of fingerprints (recast), P6_TA(2009)0378.

⁵ Such a proposal was called for by Council Conclusions on access to Eurodac by Member States' police and law enforcement authorities as well as Europol of 12 and 13 June 2007.

⁶ COM(2009) 344.

precise modalities of such access.¹

The European Parliament did not issue a legislative resolution on the September 2009 proposals.

The Council Decision proposal lapsed as a result of the entry into force of the Lisbon Treaty. The Communication on the consequences of the entry into force of the Treaty of Lisbon for ongoing interinstitutional decision-making procedures² indicated that such proposal would be formally withdrawn and replaced with a new proposal to take account of the new framework of the Treaty on the Functioning of the European Union (TFEU).

The proposal submitted by the Commission on 11 October 2010 did not include the option of access for law enforcement purposes present in the September 2009 proposal and introduced two additional elements:

- in Article 18(4) the need for a check of the automated hit result by a fingerprint expert is clarified

- in Article 24(1) appropriate provisions are inserted in order to allow the committee under the Dublin Regulation to include information on EURODAC in the leaflet to be prepared under Article 4(3).

On 3 February 2011, the Committee on Civil Liberties, Justice and Home Affairs adopted an orientation vote on the Commission's proposal.

The current proposal withdraws the 2010 proposal and replaces it with a new one in order first to better take into account the resolution of the European Parliament and the results of negotiations in the Council; second to introduce the possibility for Member States' law enforcement authorities and Europol to access the EURODAC central database for the purposes of prevention, detection and investigation of terrorist offences and other serious criminal offences. Including law enforcement access for EURODAC was needed as part of a balanced deal on the negotiations of the Common European Asylum System package with a view to completing the package by the end of 2012.

Organised crime networks from third countries seek to abuse the asylum system to bring criminal members of a network into an EU Member State as contacts for their criminal business. Once within the territory of an EU Member State, these members of the organised crime network ask for asylum with false identities in order to get a legitimate stay in the EU without any criminal record. Moreover, information provided by Europol suggests that human traffickers also seek to abuse the asylum system by requesting asylum alleging a false country of origin. With these concerns in mind, your Rapporteur welcomes the possibility for Member States' designated authorities and the European Police Office (Europol) to request the comparison of fingerprint data -on a hit/no hit basis- with those stored in the EURODAC database for the fight against terrorist offences and other serious criminal offences. The Rapporteur believes that providing for the law enforcement access to EURODAC is a significant step forward from the last proposal, capable of preventing the type of situations described above while being accompanied by the necessary safeguards.

Your Rapporteur supports the Commission's proposal. She has put forward a series of

¹ COM(2010) 555, p.2-3.

² COM(2009) 665 final/2.

amendments that can be summed up in two categories: technical amendments (e.g.: alignment to Lisbon Treaty provisions, references to the recast proposal on "Qualification Directive", internal references) and amendments aimed at providing clarifications of the text (e.g.: replacement of term "technology" by "techniques" in Article 4, additions in the Statistics section and clarification concerning the right of access to data). Additional amendments aim to include relevant remarks of the European Data Protection Supervisor.

ANNEX: LETTER FROM THE COMMITTEE ON LEGAL AFFAIRS

Ref.: D(2012)46723

Mr Juan Fernando López Aguilar
Chair of the Committee on Civil Liberties, Justice and Home Affairs
ASP 11G306
Brussels

***Subject:** Amended proposal for a regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No [.../...] (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person) and to request comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast)
(COM(2012)0254 – C7-0148/2012 – 2008/0242(COD))*

Dear Chairman,

The Committee on Legal Affairs, which I am honoured to chair, has examined the proposal referred to above, pursuant to Rule 87 on Recasting, as introduced into the Parliament's Rules of Procedure.

Paragraph 3 of that Rule reads as follows:

"If the committee responsible for legal affairs considers that the proposal does not entail any substantive changes other than those identified as such in the proposal, it shall inform the committee responsible.

In such a case, over and above the conditions laid down in Rules 156 and 157, amendments shall be admissible within the committee responsible only if they concern those parts of the proposal which contain changes.

However, if in accordance with point 8 of the Interinstitutional Agreement, the committee responsible intends also to submit amendments to the codified parts of the proposal, it shall

immediately notify its intention to the Council and to the Commission, and the latter should inform the committee, prior to the vote pursuant to Rule 54, of its position on the amendments and whether or not it intends to withdraw the recast proposal."

Following the opinion of the Legal Service, whose representatives participated in the meetings of the Consultative Working Party examining the recast proposal, and in keeping with the recommendations of the draftsman, the Committee on Legal Affairs considers that the proposal in question does not include any substantive changes other than those identified as such in the proposal and that, as regards the codification of the unchanged provisions of the earlier acts with those changes, the proposal contains a straightforward codification of the existing texts, without any change in their substance.

In conclusion, after discussing it at its meeting of 17 September 2012, the Committee on Legal Affairs, by 17 votes in favour, 2 against and no abstentions¹, recommends that your Committee, as the committee responsible, proceed to examine the above proposal in accordance with Rule 87.

Yours faithfully,

Klaus-Heiner LEHNE

Encl.: Opinion of the Consultative Working Party.

¹ Members present : Charalampos Angourakis; Raffaele Baldassarre; Edit Bauer; Luigi Berlinguer; Sebastian Valentin Bodu; Piotr Borys; Françoise Castex; Christian Engström; Marielle Gallo; Eva Lichtenberger; Antonio Masip Hidalgo; Bernhard Rapkay; Evelyn Regner; Dagmar Roth-Behrendt; Rebecca Taylor; Alexandra Thein; Axel Voss; Cecilia Wikström; Tadeusz Zwiefka.

ANNEX: OPINION OF THE CONSULTATIVE WORKING PARTY OF THE LEGAL SERVICES OF THE EUROPEAN PARLIAMENT, THE COUNCIL AND THE COMMISSION



CONSULTATIVE WORKING PARTY
OF THE LEGAL SERVICES

Brussels, 18 July 2012

OPINION

**FOR THE ATTENTION OF THE EUROPEAN PARLIAMENT
THE COUNCIL
THE COMMISSION**

Amended Proposal for a regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No [.../...] (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person) and to request comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast)

COM(2012)0254 of 30.5.2012 – 2008/0242(COD)

Having regard to the Inter-institutional Agreement of 28 November 2001 on a more structured use of the recasting technique for legal acts, and in particular to point 9 thereof, the Consultative Working Party consisting of the respective legal services of the European Parliament, the Council and the Commission met on 14 and 20 June 2012 for the purpose of examining, among others, the aforementioned proposal submitted by the Commission.

At those meetings, an examination of the proposal for a Regulation of the European Parliament and of the Council recasting Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention and Council Regulation (EC) No 407/2002 of 28 February 2002 laying down certain rules to implement Regulation (EC) No 2725/2000 concerning the establishment of "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention resulted in the Consultative Working Party's establishing, by common accord, as follows.

1) As far as the explanatory memorandum is concerned, in order to be drafted in full compliance with the relevant requirements laid down by the Inter-institutional Agreement such a document should have specified which provisions of the earlier act remain unchanged in the proposal, as is provided for under point 6(a)(iii) of that agreement.

2) In the recast proposal, the following parts of text should have been marked with the grey-shaded type generally used for identifying substantive changes:

- in the title of the act, the final words "and to request comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice";

- in Article 8(1), introductory wording, in Article 24(1), (5) and (6) and in Article 26, the replacement of the words "Central Unit" with the word "Agency";

- in Article 9(3), the words "with exception to those transmitted in accordance with Article 10 point (b)";

- in Article 9(5), the replacement of the article number "5(1)" with the number "8(a) to (g)";

- in Article 17(4), the deletion of the words "and 6";

- in Article 24(2), the words "Article 14(2) and Article 17(2)";

- in Article 27(3), the deletion of the article number "12(4)(a)".

3) The existing wordings of Recitals 13, 14, 20 and 23 of Regulation (EC) No 2725/2000 should have been present in the text of the recast proposal. Those wordings should have been identified by using the double strikethrough and the grey-shaded type generally used for marking substantive changes consisting of the proposed deletion of existing texts.

4) In Article 2(1)(c)(i) the reference made to "Article 6" appears to be inaccurate and should be replaced by a correct reference.

5) In Article 2(1)(c)(ii) the reference made to "Article 11" should be adapted so as to read as a reference made to "Article 14".

6) In Article 2(1)(c)(iii) the reference made to "Article 14" should be adapted so as to read as a reference made to "Article 17".

7) In Article 2(e) the reference made to "Article 18(4)" should be adapted so as to read as a reference made to "Article 25(4)".

8) In Article 8(1)(a), the words "applicants for asylum and the", appearing before the word "persons" in the existing wording of Article 3(3), first subparagraph, point (a), of Regulation (EC) No 2725/2000, should have been present and should have been identified with double strikethrough.

9) In Article 9(3), the words "by the Central Unit", appearing between the words "shall be

compared" and "with the fingerprint data" in the existing wording of Article 4(3) of Regulation (EC) No 2725/2000, should have been present and should have been identified with double strikethrough.

10) In Article 16(2), the reference made to "Article 28(3)" should be adapted so as to read as a reference made to "Article 27(3)".

11) In Article 29(13), the reference made to "paragraph 13" should be adapted so as to read as a reference made to "paragraph 11".

12) The existing wording of Article 20 of Regulation (EC) No 2725/2000 should have been present and should have been identified with double strikethrough.

13) The introductory wording and points (a) and (b) of Article 1 of Regulation (EC) No 407/2002 should have been present in the recast text and should have been identified with double strikethrough. Point (c) of that same article should also have been present and should have been identified with double strikethrough and grey shaded type.

14) The existing wording of Article 5 of Regulation (EC) No 407/2002 should have been present in the recast text and should have been identified with double strikethrough.

In consequence, examination of the proposal has enabled the Consultative Working Party to conclude, without dissent, that the proposal does not comprise any substantive amendments other than those identified as such. The Working Party also concluded, as regards the codification of the unchanged provisions of the earlier act with those substantive amendments, that the proposal contains a straightforward codification of the existing legal text, without any change in its substance.

C. PENNERA

H. LEGAL

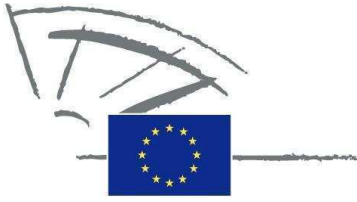
L. ROMERO REQUENA

Jurisconsult

Jurisconsult

Director General

Anlage 6



2008/0242(COD)

12.11.2012

AMENDMENTS

21 - 182

Draft report
Monica Luisa Macovei
(PE450.875v03-00)

on the amended proposal for a regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No [...] (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person) and to request comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (recast)

Proposal for a regulation
(COM(2012)0254 – C7-0148/2012 – 2008/0242(COD))

AM_Com_LegReport

Amendment 21
Franziska Keller, Jan Philipp Albrecht

Proposal for a regulation
Recital 2

Text proposed by the Commission

(2) A common policy on asylum, including a Common European Asylum System, is a constituent part of the European Union's objective of progressively establishing an area of freedom, security and justice open to those who, forced by circumstances, **legitimately** seek international protection in the Union.

Amendment

(2) A common policy on asylum, including a Common European Asylum System, is a constituent part of the European Union's objective of progressively establishing an area of freedom, security and justice open to those who, forced by circumstances, seek international protection in the Union.

Or. en

Amendment 22
Franziska Keller, Jan Philipp Albrecht

Proposal for a regulation
Recital 7

Text proposed by the Commission

(7) The Hague Programme called for the improvement of access to existing data filing systems in the European Union. In addition, The Stockholm Programme called for well targeted data collection and a development of information exchange and its tools that is driven by law enforcement needs.

Amendment

deleted

Or. en

Amendment 23
Cornelis de Jong

Proposal for a regulation

Recital 7

Text proposed by the Commission

Amendment

(7) The Hague Programme called for the improvement of access to existing data filing systems in the European Union. In addition, The Stockholm Programme called for well targeted data collection and a development of information exchange and its tools that is driven by law enforcement needs.

deleted

Or. en

Amendment 24 Cornelis de Jong

Proposal for a regulation Recital 8

Text proposed by the Commission

Amendment

(8) It is essential in the fight against terrorist offences and other serious criminal offences for the law enforcement authorities to have the fullest and most up-to-date information if they are to perform their tasks. The information contained in EURODAC is necessary for the purposes of the prevention, detection and investigation of terrorist offences and other serious criminal offences. Therefore, the data in EURODAC should be available, subject to the conditions set out in this Regulation, for comparison by the designated authorities of Member States and Europol.

deleted

Or. en

Amendment 25 Sarah Ludford

Proposal for a regulation
Recital 8 a (new)

Text proposed by the Commission

Amendment

(8a) The powers granted to law enforcement authorities to access EURODAC should be without prejudice to the right of the applicants for international protection to have his or her application processed in due course according to the relevant legislation. Furthermore, obtaining a 'hit' from EURODAC and a subsequent procedure according to Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union¹ should also be without prejudice to this right and should not be grounds for slowing down the process of examining the applicant's claim to asylum.

¹ OJ L 386, 29.12.2006, p. 89.

Or. en

Justification

It is important that Member States do not put in place practices which would link a possible result in EURODAC to the success of the asylum application since only a final judgement should have a bearing on this.

Amendment 26
Cornelis de Jong

Proposal for a regulation
Recital 9

Text proposed by the Commission

Amendment

(9) The Commission outlined in its Communication to the Council and the

deleted

European Parliament on improved effectiveness, enhanced interoperability and synergies among European data bases in the area of Justice and Home Affairs of 24 November 2005 that authorities responsible for internal security could have access to EURODAC in well defined cases, when there would be a substantiated suspicion that the perpetrator of a terrorist or other serious criminal offence has applied for asylum. In this Communication the Commission also found that the proportionality principle requires that EURODAC be queried for these purposes only once there is an overriding public security concern, that is, if the act committed by the criminal or terrorist to be identified is so reprehensible that it justifies querying a database that registers persons with a clean criminal record and it concluded that the threshold for authorities responsible for internal security to query EURODAC must therefore always be significantly higher than the threshold for querying criminal databases.

Or. en

Amendment 27
Cornelis de Jong

Proposal for a regulation
Recital 10

Text proposed by the Commission

Amendment

(10) Moreover, Europol has a key role with respect to cooperation between Member States' authorities in the field of cross-border crime investigation in supporting Union-wide crime prevention, analyses and investigation. Consequently, Europol should also have access to EURODAC data within the framework of its tasks and in accordance with the

deleted

**Decision establishing the European
Police Office (Europol) No
(2009/371/JHA).**

Or. en

**Amendment 28
Renate Weber**

**Proposal for a regulation
Recital 10 a (new)**

Text proposed by the Commission

Amendment

***(10a) Access to EURODAC data by
Europol should be allowed only for
specific cases, under specific
circumstances and under strict conditions.***

Or. en

**Amendment 29
Cornelis de Jong**

**Proposal for a regulation
Recital 11**

Text proposed by the Commission

Amendment

***(11) Since EURODAC has been
established to facilitate the application of
Council Regulation (EU) No [.../...]
[establishing the criteria and mechanisms
for determining the Member State
responsible for examining an application
for international protection lodged in one
of the Member States by a third-country
national or a stateless person], access to
EURODAC for the purposes of
preventing, detecting or investigating
terrorist offences and other serious
criminal offences constitutes a change of
the original purpose of EURODAC,
which interferes with the right to respect***

deleted

the private life of individuals whose personal data are processed in EURODAC. Any such interference must be in accordance with the law, which must be formulated with sufficient precision to allow individuals to adjust their conduct and it must protect individuals against arbitrariness and indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise. Any interference must be necessary in a democratic society to attain a legitimate and proportionate interest and proportionate to the legitimate objective it aims to achieve.

Or. en

Amendment 30
Cornelis de Jong

Proposal for a regulation
Recital 12

Text proposed by the Commission

Amendment

(12) Even though the original purpose for the establishment of EURODAC did not require the facility of requesting comparisons of data with the database on the basis of a latent which is the dactyloscopic trace which may be found at a crime scene, such a facility is a fundamental one in the field of police cooperation. The possibility to compare a latent with the fingerprint data which is stored in EURODAC will provide the designated authorities of the Member States with a very valuable tool in preventing, detecting and investigating terrorist offences and other serious criminal offences, when for example the only evidence available at a crime scene are latents. *deleted*

Amendment 31
Sarah Ludford

Proposal for a regulation
Recital 12

Text proposed by the Commission

(12) Even though the original purpose for the establishment of EURODAC did not require the facility of requesting comparisons of data with the database on the basis of a latent which is the dactyloscopic trace which may be found at a crime scene, such a facility is a fundamental one in the field of police cooperation. The possibility to compare a latent with the fingerprint data which is stored in EURODAC will provide the designated authorities of the Member States with a very valuable tool in preventing, detecting and investigating terrorist offences and other serious criminal offences, when for example the only evidence available at a crime scene are latents.

Amendment

(12) Even though the original purpose for the establishment of EURODAC did not require the facility of requesting comparisons of data with the database on the basis of a latent which is the dactyloscopic trace which may be found at a crime scene, such a facility is a fundamental one in the field of police cooperation. The possibility to compare a latent with the fingerprint data which is stored in EURODAC ***in cases where there are reasonable grounds for believing that the perpetrator or victim may fall into one of the categories covered by this Regulation*** will provide the designated authorities of the Member States with a very valuable tool in preventing, detecting and investigating terrorist offences and other serious criminal offences, when for example the only evidence available at a crime scene are latents.

Or. en

Justification

Since EURODAC should only be used in cases where there is a reasonable suspicion that an asylum seeker or other person covered by the EURODAC Regulation has been the perpetrator or victim, this principle should be underlined in cases where the police are collecting fingerprint evidence from a crime scene.

Amendment 32
Renate Weber

Proposal for a regulation
Recital 12 a (new)

Text proposed by the Commission

Amendment

(12a) The results of the comparison should be immediately checked in the Member State of origin by a fingerprint expert. Final identification should be made by the Member State of origin in cooperation with the Member States concerned, pursuant to Article 32 of Regulation (EU) No [.../...] of the European Parliament and of the Council [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person].

Or. en

Amendment 33
Renate Weber

Proposal for a regulation
Recital 12 b (new)

Text proposed by the Commission

Amendment

(12b) Information received from the Central System relating to other data found to be unreliable should be erased as soon as the unreliability of the data is established.

Or. en

Amendment 34
Cornelis de Jong

Proposal for a regulation

Recital 13

Text proposed by the Commission

(13) This Regulation also lays down the conditions under which requests for comparison of fingerprint data with EURODAC data for the purposes of preventing, detecting or investigating terrorist offences and other serious criminal offences should be allowed and the necessary safeguards to ensure the protection of the fundamental right to respect for the private life of individuals whose personal data are processed in EURODAC.

Amendment

deleted

Or. en

Amendment 35 Cornelis de Jong

Proposal for a regulation Recital 14

Text proposed by the Commission

(14) ***In*** view of ensuring equal treatment for all applicants and beneficiaries of international protection, as well as in order to ensure consistency with current Union asylum acquis, in particular with *Council Directive 2004/83/EC of 29 April 2004 on minimum standards for the qualification and status of third country nationals or stateless persons as refugees or as persons who otherwise need international protection and the content of the protection granted¹* and Regulation (EU) No [...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], it is appropriate to ***extent*** the scope of this

Amendment

(14) ***With a*** view of ensuring equal treatment for all applicants ***for*** and beneficiaries of international protection, as well as in order to ensure consistency with ***the*** current Union asylum acquis, in particular with *Directive 2011/95/EU of the European Parliament and of the Council of 13 December 2011 on standards for the qualification of third-country nationals or stateless persons as beneficiaries of international protection, for a uniform status for refugees and for persons eligible for subsidiary protection, and for the content of the protection granted¹* and Regulation (EU) No [...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of

Regulation *to* order to include applicants for subsidiary protection and persons enjoying subsidiary protection.

¹ OJL 304, 30.9.2004, p. 12.

the Member States by a third-country national or a stateless person], it is appropriate to *extend* the scope of this Regulation *in* order to include applicants for subsidiary protection and persons enjoying subsidiary protection.

¹ OJL 337, 20.12.2011, p. 9.

Or. en

Amendment 36
Sarah Ludford, Franziska Keller

Proposal for a regulation
Recital 16 a (new)

Text proposed by the Commission

Amendment

(16a) A temporary or permanent impossibility to provide fingerprints on the part of the applicant for international protection ('failure to enrol') should not adversely affect the legal situation of the individual.

Or. en

Justification

Articles 9, 14 and 17 of the proposal envisage a temporary situation in which it is not possible to take the fingerprint of an individual concerned by this measure. It should be clarified that neither a temporary or permanent failure to enrol should adversely affect the individual.

Amendment 37
Franziska Keller, Jan Philipp Albrecht

Proposal for a regulation
Recital 17

Text proposed by the Commission

Amendment

(17) Hits obtained from EURODAC should

(17) Hits obtained from EURODAC should

PE500.400v01-00

12/100

AM917925EN.doc

be verified by a fingerprint expert in order to ensure the accurate determination of responsibility under Regulation (EU) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person].

be verified by a **trained** fingerprint expert in order to ensure the accurate determination of responsibility under Regulation (EU) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person].

Or. en

Amendment 38
Cornelis de Jong

Proposal for a regulation
Recital 21

Text proposed by the Commission

(21) The European Agency for the operational management of large-scale information systems in the area of freedom security and justice established by Regulation (EU) n° 1077/2011 of the European Parliament and of the Council of 25 October 2011 (the "Agency") has been entrusted with the Commission's tasks relating to the operational management of EURODAC in accordance with this Regulation and with certain *taks* relating to the communication infrastructure as from the date on which the Agency takes up its responsibilities as of 1 December 2012. The Agency should take up the tasks entrusted to it under this Regulation and the relevant provisions of Regulation (EU) No 1077/2011 should be amended accordingly. ***In addition, Europol should have observer status at the meetings of the Management Board of the Agency, when a question in relation to the application of this Regulation concerning access for consultation of Eurodac by designated authorities of Member States and by***

Amendment

(21) The European Agency for the operational management of large-scale information systems in the area of freedom security and justice established by Regulation (EU) n° 1077/2011 of the European Parliament and of the Council of 25 October 2011 (the "Agency") has been entrusted with the Commission's tasks relating to the operational management of EURODAC in accordance with this Regulation and with certain *tasks* relating to the communication infrastructure as from the date on which the Agency takes up its responsibilities as of 1 December 2012. The Agency should take up the tasks entrusted to it under this Regulation and the relevant provisions of Regulation (EU) No 1077/2011 should be amended accordingly.

Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences is on the agenda. Europol should be able to appoint a representative to the Eurodac Advisory Group of the Agency.

Or. en

Amendment 39
Cornelis de Jong

Proposal for a regulation
Recital 24

Text proposed by the Commission

Amendment

(24) It is necessary to designate the competent Member States' authorities as well as the National Central Access Point through which the requests for comparison with EURODAC data are done and to keep a list of the operating units within the designated authorities that are authorised to request such comparison for the specific purposes of the prevention, detection and investigation of terrorist offences as referred to in the Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism and of other serious criminal offences as referred to in the Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States.

deleted

Or. en

Amendment 40
Cornelis de Jong

Proposal for a regulation
Recital 25

Text proposed by the Commission

Amendment

(25) Requests for comparison with data stored in the EURODAC central database shall be made by the operating units within the designated authorities to the National Access Point, through the verifying authority and shall be reasoned. The operating units within the designated authorities that are authorised to request comparisons with EURODAC data shall not act as a verifying authority. The verifying authorities should be responsible for ensuring strict compliance with the conditions for access as established in this Regulation. The verifying authorities should then forward the request for comparison through the National Access Point to the EURODAC Central System following verification of whether all conditions for access are fulfilled. In the exceptional case of urgency where early access is necessary to respond to a specific and actual threat related to terrorist offences or serious crime, the verifying authority should process the request immediately and only do the verification afterwards.

deleted

Or. en

Amendment 41
Sarah Ludford

Proposal for a regulation
Recital 25

Text proposed by the Commission

Amendment

(25) Requests for comparison with data stored in the EURODAC central database shall be made by the operating units within the designated authorities to the National

(25) Requests for comparison with data stored in the EURODAC central database shall be made by the operating units within the designated authorities to the National

Access Point, through the verifying authority and shall be reasoned. The operating units within the designated authorities that are authorised to request comparisons with EURODAC data shall not act as a verifying authority. The verifying authorities should be responsible for ensuring strict compliance with the conditions for access as established in this Regulation. The verifying authorities should then forward the request for comparison through the National Access Point to the EURODAC Central System following verification of whether all conditions for access are fulfilled. In the exceptional case of urgency where early access is necessary to respond to a specific and actual threat related to terrorist offences or serious crime, the verifying authority should process the request immediately and only do the verification afterwards.

Access Point, through the verifying authority and shall be reasoned. The operating units within the designated authorities that are authorised to request comparisons with EURODAC data shall not act as a verifying authority. The verifying authorities should be ***independent of the designated authorities*** and responsible for ensuring strict compliance with the conditions for access as established in this Regulation. The verifying authorities should then forward the request for comparison through the National Access Point to the EURODAC Central System following verification of whether all conditions for access are fulfilled. In the exceptional case of urgency where early access is necessary to respond to a specific and actual threat related to terrorist offences or serious crime, the verifying authority should process the request immediately and only do the verification afterwards.

Or. en

Amendment 42
Cornelis de Jong

Proposal for a regulation
Recital 26

Text proposed by the Commission

(26) For the purposes of protection of personal data, and to exclude systematic comparisons which should be forbidden, the processing of EURODAC data should only take place on a case-by-case basis and when it is necessary for the purposes of preventing, detecting and investigating terrorist offences and other serious criminal offences. In addition access should only be allowed when comparisons with the national databases of the Member State and with the Automated

Amendment

deleted

Fingerprint Databases of other Member States under the Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime have returned negative results. This condition requires prior implementation of the Council Decision as it shall not be permitted to conduct a EURODAC check for law enforcement purposes where these above steps have not been first undertaken. A specific case exists in particular when the request for comparison is connected to a specific and concrete situation or to a specific and concrete danger associated with a terrorist or other serious criminal offence, or to specific persons in respect of whom there are serious grounds for believing that the persons will commit or have committed terrorist offences or other serious criminal offences. A specific case also exists when the request for comparison is connected to a person who is a victim of a terrorist or other serious criminal offence. The designated authorities and Europol should thus only request a comparison with EURODAC when they have reasonable grounds to believe that such a comparison will provide information that will substantially assist them in preventing, detecting or investigating a terrorist or other serious criminal offence.

Or. en

Amendment 43
Sarah Ludford

Proposal for a regulation
Recital 26

Text proposed by the Commission

Amendment

(26) For the purposes of protection of

(26) For the purposes of protection of

personal data, and to exclude systematic comparisons which should be forbidden, the processing of EURODAC data should only take place on a case-by-case basis and when it is necessary for the purposes of preventing, detecting and investigating terrorist offences and other serious criminal offences. In addition access should only be allowed when comparisons with the national databases of the Member State *and* with the Automated Fingerprint Databases of other Member States under the Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime have returned negative results. This condition requires prior implementation of *the* Council Decision as it shall not be permitted to conduct a EURODAC check for law enforcement purposes where these above steps have not been first undertaken. A specific case exists in particular when the request for comparison is connected to a specific and concrete situation or to a specific and concrete danger associated with a terrorist or other serious criminal offence, or to specific persons in respect of whom there are serious grounds for believing that the persons will commit or have committed terrorist offences or other serious criminal offences. A specific case also exists when the request for comparison is connected to a person who is a victim of a terrorist or other serious criminal offence. The designated authorities and Europol should thus only request a comparison with EURODAC when they have reasonable grounds to believe that such a comparison will provide information that will substantially assist them in preventing, detecting or investigating a terrorist or other serious criminal offence.

personal data, and to exclude systematic comparisons which should be forbidden, the processing of EURODAC data should only take place on a case-by-case basis and when it is necessary for the purposes of preventing, detecting and investigating terrorist offences and other serious criminal offences. In addition access should only be allowed when comparisons with the national databases of the Member State, with the Automated Fingerprint Databases of other Member States under the Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime have returned negative results. This condition requires prior implementation of Council Decision *2008/615/JHA* as it shall not be permitted to conduct a EURODAC check for law enforcement purposes where these above steps have not been first undertaken. *Designated authorities should also be encouraged to consult the Visa Information System under Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences¹ where appropriate prior to consulting EURODAC.* A specific case exists in particular when the request for comparison is connected to a specific and concrete situation or to a specific and concrete danger associated with a terrorist or other serious criminal offence, or to specific persons in respect of whom there are serious grounds for believing that the persons will commit or have committed terrorist offences or other serious criminal offences. A specific case also exists when the request for comparison is connected to a person who is a victim of a terrorist or other serious criminal offence. The designated authorities and Europol should

thus only request a comparison with EURODAC when they have reasonable grounds to believe that such a comparison will provide information that will substantially assist them in preventing, detecting or investigating a terrorist or other serious criminal offence.

¹ OJ L 218, 13.8.2008, p. 129.

Or. en

Justification

Prior consultation of the Visa Information System before checking Eurodac is desirable. However, as this is not technically feasible and not always appropriate in all cases, it should only be done when possible.

Amendment 44

Claude Moraes, Carmen Romero López, Birgit Sippel

Proposal for a regulation

Recital 26

Text proposed by the Commission

(26) For the purposes of protection of personal data, and to exclude systematic comparisons which should be forbidden, the processing of EURODAC data should only take place on a case-by-case basis and when it is necessary for the purposes of preventing, detecting and investigating terrorist offences and other serious criminal offences. In addition access should only be allowed when comparisons with the national databases of the Member State and with the Automated Fingerprint Databases of other Member States under the Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime have returned negative results. This condition

Amendment

(26) For the purposes of protection of personal data, and to exclude systematic comparisons which should be forbidden, the processing of EURODAC data should only take place on a case-by-case basis and when it is necessary for the purposes of preventing, detecting and investigating terrorist offences and other serious criminal offences. In addition access should only be allowed when comparisons with the national databases of the Member State, ***the Visa Information System*** and with the Automated Fingerprint Databases of other Member States under the Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime have returned negative

requires prior implementation of the Council Decision as it shall not be permitted to conduct a EURODAC check for law enforcement purposes where these above steps have not been first undertaken. A specific case exists in particular when the request for comparison is connected to a specific and concrete situation or to a specific and concrete danger associated with a terrorist or other serious criminal offence, or to specific persons in respect of whom there are serious grounds for believing that the persons will commit or have committed terrorist offences or other serious criminal offences. A specific case also exists when the request for comparison is connected to a person who is a victim of a terrorist or other serious criminal offence. The designated authorities and Europol should thus only request a comparison with EURODAC when they have reasonable grounds to believe that such a comparison will provide information that will substantially assist them in preventing, detecting or investigating a terrorist or other serious criminal offence.

results. This condition requires prior implementation of the Council Decision as it shall not be permitted to conduct a EURODAC check for law enforcement purposes where these above steps have not been first undertaken. A specific case exists in particular when the request for comparison is connected to a specific and concrete situation or to a specific and concrete danger associated with a terrorist or other serious criminal offence, or to specific persons in respect of whom there are serious grounds for believing that the persons will commit or have committed terrorist offences or other serious criminal offences. A specific case also exists when the request for comparison is connected to a person who is a victim of a terrorist or other serious criminal offence. The designated authorities and Europol should thus only request a comparison with EURODAC when they have reasonable grounds to believe that such a comparison will provide information that will substantially assist them in preventing, detecting or investigating a terrorist or other serious criminal offence.

Or. en

Justification

All current EU systems should be used first before Eurodac is accessed.

Amendment 45 Cornelis de Jong

Proposal for a regulation Recital 27

Text proposed by the Commission

(27) In case the requesting Member State establishes that EURODAC data pertains to a minor, these data may only be used

Amendment

deleted

for law enforcement purposes by the requesting Member State in accordance with that State's laws for minors and in accordance with the obligation to give primary consideration to the child's best interest.

Or. en

Amendment 46
Franziska Keller, Jan Philipp Albrecht

Proposal for a regulation
Recital 29

Text proposed by the Commission

(29) *In accordance with the principle of subsidiarity as set out in Article 5 of the Treaty, the objective of the proposed measures, namely the creation of a system for the comparison of fingerprint data to assist the implementation of the Community's asylum policy, cannot, by its very nature, be sufficiently achieved by the Member States and can therefore be better achieved by the Community. In accordance with the principle of proportionality as set out in the said Article, this Regulation does not go beyond what is necessary to achieve those objectives.*

Amendment

(29) *Since the objective of this Regulation, namely the creation of a system for the comparison of fingerprint data to assist the implementation of the Union asylum policy, cannot, by its very nature, be sufficiently achieved by the Member States and can therefore be better achieved at Union level, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.*

Or. en

Amendment 47
Cornelis de Jong

Proposal for a regulation
Recital 30

Text proposed by the Commission

(30) Directive 95/46/EC of the European

Amendment

(30) Directive 95/46/EC of the European

Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data applies to the processing of personal data by the Member States carried out in application of this Regulation *within the framework of the Eurodac system unless such processing takes place by Member States' designated authorities for the purposes of the prevention, detection and investigation of terrorist offences and other serious criminal offences.*

Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data applies to the processing of personal data by the Member States carried out in application of this Regulation.

Or. en

Amendment 48
Cornelis de Jong

Proposal for a regulation
Recital 31

Text proposed by the Commission

(31) Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters applies to all processing of personal data by Member States' designated authorities for the purposes of the prevention, detection and investigation of terrorist offences and other serious criminal offences pursuant to this Regulation.

Amendment

deleted

Or. en

Amendment 49
Sarah Ludford, Franziska Keller

Proposal for a regulation

Recital 33

Text proposed by the Commission

(33) Transfers of data obtained pursuant to this Decision to third countries or international organisations or private entities should be prohibited, in order to ensure the right to asylum and to safeguard applicants for international protection from having their data disclosed to any third country. This prohibition shall be without prejudice to the right of Member States to transfer such data to third countries to which Regulation (EU) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] applies, in order to ensure that Member States have the possibility of cooperating with such third countries for the purposes of this Regulation.

Amendment

(33) Transfers of data obtained pursuant to this Decision to third countries or international organisations or private entities should be prohibited, in order to ensure the right to asylum and to safeguard applicants for international protection from having their data disclosed to any third country. This prohibition shall be without prejudice to the right of Member States to transfer such data to third countries to which Regulation (EU) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] applies, in order to ensure that Member States have the possibility of cooperating with such third countries for the purposes of this Regulation. ***The prohibition of transfer to third countries should cover both EURODAC data obtained under this Regulation and personal data exchanged bilaterally subsequent to a EURODAC search which are stored or processed at national level.***

Or. en

Justification

This complements the amendment to Article 35. It is important to ensure that the risk of the asylum seeker's application becoming known to their state of origin is minimised.

Amendment 50

Claude Moraes, Carmen Romero López, Birgit Sippel

Proposal for a regulation

Recital 33

Text proposed by the Commission

(33) Transfers of data obtained pursuant to this Decision to third countries or international organisations or private entities should be prohibited, in order to ensure the right to asylum and to safeguard applicants for international protection from having their data disclosed to any third country. This prohibition shall be without prejudice to the right of Member States to transfer such data to third countries to which Regulation (EU) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] applies, in order to ensure that Member States have the possibility of cooperating with such third countries for the purposes of this Regulation.

Amendment

(33) Transfers of data obtained pursuant to this Decision to third countries or international organisations or private entities should be prohibited, in order to ensure the right to asylum and to safeguard applicants for international protection from having their data disclosed to any third country. This prohibition shall be without prejudice to the right of Member States to transfer such data to third countries to which Regulation (EU) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] applies, in order to ensure that Member States have the possibility of cooperating with such third countries for the purposes of this Regulation. ***This right should not apply to transfers of data to third countries in the context of law enforcement.***

Or. en

Justification

As we are dealing with a vulnerable group of people, transfer of data to third countries in the context of law enforcement should be prohibited.

Amendment 51 Cornelis de Jong

Proposal for a regulation Recital 34

Text proposed by the Commission

(34) National competent authorities for the supervision of the processing of

Amendment

deleted

personal data should monitor the lawfulness of the processing of personal data by the Member States, and the supervisory authority set up by the Europol Decision should monitor the lawfulness of data processing activities performed by Europol.

Or. en

Amendment 52
Cornelis de Jong

Proposal for a regulation
Recital 35

Text proposed by the Commission

(35) Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data *and in particular Articles 21 and 22 thereof concerning confidentiality and security of processing apply* to the processing of personal data by *Union* institutions, bodies, *offices and agencies* carried out *in application of* this Regulation. However, certain points should be clarified in respect of the responsibility for the processing of data and of the supervision of data protection.

Amendment

(35) Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data *applies* to the processing of personal data by *the* institutions *and* bodies *of the Union* carried out *pursuant to* this Regulation. However, certain points should be clarified in respect of the responsibility for the processing of data and of the supervision of data protection.

Or. en

Amendment 53
Sarah Ludford

Proposal for a regulation

Recital 35 a (new)

Text proposed by the Commission

Amendment

(35a) The data subject should be informed of the purpose for which his or her data will be processed within EURODAC, including a description of the aims of the Dublin Regulation and the use to which law enforcement authorities may put his or her data.

Or. en

Justification

It is useful to underline that Article 29(1) includes the obligation on the authorities to inform the data subject of the use to which law enforcement authorities may put their data.

Amendment 54

Sarah Ludford

Proposal for a regulation

Recital 37

Text proposed by the Commission

Amendment

(37) It is appropriate to monitor and evaluate the performance of EURODAC at regular intervals.

(37) It is appropriate to monitor and evaluate the performance of EURODAC at regular intervals, including whether law enforcement access has led to the stigmatisation of applicants for international protection as raised in the Commission's evaluation of the compliance of the proposal with the Charter of Fundamental Rights.

Or. en

Amendment 55

Cornelis de Jong

Proposal for a regulation

Recital 39

Text proposed by the Commission

(39) It is necessary that Member States **are** informed of the status of particular asylum procedures, with a view to facilitating the adequate application of Regulation (EU) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person].

Amendment

(39) It is necessary that Member States **be** informed of the status of particular asylum procedures, with a view to facilitating the adequate application of Regulation (EU) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person].

Or. en

Amendment 56 Cornelis de Jong

Proposal for a regulation Recital 40

Text proposed by the Commission

(40) This Regulation respects and has to be applied in accordance with fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union. In particular, this Regulation **fully respects the individual's right to** protection of **his or her** personal data and the right to asylum.

Amendment

(40) This Regulation respects and has to be applied in accordance with fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union. In particular, this Regulation **seeks to ensure full respect for the** protection of personal data and the right to **seek** asylum **and to promote the application of Articles 8 and 18 of the Charter.**

Or. en

Amendment 57 Cornelis de Jong

Proposal for a regulation

Recital 41

Text proposed by the Commission

(41) In accordance with Articles 1 and 2 of the Protocol on the position of Denmark annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application. As regards Denmark, this Regulation, ***with the exception of the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43***, constitutes amendment to the EURODAC Regulation within the meaning of the Agreement between the European Community and the Kingdom of Denmark on the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in Denmark or any other Member State of the European Union and ‘Eurodac’ for the comparison of fingerprints for the effective application of the Dublin Convention. Consequently, in accordance with Article 3 thereof, Denmark is to notify the Commission whether it will implement the contents of this Regulation and when it does so, this Regulation creates mutual obligations under international law between Denmark and the European Union. ***Once this Recast Regulation is adopted and subject to a Commission recommendation for a Council Decision authorising the opening of negotiations, Denmark will be consulted as to whether it wishes to enter into negotiations on complementary agreements also covering the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43.***

Amendment

(41) In accordance with Articles 1 and 2 of the Protocol on the position of Denmark annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application. As regards Denmark, this Regulation constitutes amendment to the EURODAC Regulation within the meaning of the Agreement between the European Community and the Kingdom of Denmark on the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in Denmark or any other Member State of the European Union and ‘Eurodac’ for the comparison of fingerprints for the effective application of the Dublin Convention. Consequently, in accordance with Article 3 thereof, Denmark is to notify the Commission whether it will implement the contents of this Regulation and when it does so, this Regulation creates mutual obligations under international law between Denmark and the European Union.

Or. en

Amendment 58
Cornelis de Jong

Proposal for a regulation
Recital 44

Text proposed by the Commission

(44) As regards the Republic of Iceland and the Kingdom of Norway, this Regulation, ***with the exception of the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43***, constitutes a new measure related to EURODAC within the meaning of the Agreement between the European Community and the Republic of Iceland and the Kingdom of Norway concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Iceland or Norway . Consequently, subject to their decision to implement it in their internal legal order, this Regulation shall be applied between the Republic of Iceland and the Kingdom of Norway in their mutual relations and in *there* relations with the Member States of the European Union. ***Once this Recast Regulation is adopted and subject to a Commission recommendation for a Council Decision authorising the opening of negotiations, the Republic of Iceland and the Kingdom of Norway will be consulted as to whether they wish to enter into negotiations on complementary agreements also covering the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43.***

Amendment

(44) As regards the Republic of Iceland and the Kingdom of Norway, this Regulation constitutes a new measure related to EURODAC within the meaning of the Agreement between the European Community and the Republic of Iceland and the Kingdom of Norway concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Iceland or Norway. Consequently, subject to their decision to implement it in their internal legal order, this Regulation shall be applied between the Republic of Iceland and the Kingdom of Norway in their mutual relations and in *their* relations with the Member States of the European Union.

Or. en

Amendment 59
Cornelis de Jong

Proposal for a regulation
Recital 45

Text proposed by the Commission

(45) As regards the Swiss Confederation, this Regulation, ***with the exception of the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43***, constitutes a new measure related to EURODAC within the meaning of the Agreement between the European Community and the Swiss Confederation concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Switzerland . Consequently, subject to its decision to implement it in its internal legal order, this Regulation shall be applied between the Swiss Confederation and the Member States of the European Union. ***Once this Recast Regulation is adopted and subject to a Commission recommendation for a Council Decision authorising the opening of negotiations, the Swiss Confederation will be consulted as to whether it wishes to enter into negotiations on complementary agreements also covering the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43, subject to a separate agreement on the application of relevant provisions of Council Decision 2008/615/JHA on the stepping up of cross-border cooperation.***

Amendment

(45) As regards the Swiss Confederation, this Regulation constitutes a new measure related to EURODAC within the meaning of the Agreement between the European Community and the Swiss Confederation concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Switzerland. Consequently, subject to its decision to implement it in its internal legal order, this Regulation shall be applied between the Swiss Confederation and the Member States of the European Union.

Or. en

Amendment 60
Cornelis de Jong

Proposal for a regulation
Recital 46

Text proposed by the Commission

(46) As regards the Principality of Liechtenstein, this Regulation, ***with the exception of the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43***, constitutes a new measure related to EURODAC within the meaning of the Protocol between the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Community and the Swiss Confederation concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Switzerland . Consequently, subject to its decision to implement it in its internal legal order, this Regulation shall be applied between the Principality of Liechtenstein, the Swiss Confederation and the Member States of the European Union. ***Once this Recast Regulation is adopted and subject to a Commission recommendation for a Council Decision authorising the opening of negotiations, the Principality of Liechtenstein will be consulted as to whether it wishes to enter into negotiations on complementary agreements also covering the procedure for comparison and data transmission for law enforcement purposes laid down in Articles 5, 6, 19-22, 33, 36, 39(3), 40(8) and 43, subject to a separate agreement on their application of relevant provisions of Council Decision 2008/615/JHA on the stepping up of cross-border cooperation.***

Amendment

(46) As regards the Principality of Liechtenstein, this Regulation constitutes a new measure related to EURODAC within the meaning of the Protocol between the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Community and the Swiss Confederation concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a Member State or in Switzerland. Consequently, subject to its decision to implement it in its internal legal order, this Regulation shall be applied between the Principality of Liechtenstein, the Swiss Confederation and the Member States of the European Union.

Or. en

Amendment 61
Claude Moraes, Carmen Romero López, Birgit Sippel

Proposal for a regulation
Article 1 – paragraph 2

Text proposed by the Commission

Amendment

2. This Regulation also lays down the conditions under which Member States' designated authorities and the European Police Office (Europol) may request the comparison of fingerprint data with those stored in the EURODAC central database for the purposes of the prevention, detection and investigation of terrorist offences and other serious criminal offences.

deleted

(This amendment applies throughout the text; its adoption will imply the deletion of all provisions related to access to EURODAC for law enforcement purposes and the necessary adjustments throughout the text.)

Or. en

Justification

Access by law enforcement authorities to the Eurodac database should not be granted. This amendment should affect the whole text respectively.

Amendment 62
Franziska Keller, Jan Philipp Albrecht

Proposal for a regulation
Article 1 – paragraph 2

Text proposed by the Commission

Amendment

2. This Regulation also lays down the conditions under which Member States' designated authorities and the European

deleted

Police Office (Europol) may request the comparison of fingerprint data with those stored in the EURODAC central database for the purposes of the prevention, detection and investigation of terrorist offences and other serious criminal offences.

(This amendment applies throughout the text; its adoption will imply the deletion of all provisions related to access to EURODAC for law enforcement purposes and the necessary adjustments throughout the text.)

Or. en

**Amendment 63
Cornelis de Jong**

**Proposal for a regulation
Article 1 – paragraph 2**

Text proposed by the Commission

Amendment

2. This Regulation also lays down the conditions under which Member States' designated authorities and the European Police Office (Europol) may request the comparison of fingerprint data with those stored in the EURODAC central database for the purposes of the prevention, detection and investigation of terrorist offences and other serious criminal offences.

deleted

(This amendment applies throughout the text; its adoption will imply the deletion of all provisions related to access to EURODAC for law enforcement purposes and the necessary adjustments throughout the text.)

Or. en

Amendment 64
Cornelis de Jong

Proposal for a regulation
Article 2 – paragraph 1 – point d

Text proposed by the Commission

(d) "person granted international protection" means a third country national or a stateless person recognised as entitled to international protection as defined in *point (a) of Article 2 of Council Directive 2004/83/EC*;

Amendment

(d) "person granted international protection" means a third country national or stateless person recognised as entitled to international protection as defined in *point (a) of Article 2 of Directive 2011/95/EU*;

Or. en

Amendment 65
Cornelis de Jong

Proposal for a regulation
Article 2 – paragraph 1 – point h

Text proposed by the Commission

(h) '*Europol*' means the *European Police Office as established by Decision 2009/371/JHA*;

Amendment

deleted

Or. en

Amendment 66
Cornelis de Jong

Proposal for a regulation
Article 2 – paragraph 1 – point j

Text proposed by the Commission

(j) '*terrorist offences*' means the *offences under national law which correspond or are equivalent to the offences referred to in Articles 1 to 4 of Framework Decision 2002/475/JHA*;

Amendment

deleted

Amendment 67
Cornelis de Jong

Proposal for a regulation
Article 2 – paragraph 1 – point k

Text proposed by the Commission

Amendment

(k) 'serious criminal offences' means the forms of crime which correspond or are equivalent to those referred to in Article 2(2) of Framework Decision 2002/584/JHA if they are punishable by a custodial sentence or a detention order for a maximum period of at least three years under national law;

deleted

Or. en

Amendment 68
Franziska Keller, Jan Philipp Albrecht

Proposal for a regulation
Article 2 – paragraph 1 – point l

Text proposed by the Commission

Amendment

(l) 'fingerprint data' means the data relating to fingerprints of all or at least the index fingers, and if those are missing, the prints of all other fingers of a person, *or a latent*.

(l) 'fingerprint data' means the data relating to fingerprints of all or at least the index fingers, and if those are missing, the prints of all other fingers of a person.

Or. en

Justification

Since there are no common European standards on the verification of latents and since a latent can easily result in a false accusation if the verification procedure and criteria are not thorough enough, latents should be excluded from the comparison of data with the EURODAC database for law enforcement purposes.

Amendment 69

Claude Moraes, Carmen Romero López, Birgit Sippel

Proposal for a regulation

Article 2 – paragraph 1 – point 1

Text proposed by the Commission

(l) 'fingerprint data' means the data relating to fingerprints of all or at least the index fingers, and if those are missing, the prints of all other fingers of a person, **or a latent**.

Amendment

(l) 'fingerprint data' means the data relating to fingerprints of all or at least the index fingers, and if those are missing, the prints of all other fingers of a person.

Or. en

Justification

A latent fingerprint may lead to a high number of possible matches as it is only a partial or fragmentary print. This carries a higher risk of the wrongful implication of innocent persons. As we are dealing with a vulnerable group of people, only clean prints should be used.

Amendment 70

Cornelis de Jong

Proposal for a regulation

Article 2 – paragraph 2

Text proposed by the Commission

2. The terms defined in Article 2 of Directive 95/46/EC shall have the same meaning in this Regulation ***unless the processing of personal data takes place by Member States' designated authorities for the purposes of the prevention, detection and investigation of terrorist offences and other serious criminal offences.***

Amendment

2. The terms defined in Article 2 of Directive 95/46/EC shall have the same meaning in this Regulation.

Or. en

Amendment 71

Cornelis de Jong

Proposal for a regulation
Article 2 – paragraph 4

Text proposed by the Commission

Amendment

4. The terms defined in Article 2 of the Framework Decision 2008/977/JHA shall have the same meaning in this Regulation in so far as personal data are processed by Member States' designated authorities for the purposes of the prevention, detection and investigation of terrorist offences and other serious criminal offences pursuant to this Regulation.

deleted

Or. en

Amendment 72
Franziska Keller, Jan Philipp Albrecht

Proposal for a regulation
Article 3 – paragraph 1 – point a

Text proposed by the Commission

Amendment

(a) a computerised central fingerprint database (Central System) composed of
– a Central Unit,
– a Business Continuity **System**.

(a) a computerised central fingerprint database (Central System) composed of:
– a Central Unit,
– a Business Continuity **Plan**.

Or. en

Justification

A critical system such as EURODAC should be covered by a sound and tested Business Continuity Plan rather than just a technical system. The Business Continuity Plan should include repercussions on data protection, security and costs in case of major disruptions or disasters.

Amendment 73
Franziska Keller, Jan Philipp Albrecht

Proposal for a regulation

Article 4 – paragraph 1

Text proposed by the Commission

1. The Agency, shall be responsible for the operational management of EURODAC. The Agency shall ensure, in cooperation with the Member States, that at all times the best available **technology**, subject to a cost-benefit analysis, is used for the Central System.

Amendment

1. The Agency shall be responsible for the operational management of EURODAC. The Agency shall ensure, in cooperation with the Member States, that at all times the best available **and most secure techniques**, subject to a cost-benefit analysis, is used for the Central System.

Or. en

Justification

The concept of techniques is broader; it includes both the technology used and the way in which the installation is designed, built, maintained and operated.

Amendment 74

Sarah Ludford, Renate Weber

Proposal for a regulation

Article 4 – paragraph 1

Text proposed by the Commission

1. The Agency, shall be responsible for the operational management of EURODAC. The Agency shall ensure, in cooperation with the Member States, that at all times the best available **technology**, subject to a cost-benefit analysis, is used for the Central System.

Amendment

1. The Agency shall be responsible for the operational management of EURODAC. The Agency shall ensure, in cooperation with the Member States, that at all times the best available **techniques**, subject to a cost-benefit analysis, is used for the Central System.

Or. en

Justification

Best available techniques include both technology used and the way in which the installation is designed, built, maintained and operated. The term is considered a key principle in the review of the EU data protection framework.

Amendment 75

Claude Moraes, Carmen Romero López, Birgit Sippel

Proposal for a regulation

Article 4 – paragraph 1

Text proposed by the Commission

1. The Agency, shall be responsible for the operational management of EURODAC. The Agency shall ensure, in cooperation with the Member States, that at all times the best available **technology**, subject to a cost-benefit analysis, is used for the Central System.

Amendment

1. The Agency shall be responsible for the operational management of EURODAC. The Agency shall ensure, in cooperation with the Member States, that at all times the best available **techniques**, subject to a cost-benefit analysis, is used for the Central System.

Or. en

Justification

Best available techniques include both technology used and the way in which the installation is designed, built, maintained and operated. The term is considered a key principle in the review of the EU data protection framework.

Amendment 76

Franziska Keller, Jan Philipp Albrecht

Proposal for a regulation

Article 4 – paragraph 5

Text proposed by the Commission

5. Operational management of EURODAC shall consist of all the tasks necessary to keep EURODAC functioning 24 hours a day, 7 days a week in accordance with this Regulation, in particular the maintenance work and technical developments necessary to ensure that the system functions at a satisfactory level of operational quality, in particular as regards the time required for interrogation of the Central System.

Amendment

5. Operational management of EURODAC shall consist of all the tasks necessary to keep EURODAC functioning 24 hours a day, 7 days a week in accordance with this Regulation, in particular the maintenance work and technical developments necessary to ensure that the system functions at a satisfactory level of operational quality, in particular as regards the time required for interrogation of the Central System. ***A Business Continuity Plan shall be developed taking into account maintenance needs and***

*unforeseen downtime of the system,
including the impact of business
continuity measures on data protection
and security.*

Or. en

Amendment 77
Cornelis de Jong

Proposal for a regulation
Article 5

Text proposed by the Commission

Amendment

Article 5

deleted

*Designated Authorities for the purpose of
law enforcement access*

*1. Member States shall designate the
authorities which are authorised to access
EURODAC data pursuant to this
Regulation. Designated authorities shall
be authorities of the Member States which
are responsible for the prevention,
detection or investigation of terrorist
offences and other serious criminal
offences.*

*2. Every Member State shall keep a list of
the designated authorities.*

*3. At national level, each Member State
shall keep a list of the operating units
within the designated authorities that are
authorised to request comparisons with
EURODAC data through the National
Access Point.*

Or. en

Amendment 78
Sarah Ludford, Renate Weber, Franziska Keller

Proposal for a regulation

Article 5 – paragraph 1

Text proposed by the Commission

1. Member States shall designate the authorities which are authorised to access EURODAC data pursuant to this Regulation. Designated authorities shall be authorities of the Member States which are responsible for the prevention, detection or investigation of terrorist offences and other serious criminal offences.

Amendment

1. ***For the purposes laid down in Article 1(2)***, Member States shall designate the authorities which are authorised to access EURODAC data pursuant to this Regulation. Designated authorities shall be authorities of the Member States which are responsible for the prevention, detection or investigation of terrorist offences and other serious criminal offences. ***Designated authorities shall not include agencies or units responsible for intelligence relating to national security.***

Or. en

Justification

To ensure that access is limited to law enforcement purposes it is best to refer to Article 1(2). As this is a law enforcement measure those national entities which are responsible for intelligence rather than the prosecution of crimes should be excluded consistent with Article 72 TEC.

Amendment 79
Claude Moraes

Proposal for a regulation
Article 5 – paragraph 1

Text proposed by the Commission

1. Member States shall designate the authorities which are authorised to access EURODAC data pursuant to this Regulation. Designated authorities shall be authorities of the Member States which are responsible for the prevention, detection or investigation of terrorist offences and other serious criminal offences.

Amendment

1. ***For the purposes laid down in Article 1(2)***, Member States shall designate the authorities which are authorised to access EURODAC data pursuant to this Regulation. Designated authorities shall be authorities of the Member States which are responsible for the prevention, detection or investigation of terrorist offences and other serious criminal offences.

Or. en

Amendment 80
Franziska Keller, Jan Philipp Albrecht

Proposal for a regulation
Article 5 – paragraph 3

Text proposed by the Commission

3. *At national level, each* Member State shall keep a list of the operating units within the designated authorities that are authorised to request comparisons with EURODAC data through the National Access Point.

Amendment

3. **Each** Member State shall keep a list of the operating units within the designated authorities that are authorised to request comparisons with EURODAC data through the National Access Point.

Or. en

Amendment 81
Cornelis de Jong

Proposal for a regulation
Article 6

Text proposed by the Commission

Article 6

Verifying Authorities

1. Each Member State shall designate a single national body to act as its verifying authority. The verifying authority shall be an authority of the Member State which is responsible for the prevention, detection or investigation of terrorist offences and other serious criminal offences.

2. The verifying authority shall ensure that the conditions for requesting comparisons of fingerprints with EURODAC data are fulfilled.

Only the verifying authority shall be authorised to forward requests for comparison of fingerprints to the National Access Point which communicates with

Amendment

deleted

the Central System.

Or. en

Amendment 82

Carmen Romero López, Birgit Sippel

Proposal for a regulation

Article 6 – paragraph 1

Text proposed by the Commission

1. Each Member State shall designate a single national body to act as its verifying authority. The verifying authority shall be **an** authority of the Member State which is responsible for the prevention, detection or investigation of terrorist offences and other serious criminal offences.

Amendment

1. Each Member State shall designate a single national body to act as its verifying authority. The verifying authority shall be **a judicial** authority of the Member State which is responsible for the prevention, detection or investigation of terrorist offences and other serious criminal offences **and shall be independent from the designated authorities referred to in Article 5.**

Or. en

Amendment 83

Claude Moraes

Proposal for a regulation

Article 6 – paragraph 1

Text proposed by the Commission

1. Each Member State shall designate a single national body to act as its verifying authority. The verifying authority shall be an authority of the Member State which is responsible for the prevention, detection or investigation of terrorist offences and other serious criminal offences.

Amendment

1. Each Member State shall designate a single national body to act as its verifying authority. The verifying authority shall be an authority of the Member State which is responsible for the prevention, detection or investigation of terrorist offences and other serious criminal offences **and shall be independent from the designated authorities referred to in Article 5.**

Or. en

Amendment 84
Franziska Keller, Jan Philipp Albrecht

Proposal for a regulation
Article 6 – paragraph 1

Text proposed by the Commission

1. Each Member State shall designate a single national body to act as its verifying authority. The verifying authority shall be an authority of the Member State which is responsible for the prevention, detection or investigation of terrorist offences and other serious criminal offences.

Amendment

1. Each Member State shall designate a single national body to act as its verifying authority. The verifying authority shall be a **judicial** authority of the Member State which is responsible for the prevention, detection or investigation of terrorist offences and other serious criminal offences.

Or. en

Justification

As the concerned authority is the verifying authority, deciding on access to very sensitive data, it is appropriate to appoint a judicial authority as the verifying authority.

Amendment 85
Claude Moraes, Carmen Romero López, Birgit Sippel

Proposal for a regulation
Article 6 – paragraph 1 a (new)

Text proposed by the Commission

Amendment

1a. The verifying authority shall perform its duties and tasks independently and shall neither seek nor receive instructions as regards the exercise of the verification.

Or. en

Amendment 86
Sarah Ludford

Proposal for a regulation
Article 6 – paragraph 2 – subparagraph 2 a (new)

Text proposed by the Commission

Amendment

Only duly empowered staff of the verifying authority shall be authorised to access EURODAC in accordance with Article 19.

Or. en

Justification

This provision is in the VIS Decision 2008/633/JHA and is a sensible addition.

Amendment 87
Renate Weber, Sarah Ludford

Proposal for a regulation
Article 6 – paragraph 2 a (new)

Text proposed by the Commission

Amendment

2a. The verifying authority shall perform its duties and tasks independently and shall not receive instructions as regards the exercise of the verification.

Or. en

Amendment 88
Cornelis de Jong

Proposal for a regulation
Article 7

Text proposed by the Commission

Amendment

Article 7

deleted

Europol

1. Europol shall designate a specialised unit with duly empowered Europol

officials to act as its verifying authority and shall designate in agreement with any Member State the National Access Point of that Member State which shall communicate its requests for comparison of fingerprint data to the Central System.

2. Europol shall designate an operating unit that is authorised to request comparisons with EURODAC data through its designated National Access Point.

Or. en

Amendment 89
Claude Moraes

Proposal for a regulation
Article 7 – paragraph 1

Text proposed by the Commission

1. Europol shall designate a specialised unit with duly empowered Europol officials to act as its verifying authority and shall designate in agreement with any Member State the National Access Point of that Member State which shall communicate its requests for comparison of fingerprint data to the Central System.

Amendment

1. Europol shall designate a specialised unit with duly empowered Europol officials to act as its verifying authority, ***which will neither seek nor receive instructions as regards the exercise of the verification,*** and shall designate in agreement with any Member State the National Access Point of that Member State which shall communicate its requests for comparison of fingerprint data to the Central System.

Or. en

Amendment 90
Renate Weber, Sarah Ludford

Proposal for a regulation

Article 7 – paragraph 2 a (new)

Text proposed by the Commission

Amendment

2a. The verifying authority shall perform its duties and tasks independently and shall not receive instructions as regards the exercise of the verification.

Or. en

Amendment 91

Franziska Keller, Jan Philipp Albrecht

Proposal for a regulation

Article 8 – paragraph 1 – point f

Text proposed by the Commission

Amendment

(f) the number of requests for **marking and unmarking** transmitted in accordance with Article 18(1) and (2).

(f) the number of requests for **blocking and unblocking** transmitted in accordance with Article 18(1) and (2).

Or. en

Amendment 92

Franziska Keller, Jan Philipp Albrecht

Proposal for a regulation

Article 8 – paragraph 2

Text proposed by the Commission

Amendment

2. At the end of each year, statistical data shall be established in the form of a compilation of the monthly statistics for that year, including an indication of the number of persons for whom hits have been recorded under points (b), (c), and (d). The statistics shall contain a breakdown of data for each Member State.

2. At the end of each year, statistical data shall be established in the form of a compilation of the monthly statistics for that year, including an indication of the number of persons for whom hits have been recorded under points (b), (c) and (d). The statistics shall contain a breakdown of data for each Member State. **The result shall be made public.**

Or. en

Amendment 93
Franziska Keller, Jan Philipp Albrecht

Proposal for a regulation
Article 9 – paragraph 2

Text proposed by the Commission

2. By way of derogation from paragraph 1, where it is not possible to take the fingerprints of an applicant on account of measures taken to ensure the health of the applicant or the protection of public health, Member States shall take and send the fingerprints of the applicant as soon as possible and no later than 48 hours after these grounds no longer prevail.

Amendment

2. By way of derogation from paragraph 1, where it is not possible to take the fingerprints of an applicant on account of measures taken to ensure the health of the applicant or the protection of public health, Member States shall take and send the fingerprints of the applicant as soon as possible and no later than 48 hours after these grounds no longer prevail. ***The temporary or permanent impossibility to provide usable fingerprints shall not adversely affect the legal situation of a third-country national or a stateless person. In particular, it shall not represent sufficient grounds to refuse to examine or to reject an asylum application.***

Or. en

Amendment 94
Renate Weber

Proposal for a regulation
Article 9 – paragraph 2 a (new)

Text proposed by the Commission

Amendment

2a. Temporary or permanent impossibility to provide usable fingerprints shall not adversely affect the legal situation of the individual. In any case, it cannot represent sufficient grounds to refuse to examine or to reject an international protection application.

Amendment 95
Franziska Keller, Jan Philipp Albrecht

Proposal for a regulation
Article 13 – paragraph 2

Text proposed by the Commission

2. The Central System shall inform all Member States of origin about the erasure of data for the reason specified in paragraph 1 by another Member State of origin having produced a hit with data which they transmitted relating to persons referred to in Article 9(1) or Article 14(1).

Amendment

2. The Central System shall inform ***as soon as possible and not later than after 72 hours***, all Member States of origin about the erasure of data for the reason specified in paragraph 1 by another Member State of origin having produced a hit with data which they transmitted relating to persons referred to in Article 9(1) or Article 14(1).

Amendment 96
Franziska Keller, Jan Philipp Albrecht

Proposal for a regulation
Article 14 – paragraph 1

Text proposed by the Commission

1. Each Member State shall promptly take the fingerprints of all fingers of every third country national or stateless person of at least 14 years of age who is apprehended by the competent control authorities in connection with the irregular crossing by land, sea or air of the border of that Member State having come from a third country and who is not turned back ***or who remains physically on the territory of the Member States and who is not kept in custody, confinement or detention during the entirety of the period between apprehension and removal on the basis of the decision to turn them back.***

Amendment

1. Each Member State shall promptly take the fingerprints of all fingers of every third country national or stateless person of at least 14 years of age who is apprehended by the competent control authorities in connection with the irregular crossing by land, sea or air of the border of that Member State having come from a third country and who is not turned back.

Amendment 97
Cornelis de Jong

Proposal for a regulation
Article 14 – paragraph 1

Text proposed by the Commission

1. Each Member State shall promptly take the fingerprints of all fingers of every third country national or stateless person of at least 14 years of age who is apprehended by the competent control authorities in connection with the irregular crossing by land, sea or air of the border of that Member State having come from a third country and who is not turned back *or who remains physically on the territory of the Member States and who is not kept in custody, confinement or detention during the entirety of the period between apprehension and removal on the basis of the decision to turn them back.*

Amendment

1. Each Member State shall, *whilst fully respecting the safeguards laid down in the Charter of Fundamental Rights of the European Union, the European Convention on Human Rights and the United Nations Convention on the Rights of the Child*, promptly take the fingerprints of all fingers of every third country national or stateless person of at least 14 years of age who is apprehended by the competent control authorities in connection with the irregular crossing by land, sea or air of the border of that Member State having come from a third country and who is not turned back.

Amendment 98
Cornelis de Jong

Proposal for a regulation
Article 14 – paragraph 2 – introductory part

Text proposed by the Commission

2. The Member State concerned shall *as soon as possible and* no later than *72 hours from the date of apprehension* transmit to the Central System the following data in relation to *any third country national or stateless person, as referred to in paragraph 1, who is not turned back:*

Amendment

2. The Member State concerned shall no later than *24 hours after the taking of the fingerprints of the third-country national or stateless person, as referred to in paragraph 1*, transmit to the Central System the following data in relation to *that person:*

Amendment 99
Franziska Keller, Jan Philipp Albrecht

Proposal for a regulation
Article 14 – paragraph 3

Text proposed by the Commission

Amendment

3. By way of derogation from paragraph 2, as regards persons apprehended in the manner described in paragraph 1 who remain physically on the territory of the Member States but are kept in custody, confinement or detention upon their apprehension for a period exceeding 72 hours, the transmission of the data specified in paragraph 2 relating to those persons shall take place before their release from custody, confinement or detention. *deleted*

Amendment 100
Cornelis de Jong

Proposal for a regulation
Article 14 – paragraph 3

Text proposed by the Commission

Amendment

3. By way of derogation from paragraph 2, as regards persons apprehended in the manner described in paragraph 1 who remain physically on the territory of the Member States but are kept in custody, confinement or detention upon their apprehension for a period exceeding 72 hours, the transmission of the data specified in paragraph 2 relating to those persons shall take place before their *deleted*

release from custody, confinement or detention.

Or. en

Amendment 101
Franziska Keller, Jan Philipp Albrecht

Proposal for a regulation
Article 14 – paragraph 4

Text proposed by the Commission

4. ***Non compliance with the 72 hours time limit referred to in paragraph 2 does not relieve Member States of the obligation to take and transmit the fingerprints to the Central System.*** Where the condition of the fingertips does not allow to take the fingerprints in a quality ensuring appropriate comparison under Article 25, the Member State of origin shall retake the fingerprints of such person and resend them as soon as possible and no later than 48 hours after they have been successfully taken.

Amendment

4. Where the condition of the fingertips does not allow to take the fingerprints in a quality ensuring appropriate comparison under Article 25, the Member State of origin shall retake the fingerprints of such person and resend them as soon as possible and no later than 48 hours after they have been successfully taken.

Or. en

Amendment 102
Franziska Keller, Jan Philipp Albrecht

Proposal for a regulation
Article 14 – paragraph 5

Text proposed by the Commission

5. By way of derogation from paragraph 1, where it is not possible to take the fingerprints of such person on account of measures taken to ensure the health of the person or the protection of public health, the Member State concerned shall take and send the fingerprints of the person, in

Amendment

5. By way of derogation from paragraph 1, where it is not possible to take the fingerprints of such person on account of measures taken to ensure the health of the person or the protection of public health, the Member State concerned shall take and send the fingerprints of the person, in

accordance with the deadline set out in paragraph 2, once these grounds no longer prevail.

accordance with the deadline set out in paragraph 2, once these grounds no longer prevail. ***The temporary or permanent impossibility to provide usable fingerprints shall not adversely affect the legal situation of a third-country national or a stateless person.***

Or. en

Amendment 103
Renate Weber

Proposal for a regulation
Article 14 – paragraph 5 a (new)

Text proposed by the Commission

Amendment

5a. Temporary or permanent impossibility to provide usable fingerprints shall not adversely affect the legal situation of the individual. In any case, it cannot represent sufficient grounds to refuse to examine or to reject an international protection application.

Or. en

Amendment 104
Franziska Keller, Jan Philipp Albrecht

Proposal for a regulation
Article 16 – paragraph 3

Text proposed by the Commission

Amendment

3. The Central System shall inform all Member States of origin about the erasure of data for the reason specified in point (a) or (b) of paragraph 2 or by another Member State of origin having produced a hit with data which they transmitted relating to persons referred to in Article 14(1).

3. The Central System shall inform ***as soon as possible and no later than after 72 hours*** all Member States of origin about the erasure of data for the reason specified in point (a) or (b) of paragraph 2 or by another Member State of origin having produced a hit with data which they transmitted relating to persons referred to

in Article 14(1).

Or. en

Amendment 105
Franziska Keller, Jan Philipp Albrecht

Proposal for a regulation
Article 16 – paragraph 4

Text proposed by the Commission

4. The Central System shall inform all Member States of origin about the erasure of data for the reason specified in point (c) of paragraph 2 by another Member State of origin having produced a hit with data which they transmitted relating to persons referred to in Article 9(1) or Article 14(1).

Amendment

4. The Central System shall inform ***as soon as possible and no later than after 72 hours*** all Member States of origin about the erasure of data for the reason specified in point (c) of paragraph 2 by another Member State of origin having produced a hit with data which they transmitted relating to persons referred to in Article 9(1) or Article 14(1).

Or. en

Amendment 106
Claude Moraes, Carmen Romero López, Birgit Sippel

Proposal for a regulation
Article 17 – paragraph 4 a (new)

Text proposed by the Commission

Amendment

4a. Once the results of the comparison have been transmitted to the Member State of origin, the Central System shall immediately:

- (a) erase the fingerprint data and other data transmitted to it pursuant to paragraph 1; and***
- (b) destroy the media used by the Member State of origin for transmitting the data to the Central System, unless the Member State of origin has requested their return.***

Justification

In June 2012 the EDPS inspectors noted that the archiving system of EURODAC stores full fingerprint data, including category 3 requests, contrary to the obligation under Article 11(5) of the current Eurodac regulation. The Commission seeks to delete the provision, but on the contrary it should be reinforced given the implications of law enforcement access to Eurodac and the necessity for proportionality.

Amendment 107
Renate Weber

Proposal for a regulation
Article 17 – paragraph 4 a (new)

Text proposed by the Commission

Amendment

4a. Once the results of the comparison have been transmitted to the Member State of origin, the Central System shall forthwith:

(a) erase the fingerprint data and other data transmitted to it pursuant to paragraph 1; and

(b) destroy the media used by the Member State of origin for transmitting the data to the Central System, unless the Member State of origin has requested their return.

Temporary or permanent impossibility to provide usable fingerprints shall not adversely affect the legal situation of the individual. In any case, it cannot represent sufficient grounds to refuse to examine or to reject an application for international protection.

Amendment 108
Franziska Keller, Jan Philipp Albrecht

Proposal for a regulation

Article 17 – paragraph 4 a (new)

Text proposed by the Commission

Amendment

4a. Once the results of the comparison have been transmitted to the Member State of origin, the Central System shall forthwith:

(a) erase the fingerprint data and other data transmitted to it pursuant to paragraph 1; and

(b) destroy the media used by the Member State of origin for transmitting the data to the Central Unit, unless the Member State of origin has requested their return.

Or. en

Amendment 109

Sarah Ludford

Proposal for a regulation

Article 17 – paragraph 4 a (new)

Text proposed by the Commission

Amendment

4a. Once the results of the comparison have been transmitted to the Member State of origin, the Central Unit shall immediately:

(a) erase the fingerprint data and other data transmitted to it pursuant to paragraph 1; and

(b) destroy the media used by the Member State of origin for transmitting the data to the Central System, unless the Member State of origin has requested their return.

Or. en

Justification

In June 2012 the EDPS inspectors noted that the archiving system of EURODAC stores full

fingerprint data, including category 3 requests, contrary to the obligation under Article 11(5) of the current Eurodac regulation. The Commission seeks to delete the provision, but on the contrary it should be reinforced given the implications of law enforcement access to Eurodac and the necessity for proportionality.

Amendment 110

Franziska Keller, Jan Philipp Albrecht

Proposal for a regulation

Article 18

Text proposed by the Commission

Article 18

Marking of data

1. The Member State of origin which granted international protection to an applicant for international protection whose data were previously recorded pursuant to Article 11 in the Central System shall mark the relevant data in conformity with the requirements for electronic communication with the Central System established by the Agency. This mark shall be stored in the Central System in accordance with Article 12 for the purpose of transmission under Article 9(5).

2. The Member State of origin shall unmark data concerning a third country national or stateless person whose data were previously marked in accordance with paragraph 1 if his or her status is revoked or ended or renewal of his status is refused under Article 14 or 19 of Council Directive 2004/83/EC.

Amendment

Article 18

Blocking of data

1. Data relating to an applicant for international protection which have been recorded pursuant to Article 11 shall be blocked in the central database if that person is granted international protection in a Member State. Such blocking shall be carried out by the Central System on the instructions of the Member State of origin.

2. Hits concerning persons who have been granted international protection in a Member State shall not be transmitted. The Central System shall return a negative result to the requesting Member State.

Or. en

Amendment 111

Sarah Ludford, Renate Weber

Proposal for a regulation

Article 18

Text proposed by the Commission

Article 18

Marking of data

1. *The Member State of origin which granted international protection to an applicant for international protection whose data were previously recorded pursuant to Article 11 in the Central System shall mark the relevant data in conformity with the requirements for electronic communication with the Central System established by the Agency. This mark shall be stored in the Central System in accordance with Article 12 for the purpose of transmission under Article 9(5).*

2. *The Member State of origin shall unmark data concerning a third country national or stateless person whose data were previously marked in accordance with paragraph 1 if his or her status is revoked or ended or renewal of his status is refused under Article 14 or 19 of Council Directive 2004/83/EC.*

Amendment

Article 18

Blocking of data

1. *Data relating to an applicant for international protection which have been recorded pursuant to Article 11 shall be blocked in the central database if that person is granted international protection in a Member State. Such blocking shall be carried out by the Central System on the instructions of the Member State of origin.*

2. *Hits concerning persons who have been granted international protection in a Member State shall not be transmitted. The Central System shall return a negative result to the requesting Member State.*

Or. en

Amendment 112

Claude Moraes, Carmen Romero López, Birgit Sippel

Proposal for a regulation

Article 18

Text proposed by the Commission

Article 18

Marking of data

1. *The Member State of origin which granted international protection to an applicant for international protection*

Amendment

Article 18

Blocking of data

1. *Data relating to an applicant for international protection which have been recorded pursuant to Article 11 shall be*

whose data were previously recorded pursuant to Article 11 in the Central System shall mark the relevant data in conformity with the requirements for electronic communication with the Central System established by the Agency. This mark shall be stored in the Central System in accordance with Article 12 for the purpose of transmission under Article 9(5).

2. The Member State of origin shall unmark data concerning a third country national or stateless person whose data were previously marked in accordance with paragraph 1 if his or her status is revoked or ended or renewal of his status is refused under Article 14 or 19 of Council Directive 2004/83/EC.

blocked in the central database if that person is granted international protection in a Member State. Such blocking shall be carried out by the Central System on the instructions of the Member State of origin.

2. Hits concerning persons who have been granted international protection in a Member State shall not be transmitted. The Central System shall return a negative result to the requesting Member State.

Or. en

Justification

Data of persons who are granted international protection should not be marked as this means that data can be transmitted to the Member States, even if the applicant has been granted international protection.

Amendment 113
Cornelis de Jong

Proposal for a regulation
Article 19

Text proposed by the Commission

Article 19

Procedure for comparison of fingerprint data with EURODAC data

1. The designated authorities referred to in Article 5(1) and Europol may submit a reasoned electronic request to the verifying authority for the transmission for comparison of fingerprint data to the EURODAC

Amendment

deleted

Central System via the National Access Point. Upon receipt of such a request, the verifying authority shall verify whether the conditions for requesting a comparison referred to in Article 20 or Article 21, as appropriate, are fulfilled.

2. Where all the conditions for requesting a comparison are fulfilled, the verifying authority shall transmit the request for comparison to the National Access Point which will process it to the EURODAC Central System for the purpose of comparison with all the EURODAC data.

3. In exceptional cases of urgency, the verifying authority may transmit the fingerprint data to the National Access Point for comparison immediately upon receipt of a request by a designated authority and only verify ex-post whether all the conditions of Article 20 or Article 21 are fulfilled, including whether an exceptional case of urgency actually existed. The ex-post verification shall take place without undue delay after the processing of the request.

4. Where the ex-post verification determines that the access was not justified, the information communicated from EURODAC shall be destroyed by all authorities that have accessed it and they shall inform the verifying authority of such destruction.

Or. en

Amendment 114
Sarah Ludford

Proposal for a regulation
Article 19 – paragraph 1

Text proposed by the Commission

Amendment

1. The designated authorities referred to in Article 5(1) and Europol may submit a

1. The designated authorities referred to in Article 5(1) and Europol may submit a

reasoned electronic request to the verifying authority for the transmission for comparison of fingerprint data to the EURODAC Central System via the National Access Point. Upon receipt of such a request, the verifying authority shall verify whether the conditions for requesting a comparison referred to in Article 20 or Article 21, as appropriate, are fulfilled.

reasoned electronic request *as provided for in Article 20(1)* to the verifying authority for the transmission for comparison of fingerprint data to the EURODAC Central System via the National Access Point. Upon receipt of such a request, the verifying authority shall verify whether the conditions for requesting a comparison referred to in Article 20 or Article 21, as appropriate, are fulfilled.

Or. en

Justification

It should be specified that the reasoned request should justify the request according to all criteria stipulated in Article 20.

Amendment 115

Claude Moraes, Carmen Romero López, Birgit Sippel

**Proposal for a regulation
Article 19 – paragraph 1**

Text proposed by the Commission

1. The designated authorities referred to in Article 5(1) and Europol may submit a reasoned electronic request to the verifying authority for the transmission for comparison of fingerprint data to the EURODAC Central System via the National Access Point. Upon receipt of such a request, the verifying authority shall verify whether the conditions for requesting a comparison referred to in Article 20 or Article 21, as appropriate, are fulfilled.

Amendment

1. The designated authorities referred to in Article 5(1) and Europol may submit a reasoned electronic request *as provided for in Article 20(1)* to the verifying authority for the transmission for comparison of fingerprint data to the EURODAC Central System via the National Access Point. Upon receipt of such a request, the verifying authority shall verify whether the conditions for requesting a comparison referred to in Article 20 or Article 21, as appropriate, are fulfilled.

Or. en

Justification

It should be specified that the reasoned request should justify the request according to all

criteria stipulated in Article 20. Otherwise it is not clear what the reasoned request should contain.

Amendment 116

Sarah Ludford, Renate Weber, Franziska Keller

Proposal for a regulation

Article 19 – paragraph 3

Text proposed by the Commission

3. In exceptional cases of urgency, the verifying authority may transmit the fingerprint data to the National Access Point for comparison immediately upon receipt of a request by a designated authority and only verify ex-post whether all the conditions of Article 20 or Article 21 are fulfilled, including whether an exceptional case of urgency actually existed. The ex-post verification shall take place without undue delay after the processing of the request.

Amendment

3. In exceptional cases of urgency ***of the need to prevent an imminent danger associated with serious criminal or terrorist offences***, the verifying authority may transmit the fingerprint data to the National Access Point for comparison immediately upon receipt of a request by a designated authority and only verify ex-post whether all the conditions of Article 20 or Article 21 are fulfilled, including whether an exceptional case of urgency actually existed. The ex-post verification shall take place without undue delay after the processing of the request.

Or. en

Justification

The threshold for justifying the bypassing of prior scrutiny should be tightened.

Amendment 117

Sarah Ludford

Proposal for a regulation

Article 19 – paragraph 4 a (new)

Text proposed by the Commission

Amendment

4a. The Commission shall publish an indicative, non-binding model EURODAC request form for use under Article 19, and which correctly reflects the criteria set out

in Article 20(1).

Or. en

Justification

It is reasonable that Member States can decide internally in what way the requesting authority interacts with the verifying authority. But since the verifying authority is called on to evaluate the criteria set out in Article 20(1) in the form of a 'reasoned electronic request' it could be helpful to have some EU-level guidance on what such a form could look like.

Amendment 118
Cornelis de Jong

Proposal for a regulation
Article 20

Text proposed by the Commission

Amendment

Article 20

deleted

*Conditions for access to EURODAC data
by designated authorities*

1. Designated authorities may request the comparison of fingerprint data with those stored in the EURODAC central database within the scope of their powers only if comparisons of national fingerprint databases and of the Automated Fingerprint Databases of other Member States under Decision 2008/615/JHA return negative results and where:

(a) the comparison is necessary for the purpose of the prevention, detection or investigation of terrorist offences or other serious criminal offences;

(b) the comparison is necessary in a specific case; systematic comparisons shall not be carried out; and

(c) there are reasonable grounds to consider that such comparison with EURODAC data will contribute to the prevention, detection or investigation of

any of the criminal offences in question.

2. Requests for comparison with EURODAC data shall be limited to searching with fingerprint data.

Or. en

Amendment 119

Claude Moraes, Carmen Romero López, Birgit Sippel

Proposal for a regulation

Article 20 – paragraph 1 – introductory part

Text proposed by the Commission

1. Designated authorities may request the comparison of fingerprint data with those stored in the EURODAC central database within the scope of their powers only if comparisons of national fingerprint databases and of the Automated Fingerprint Databases of other Member States under Decision 2008/615/JHA return negative results and where:

Amendment

1. Designated authorities may request the comparison of fingerprint data with those stored in the EURODAC central database within the scope of their powers only if comparisons of national fingerprint databases, ***the Visa Information System*** and of the Automated Fingerprint Databases of ***at least a third of*** other Member States under Decision 2008/615/JHA return negative results and where ***all the following cumulative conditions are met:***

Or. en

Justification

Prior consultation of the Visa Information System should be a prerequisite to checking Eurodac as it contains a wider set of third country national fingerprints. It should be clear that the conditions of article 20 (1) are cumulative.

Amendment 120

Franziska Keller, Jan Philipp Albrecht

Proposal for a regulation

Article 20 – paragraph 1 – introductory part

Text proposed by the Commission

1. Designated authorities may request the comparison of fingerprint data with those stored in the EURODAC central database within the scope of their powers only if comparisons of national fingerprint databases **and** of the Automated Fingerprint Databases of other Member States under Decision 2008/615/JHA return negative results and where:

Amendment

1. Designated authorities may request the comparison of fingerprint data with those stored in the EURODAC central database within the scope of their powers only if comparisons of national fingerprint databases, of the Automated Fingerprint Databases of **at least a third of** other Member States under Decision 2008/615/JHA **and of the Visa Information System** return negative results and where:

Or. en

Amendment 121 Sarah Ludford

Proposal for a regulation Article 20 – paragraph 1 – introductory part

Text proposed by the Commission

1. Designated authorities may **request** the comparison of fingerprint data with those stored in the EURODAC central database within the scope of their powers only if comparisons of national fingerprint databases and of the Automated Fingerprint Databases of other Member States under Decision 2008/615/JHA return negative results and where:

Amendment

1. Designated authorities may **submit a reasoned electronic request for** the comparison of fingerprint data with those stored in the EURODAC central database within the scope of their powers only if comparisons of national fingerprint databases and of the Automated Fingerprint Databases of other Member States under Decision 2008/615/JHA return negative results and where:

Or. en

Amendment 122 Renate Weber

Proposal for a regulation

Article 20 – paragraph 1 – point b a (new)

Text proposed by the Commission

Amendment

(ba) there is a substantiated suspicion that the perpetrator of a terrorist or other serious criminal offences has applied for international protection;

Or. en

Amendment 123

Claude Moraes, Carmen Romero López, Birgit Sippel

Proposal for a regulation

Article 20 – paragraph 1 – point c

Text proposed by the Commission

Amendment

(c) there **are** reasonable grounds to consider that such comparison with EURODAC data will contribute to the prevention, detection or investigation of any of the criminal offences in question.

(c) there **is an overriding public security concern which makes proportionate the querying of a database registering persons with a clean criminal record, and there are** reasonable grounds to consider that such comparison with EURODAC data will **substantially** contribute to the prevention, detection or investigation of any of the criminal offences in question **because there are serious grounds to believe that persons in respect of whom comparison with EURODAC is requested will commit or have committed terrorist offences or other serious criminal offences or are victims of a terrorist or serious criminal offence.**

Or. en

Amendment 124

Sarah Ludford, Renate Weber, Franziska Keller

Proposal for a regulation

Article 20 – paragraph 1 – point c

Text proposed by the Commission

(c) there **are** reasonable grounds to consider that such comparison with EURODAC data will contribute to the prevention, detection or investigation of any of the criminal offences in question.

Amendment

(c) there **is an overriding public security concern which makes proportionate the querying of a database registering persons with a clean criminal record, and there are** reasonable grounds to consider that such comparison with EURODAC data will **substantially** contribute to the prevention, detection or investigation of any of the criminal offences in question.

Or. en

Justification

This wording in recital 9 needs to be incorporated in the text.

Amendment 125

Claude Moraes, Carmen Romero López, Birgit Sippel

Proposal for a regulation

Article 20 – paragraph 1 – point c a (new)

Text proposed by the Commission

Amendment

(ca) there is a substantiated suspicion that the suspect, perpetrator or victim of a terrorist or other serious criminal offence has applied for international protection.

Or. en

Justification

Eurodac data searches should be permitted in limited circumstances only, as part of an ongoing criminal investigation and in cases where there is a substantiated suspicion that the perpetrator or suspect has applied for asylum. Eurodac searches should not become an 'automatic' search carried out by the law enforcement authorities.

Amendment 126
Sarah Ludford

Proposal for a regulation
Article 20 – paragraph 1 – point c a (new)

Text proposed by the Commission

Amendment

(ca) there is a substantiated suspicion that the perpetrator or victim of the offence falls in a category covered by this Regulation.

Or. en

Justification

Recital 9 specifies that the Commission believes that authorities responsible for internal security could have access to EURODAC in well defined cases, when there would be a substantiated suspicion that the perpetrator of a terrorist or other serious criminal offence has applied for asylum. Recital 26 specifies that this can equally be the case for a victim of crime. As this is a very important principle it should be reflected in the Article as well as in the recital.

Amendment 127
Franziska Keller, Jan Philipp Albrecht

Proposal for a regulation
Article 20 – paragraph 1 – point c a (new)

Text proposed by the Commission

Amendment

(ca) there is a substantiated suspicion that the perpetrator or victim of the offence is an applicant for international protection.

Or. en

Amendment 128
Cornelis de Jong

Proposal for a regulation

Article 21

Text proposed by the Commission

Amendment

Article 21

deleted

Conditions for access to EURODAC data by Europol

1. Requests for comparison with EURODAC data by Europol shall take place within the limits of its mandate and where necessary for the performance of its tasks pursuant to the Europol Decision and for the purposes of a specific analysis or an analysis of a general nature and of a strategic type.

2. Requests for comparison with EURODAC data shall be limited to comparisons of fingerprint data.

3. Processing of information obtained by Europol from comparison with EURODAC shall be subject to the authorisation of the Member State of origin. Such authorisation shall be obtained via the Europol national unit of that Member State.

Or. en

Amendment 129

Renate Weber

Proposal for a regulation

Article 21 – paragraph 1 a (new)

Text proposed by the Commission

Amendment

1a. However, access to EURODAC data by Europol shall be allowed only for specific cases, under specific circumstances and under the strict conditions provided for in Article 20(1).

Or. en

Amendment 130
Cornelis de Jong

Proposal for a regulation
Article 22

Text proposed by the Commission

Amendment

Article 22

deleted

*Communication between the verifying
authorities and the National Access
Points*

1. EURODAC Communication
*Infrastructure shall be used for the data
transmission by the verifying authorities
of Member States and Europol to the
National Access Points and vice versa. All
communications shall take place
electronically.*

*2. Fingerprints shall be digitally
processed by the Member State and
transmitted in the data format referred to
in Annex I, in order to ensure that the
comparison can be carried out by means
of the computerised fingerprint
recognition system.*

Or. en

Amendment 131
Franziska Keller, Jan Philipp Albrecht

Proposal for a regulation
Article 25 – paragraph 4

Text proposed by the Commission

Amendment

4. The results of the comparison shall be immediately checked in the Member State of origin by a fingerprint expert. Final identification shall be made by the Member State of origin in cooperation with the Member States concerned, pursuant to

4. The results of the comparison shall be immediately checked in the Member State of origin by a **trained** fingerprint expert. Final identification shall be made by the Member State of origin in cooperation with the Member States concerned, pursuant to

Article 32 of the Dublin Regulation.

Article 32 of the Dublin Regulation.

Or. en

Amendment 132
Franziska Keller, Jan Philipp Albrecht

Proposal for a regulation
Article 25 – paragraph 5

Text proposed by the Commission

5. Where final identification in accordance with paragraph 4 *reveal* that the result of the comparison received from the Central System is inaccurate, Member States shall communicate this fact to the Commission and to the Agency.

Amendment

5. Where final identification in accordance with paragraph 4 *reveals* that the result of the comparison received from the Central System is inaccurate, Member States shall communicate this fact ***as soon as possible and no later than after 72 hours*** to the Commission and to the Agency ***and inform the other Member States concerned as soon as possible and no later than after 72 hours on the inaccuracy of the data.***

Or. en

Amendment 133
Cornelis de Jong

Proposal for a regulation
Article 25 – paragraph 5

Text proposed by the Commission

5. Where final identification in accordance with paragraph 4 *reveal* that the result of the comparison received from the Central System is inaccurate, Member States shall communicate this fact to the Commission and to the Agency.

Amendment

5. Where final identification in accordance with paragraph 4 *reveals* that the result of the comparison received from the Central System is inaccurate, Member States shall communicate this fact to the Commission and to the Agency.

Or. en

Amendment 134
Cornelis de Jong

Proposal for a regulation
Article 27 – paragraph 2

Text proposed by the Commission

2. The authorities of Member States which, pursuant to paragraph 1, have access to data recorded in the Central System shall be those designated by each Member State for the purpose of Article 1(1). **This** designation shall specify the **exact** unit responsible for carrying out tasks related to the application of this Regulation. Each Member State shall without delay communicate to the Commission and the Agency a list of those authorities and any amendments thereto. The Agency shall publish the consolidated list in the Official Journal of the European Union. Where there are amendments thereto, the Agency shall publish once a year an updated consolidated list.

Amendment

2. The authorities of Member States which, pursuant to paragraph 1, have access to data recorded in the Central System shall be those designated by each Member State for the purpose of Article 1(1). **That** designation shall specify the **precise** unit responsible for carrying out tasks related to the application of this Regulation. Each Member State shall without delay communicate to the Commission and the Agency a list of those authorities and any amendments thereto, **in the case of amendments at the latest 30 days after the list was amended**. The Agency shall publish the consolidated list in the Official Journal of the European Union. Where there are amendments thereto, the Agency shall publish once a year an updated consolidated list.

Or. en

Amendment 135
Franziska Keller, Jan Philipp Albrecht

Proposal for a regulation
Article 27 – paragraph 2

Text proposed by the Commission

2. The authorities of Member States which, pursuant to paragraph 1, have access to data recorded in the Central System shall be those designated by each Member State for the purpose of Article 1(1). This designation shall specify the exact unit responsible for carrying out tasks related to the application of this Regulation. Each

Amendment

2. The authorities of Member States which, pursuant to paragraph 1, have access to data recorded in the Central System shall be those designated by each Member State for the purpose of Article 1(1). This designation shall specify the exact unit responsible for carrying out tasks related to the application of this Regulation. Each

Member State shall without delay communicate to the Commission and the Agency a list of those **authorities** and any amendments thereto. The Agency shall publish the consolidated list in the Official Journal of the European Union. Where there are amendments thereto, the Agency shall publish **once a year** an updated consolidated list.

Member State shall without delay communicate to the Commission and the Agency a list of those **units** and any amendments thereto. The Agency shall publish the consolidated list in the Official Journal of the European Union. Where there are amendments thereto, the Agency shall publish **regularly** an updated consolidated list **online**.

Or. en

Justification

As a matter of consistency, Member States should not just be obliged to specify the exact unit responsible but also to notify it to the Commission and the Agency.

Amendment 136

Claude Moraes, Carmen Romero López, Birgit Sippel

Proposal for a regulation

Article 29 – paragraph 1 – introductory part

Text proposed by the Commission

1. A person covered by this Regulation shall be informed by the Member State of origin in writing, and where appropriate, orally, in a language which he or she understands **or may reasonably be presumed to understand** of the following:

Amendment

1. A person covered by this Regulation shall be informed by the Member State of origin in writing, and where appropriate, orally, in a language which he or she understands of the following:

Or. en

Justification

The fingerprints may be used by law enforcement authorities as part of a criminal case, therefore it is essential that the person in question fully understands the possible repercussions of providing their data.

Amendment 137

Franziska Keller, Jan Philipp Albrecht

Proposal for a regulation
Article 29 – paragraph 1 – introductory part

Text proposed by the Commission

1. A person covered by this Regulation shall be informed by the Member State of origin in writing, and where **appropriate**, orally, in a language which he or she understands or may reasonably be presumed to understand of the following:

Amendment

1. A person covered by this Regulation shall be informed by the Member State of origin in writing, and where **necessary**, orally, in a language which he or she understands or may reasonably be presumed to understand of the following:

Or. en

Amendment 138
Claude Moraes, Carmen Romero López, Birgit Sippel

Proposal for a regulation
Article 29 – paragraph 1 – point b

Text proposed by the Commission

(b) **regarding** the purpose for which his or her data will be processed within EURODAC including a description of the aims of the Dublin Regulation, in accordance with Article 4 of that Regulation.

Amendment

(b) the purpose for which his or her data will be processed within EURODAC including a description of the aims of the Dublin Regulation, in accordance with Article 4 of that Regulation **and a full and clear explanation of the access that may be granted to law enforcement authorities and Europol for law enforcement purposes.**

Or. en

Justification

The fingerprints may be used by law enforcement authorities as part of a criminal case, therefore it is essential that the person in question fully understands the possible repercussions of providing their data.

Amendment 139
Renate Weber

Proposal for a regulation
Article 29 – paragraph 1 – point b

Text proposed by the Commission

(b) regarding the purpose for which his or her data will be processed within EURODAC including a description of the aims of the Dublin Regulation, in accordance with Article 4 of that Regulation.

Amendment

(b) regarding the purpose for which his or her data will be processed within EURODAC including a description of the aims of the Dublin Regulation, in accordance with Article 4 of that Regulation ***and the fact that EURODAC may be accessed for law enforcement purposes.***

Or. en

Amendment 140
Cornelis de Jong

Proposal for a regulation
Article 29 – paragraph 1 – point e

Text proposed by the Commission

(e) the existence of the right of access to data relating to him/her, and the right to request that inaccurate data relating to him/her be corrected or that unlawfully processed data relating to ***them*** be erased, as well as the right to receive information on the procedures for exercising those rights including the contact details of the controller and the National Supervisory Authorities referred to in Article 31(1).

Amendment

(e) the existence of the right of access to data relating to him/her, and the right to request that inaccurate data relating to him/her be corrected or that unlawfully processed data relating to ***him/her*** be erased, as well as the right to receive information on the procedures for exercising those rights including the contact details of the controller and the National Supervisory Authorities referred to in Article 31(1).

Or. en

Amendment 141
Franziska Keller, Jan Philipp Albrecht

Proposal for a regulation

Article 29 – paragraph 1 – subparagraph 4

Text proposed by the Commission

A common leaflet, containing at least the information referred to in paragraph 1 of this Article and the information referred to in Article 4(1) of the Dublin Regulation shall be drawn up in accordance with the procedure referred to in Article 40(2) of the Dublin Regulation. The leaflet **should** be "clear and simple, drafted in a language that the person understands or may reasonably be presumed to understand.

Amendment

A common leaflet, containing at least the information referred to in paragraph 1 of this Article and the information referred to in Article 4(1) of the Dublin Regulation shall be drawn up in accordance with the procedure referred to in Article 40(2) of the Dublin Regulation. The leaflet **shall** be "clear and simple, drafted in a language that the person understands or may reasonably be presumed to understand. ***It shall also include information on the rights of the data subject and the possibility of assistance by the National Supervisory Authorities as well as the contact details of the controller and the National Supervisory Authorities.***

Or. en

Amendment 142

Franziska Keller, Jan Philipp Albrecht

Proposal for a regulation

Article 29 – paragraph 1 – subparagraph 5

Text proposed by the Commission

Where a person covered by this Regulation is a minor, Member States shall provide the information in an age-appropriate manner.

Amendment

Where a person covered by this Regulation is a minor, Member States shall provide the information in an age-appropriate manner. ***The Commission shall provide templates of the leaflets for adults and minors to the Member States.***

Or. en

Amendment 143

Franziska Keller, Jan Philipp Albrecht

Proposal for a regulation

Article 29 – paragraph 9

Text proposed by the Commission

9. Whenever a person requests data relating to him or her in accordance with paragraph 2, the competent authority shall keep a record in the form of a written document that such a request was made, and shall make this document available to the National Supervisory Authorities without delay, upon their request.

Amendment

9. Whenever a person requests data relating to him or her in accordance with paragraph 2, the competent authority shall keep a record in the form of a written document that such a request was made, and shall make this document available to the National Supervisory Authorities without delay, upon their request. ***It shall immediately inform the National Supervisory Authorities in case a person requests the correction or erasure of its data. No later than three weeks after the request it shall confirm to the National Supervisory Authorities that it has taken action to correct or erase the data or, in case the Member State does not agree that the data recorded in the Central System are inaccurate or have been recorded unlawfully, explain why it is not prepared to correct or erase the data.***

Or. en

Justification

Since persons whose data are stored in Eurodac are presumably not familiar with rights and procedures related to data protection in the Member States, the role of National Supervisory Authorities should be strengthened. Assistance by National Supervisory Authorities is all the more important if law enforcement agencies get access to the data.

Amendment 144
Claude Moraes

Proposal for a regulation
Article 30 – paragraph 1 a (new)

Text proposed by the Commission

Amendment

1a. The National Supervisory Authority shall ensure that every year an audit of the processing of personal data according

to Article 1(2) is carried out, including an analysis of all reasoned electronic requests.

The audit shall be attached to the Member State annual report referred to in Article 40(8).

Or. en

Justification

The national data protection authority should annually audit the use of Eurodac specifically as a law enforcement tool. The Member States have to present the European Parliament with annual reports according to Article 40, but the use of Eurodac for law enforcement access by national authorities should be audited by national DPs and the results of these audits communicated equally to the Parliament.

Amendment 145 **Renate Weber**

Proposal for a regulation **Article 31 – paragraph 1**

Text proposed by the Commission

1. The European Data Protection Supervisor shall ensure that all the personal data processing activities concerning EURODAC, in particular by the Agency are carried out in accordance with Regulation (EC) No 45/2001 and this Regulation.

Amendment

1. The European Data Protection Supervisor shall ensure that all the personal data processing activities concerning EURODAC, in particular by the Agency **and by Europol** are carried out in accordance with Regulation (EC) No 45/2001 and this Regulation.

Or. en

Amendment 146 **Franziska Keller, Jan Philipp Albrecht**

Proposal for a regulation

Article 31 – paragraph 2

Text proposed by the Commission

2. The European Data Protection Supervisor shall ensure that an audit of the Agency's personal data processing activities is carried out in accordance with international auditing standards at least every **four years**. A report of such audit shall be sent to the European Parliament, the Council, the Agency, the Commission and the National Supervisory Authorities. The Agency shall be given an opportunity to make comments before the report is adopted.

Amendment

2. The European Data Protection Supervisor shall ensure that an audit of the Agency's personal data processing activities is carried out in accordance with international auditing standards at least every **two years**. A report of such audit shall be sent to the European Parliament, the Council, the Agency, the Commission and the National Supervisory Authorities. The Agency shall be given an opportunity to make comments before the report is adopted.

Or. en

Amendment 147

Sarah Ludford, Franziska Keller

Proposal for a regulation

Article 32 – paragraph 1 a (new)

Text proposed by the Commission

Amendment

1a. The National Supervisory Authority shall ensure that every year an audit of the processing of personal data according to Article 1(2) is carried out, including an analysis of all reasoned electronic requests.

The audit shall be attached to the Member State annual report referred to in Article 40(8).

Or. en

Justification

The national data protection authority should annually audit the use of Eurodac specifically as a law enforcement tool. The Member States have to present the European Parliament with annual reports according to Article 40, but the use of Eurodac for law enforcement access by national authorities should be audited by national DPs and the results of these audits

communicated equally to the Parliament.

Amendment 148
Sarah Ludford, Renate Weber

Proposal for a regulation
Article 32 – paragraph 2 a (new)

Text proposed by the Commission

Amendment

2a. Both the national and European supervisory authorities shall be provided with sufficient financial and personal resources to be able to supervise the use and access to Eurodac data adequately.

Or. en

Amendment 149
Cornelis de Jong

Proposal for a regulation
Article 33

Text proposed by the Commission

Amendment

Article 33

deleted

Protection of personal data for the purposes of the prevention, detection and investigation of terrorist offences or of other serious criminal offences

- 1. The Framework Decision 2008/977/JHA is applicable to the processing of relevant personal data for law enforcement purposes under this Regulation.***
- 2. The processing of personal data by Europol pursuant to this Regulation shall be in accordance with Decision 2009/371/JHA.***
- 3. Personal data obtained pursuant to this Regulation from EURODAC shall only be processed for the purposes of the***

prevention, detection and investigation of terrorist offences or of other serious criminal offences.

4. Personal data obtained by a Member State or Europol pursuant to this Regulation from EURODAC shall be erased in national and Europol files after a period of one month, if the data are not required for a specific ongoing criminal investigation by that Member State, or Europol.

5. The monitoring of the lawfulness of the processing of personal data under this Regulation by the Member States, including their transmission to and from EURODAC shall be carried out by the national competent authorities designated pursuant to Framework Decision 2008/977/JHA.

Or. en

Amendment 150

Claude Moraes, Carmen Romero López, Birgit Sippel

Proposal for a regulation

Article 33 – paragraph 3

Text proposed by the Commission

3. Personal data obtained pursuant to this Regulation from EURODAC shall only be processed for the purposes of the prevention, detection and investigation of ***terrorist offences or of other serious criminal offences.***

Amendment

3. Personal data obtained pursuant to this Regulation from EURODAC ***for the purposes as laid down in Article 1(2)*** shall only be processed for the purposes of the prevention, detection and investigation of ***the specific criminal investigation for which the data has been requested by that Member State, or Europol.***

Or. en

Justification

To ensure consistency with amendment to article 33, paragraph 4.

Amendment 151
Renate Weber

Proposal for a regulation
Article 33 – paragraph 4

Text proposed by the Commission

Amendment

4. Personal data obtained by a Member State or Europol pursuant to this Regulation from EURODAC shall be erased in national and Europol files after a period of one month, if the data are not required for a specific ongoing criminal investigation by that Member State, or Europol.

deleted

Or. en

Amendment 152
Sarah Ludford, Franziska Keller

Proposal for a regulation
Article 33 – paragraph 4

Text proposed by the Commission

Amendment

4. Personal data obtained by a Member State or Europol pursuant to this Regulation from EURODAC shall be erased in national and Europol files after a period of one month, if the data are not required for **a** specific ongoing criminal investigation by that Member State, or Europol.

4. Personal data, **as well as the record of the search**, obtained by a Member State or Europol pursuant to this Regulation from EURODAC shall be erased in national and Europol files after a period of one month, if the data are not required for **the purposes of the** specific ongoing criminal investigation **for which the data has been requested** by that Member State, or Europol.

Or. en

Justification

The requirement for erasure needs to be tightened and extended to the record of the search

having been made.

Amendment 153

Claude Moraes, Carmen Romero López, Birgit Sippel

Proposal for a regulation

Article 33 – paragraph 4

Text proposed by the Commission

4. Personal data obtained by a Member State or Europol pursuant to this Regulation from EURODAC shall be erased in national and Europol files after a period of one month, if the data are not required for **a** specific ongoing criminal investigation by that Member State, or Europol.

Amendment

4. Personal data, **as well as the record of the search**, obtained by a Member State or Europol pursuant to this Regulation from EURODAC shall be erased in **all** national and Europol files after a period of one month, if the data are not required for **the purposes of the** specific ongoing criminal investigation **for which the data has been requested** by that Member State, or Europol.

Or. en

Justification

The requirement for erasure needs to be tightened and extended to the record of the search having been made.

Amendment 154

Cornelis de Jong

Proposal for a regulation

Article 34 – paragraph 2 – point a

Text proposed by the Commission

(a) physically protect data, including by making contingency plans for the protection of **critical** infrastructure;

Amendment

(a) physically protect data, including by making contingency plans for the protection of **relevant** infrastructure;

Or. en

Amendment 155
Franziska Keller, Jan Philipp Albrecht

Proposal for a regulation
Article 34 – paragraph 2 – point a

Text proposed by the Commission

(a) physically protect data, including by making contingency plans for the protection of **critical** infrastructure;

Amendment

(a) physically protect data, including by making contingency plans for the protection of **relevant** infrastructure;

Or. en

Amendment 156
Renate Weber

Proposal for a regulation
Article 34 – paragraph 2 – point a

Text proposed by the Commission

(a) physically protect data, including by making contingency plans for the protection of **critical** infrastructure;

Amendment

(a) physically protect data, including by making contingency plans for the protection of **relevant** infrastructure;

Or. en

Amendment 157
Franziska Keller, Jan Philipp Albrecht

Proposal for a regulation
Article 34 – paragraph 2 – point g

Text proposed by the Commission

(g) ensure that all authorities with a right of access to EURODAC create profiles describing the functions and responsibilities of persons who are authorised to access, enter, update, erase and search the data and make these profiles available to the National Supervisory Authorities referred to in Article 25 of

Amendment

(g) ensure that all authorities with a right of access to EURODAC create profiles describing the functions and responsibilities of persons who are authorised to access, enter, update, erase and search the data and make these profiles **and any other relevant information the authorities may require for the purpose of**

Framework Decision 2008/977/JHA without delay at their request (personnel profiles);

carrying out supervision available to the National Supervisory Authorities referred to *in Article 28 of Directive 95/46/EC and in Article 25 of Framework Decision 2008/977/JHA* without delay at their request (personnel profiles);

Or. en

Amendment 158
Franziska Keller, Jan Philipp Albrecht

Proposal for a regulation
Article 34 – paragraph 2 – point k

Text proposed by the Commission

(k) monitor the effectiveness of the security measures referred to in this paragraph and take the necessary organisational measures related to internal monitoring to ensure compliance with this Regulation (self-auditing).

Amendment

(k) monitor the effectiveness of the security measures referred to in this paragraph and take the necessary organisational measures related to internal monitoring to ensure compliance with this Regulation (self-auditing). ***For the purpose of the Business Continuity Plan, the Member States shall inform the Agency and the National Supervisory Authorities of security incidents they detected on their system. The Agency shall inform the Member States, Europol and the European Data Protection Supervisor in case of security incidents. All parties shall collaborate during a security incident.***

Or. en

Amendment 159
Renate Weber

Proposal for a regulation

Article 34 – paragraph 2 – point k

Text proposed by the Commission

(k) monitor the effectiveness of the security measures referred to in this paragraph and take the necessary organisational measures related to internal monitoring to ensure compliance with this Regulation (self-auditing).

Amendment

(k) monitor the effectiveness of the security measures referred to in this paragraph and take the necessary organisational measures related to internal monitoring to ensure compliance with this Regulation (self-auditing) **and also near real-time observation of the system using specialized tools.**

Or. en

Amendment 160

Renate Weber

Proposal for a regulation

Article 34 – paragraph 3 a (new)

Text proposed by the Commission

Amendment

3a. In cases of security incidents, Member States shall inform the Agency about the security incidents detected on their system.

The Agency shall inform all stakeholders about security incidents.

All parties shall collaborate during a security incident.

National Supervisory authorities and the EDPS shall be informed about security incidents.

Or. en

Amendment 161

Claude Moraes, Carmen Romero López, Birgit Sippel

Proposal for a regulation

Article 35

Text proposed by the Commission

Personal data obtained by a Member State or Europol pursuant to this Regulation from the EURODAC central database shall not be transferred or made available to any third country or international organisation or a private entity established in or outside the European Union. This prohibition shall be without prejudice to the right of Member States to transfer such data to third countries to which the Dublin Regulation applies.

Amendment

Personal data obtained by a Member State or Europol pursuant to this Regulation, ***including personal data obtained by a Member State and processed further in national databases for law enforcement purposes***, from the EURODAC central database shall not be transferred or made available to any third country or international organisation or a private entity established in or outside the European Union. This prohibition shall be without prejudice to the right of Member States to transfer such data to third countries to which the Dublin Regulation applies ***provided that the Member State transferring such data has obtained the commitment of the third country that it will not transfer or made available to any third country or international organisation or a private entity established in or outside the European Union this personal data.***

Or. en

Justification

Transfer of data to third countries must be prohibited, including all data and information exchanged between Member States on the basis of a 'positive hit' in Eurodac.

Amendment 162

Sarah Ludford, Renate Weber

Proposal for a regulation

Article 35

Text proposed by the Commission

Personal data obtained by a Member State or Europol pursuant to this Regulation from the EURODAC central database shall

Amendment

Personal data obtained by a Member State or Europol pursuant to this Regulation from the EURODAC central database shall

not be transferred or made available to any third country or international organisation or a private entity established in or outside the European Union. This prohibition shall be without prejudice to the right of Member States to transfer such data to third countries to which the Dublin Regulation applies.

not be transferred or made available to any third country or international organisation or a private entity established in or outside the European Union. This prohibition shall be without prejudice to the right of Member States to transfer such data to third countries to which the Dublin Regulation applies. ***Personal data obtained by a Member State or Europol and processed further in national databases shall not be transferred or made available to any third country or international organisation or a private entity established in or outside the European Union.***

Or. en

Justification

The ban on transfers to third countries should be extended to data which has been further processed.

Amendment 163 **Cornelis de Jong**

Proposal for a regulation **Article 35**

Text proposed by the Commission

Personal data obtained by a Member State or Europol pursuant to this Regulation from the EURODAC central database shall not be transferred or made available to any third country or international organisation or a private entity established in or outside the European Union. This prohibition shall be without prejudice to the right of Member States to transfer such data to third countries to which the Dublin Regulation applies.

Amendment

Personal data obtained by a Member State pursuant to this Regulation from the EURODAC central database shall not be transferred or made available to any third country or international organisation or a private entity established in or outside the European Union. This prohibition shall be without prejudice to the right of Member States to transfer such data to third countries to which the Dublin Regulation applies. ***Personal data obtained by a Member State and processed further in national databases shall not be transferred or made available to any third***

country or international organisation or a private entity established in or outside the European Union.

Or. en

Amendment 164
Cornelis de Jong

Proposal for a regulation
Article 36 – paragraph 2

Text proposed by the Commission

2. The log or documentation shall show in all cases:
- (a) the exact purpose of the request for comparison, including the concerned form of a terrorist offence or other serious criminal offence and for Europol, the exact purpose of the request for comparison;
 - (b) the respective national file reference;
 - (c) the date and exact time of the request for comparison by the National Access Point to the EURODAC Central System;
 - (d) the name of the authority having requested access for comparison, and the person responsible who has made the request and processed the data;
 - (e) where applicable the use of the urgent procedure referred to in Article 19(3) and the decision taken with regard to the ex-post verification;***
 - (f) the data used for comparison;
 - (g) according to national rules or the rules of the Europol decision the identifying mark of the official who carried out the search and of the official who ordered the search or supply.***

Amendment

2. The log or documentation shall show in all cases:
- (a) the exact purpose of the request for comparison, including the concerned form of a terrorist offence or other serious criminal offence and for Europol, the exact purpose of the request for comparison;
 - (b) the respective national file reference;
 - (c) the date and exact time of the request for comparison by the National Access Point to the EURODAC Central System;
 - (d) the name of the authority having requested access for comparison, and the person responsible who has made the request and processed the data;
 - (da)*** the data used for comparison.

Or. en

Amendment 165
Cornelis de Jong

Proposal for a regulation
Article 38 – paragraph 2 – point a

Text proposed by the Commission

(a) points (t), (u) and (v) are replaced by the following:

“(t) to adopt the reports on the technical functioning of SIS II pursuant to Article 50(4) of Regulation (EC) No 1987/2006 and Article 66(4) of Decision 2007/533/JHA respectively, of VIS pursuant to Article 50(3) of Regulation (EC) No 767/2008 and Article 17(3) of Decision 2008/633/JHA; and of EURODAC pursuant to Article 40(4) of Regulation (EU) No/... [of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No {.../....} establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third country national or a stateless person] ***and to request comparisons with EURODAC data by Member States' law enforcement authorities for law enforcement purposes;***

Amendment

(a) points (t), (u) and (v) are replaced by the following:

“(t) to adopt the reports on the technical functioning of SIS II pursuant to Article 50(4) of Regulation (EC) No 1987/2006 and Article 66(4) of Decision 2007/533/JHA respectively, of VIS pursuant to Article 50(3) of Regulation (EC) No 767/2008 and Article 17(3) of Decision 2008/633/JHA; and of EURODAC pursuant to Article 40(4) of Regulation (EU) No/... [of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No {.../....} establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third country national or a stateless person];

Or. en

Amendment 166
Cornelis de Jong

Proposal for a regulation

Article 38 – paragraph 3

Text proposed by the Commission

Amendment

3. In Article 15 paragraph (4) is replaced by the following: *deleted*

“4. Europol and Eurojust may attend the meetings of the Management Board as observers when a question concerning SIS II, in relation to the application of Decision 2007/533/JHA, is on the agenda. Europol may also attend the meetings of the Management Board as observer when a question concerning VIS, in relation to the application of Decision 2008/633/JHA, is on the agenda or when a question concerning EURODAC, in relation with the application of Regulation (EU) No .../.... [of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No/....]is on the agenda.”

Or. en

Amendment 167

Franziska Keller, Jan Philipp Albrecht

Proposal for a regulation

Article 38 – paragraph 4 – point a

Text proposed by the Commission

Amendment

(a) in paragraph 5 point (g) is replaced by the following: *deleted*

“(g) without prejudice to Article 17 of the Staff Regulations, establish confidentiality requirements in order to comply with Article 17 of Regulation (EC) No 1987/2006, Article 17 of Decision 2007/533/JHA and Article 26(9) of Regulation (EC) No 767/2008 respectively and Article 4(6) of Regulation (EU) No

.../.... [of the European Parliament and the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No .../...];”

Or. en

Amendment 168
Cornelis de Jong

Proposal for a regulation
Article 38 – paragraph 5

Text proposed by the Commission

Amendment

5. In Article 19 paragraph 3 is replaced by the following: *deleted*

"3. Europol and Eurojust may each appoint a representative to the SIS II Advisory Group. Europol may also appoint a representative to the VIS and to the EURODAC Advisory Groups."

Or. en

Amendment 169
Cornelis de Jong

Proposal for a regulation
Article 39 – paragraph 3

Text proposed by the Commission

Amendment

3. Each Member State and Europol shall set up and maintain at their expense the technical infrastructure necessary to implement this Regulation, and be responsible for bearing its costs resulting from requests for comparison with EURODAC data for the purposes of the prevention, detection or investigation of any of the criminal offences defined in *deleted*

this Regulation.

Or. en

Amendment 170

Franziska Keller, Jan Philipp Albrecht

Proposal for a regulation

Article 40 – paragraph 4

Text proposed by the Commission

4. Every **two years**, the Agency shall submit to the European Parliament, the Council, the Commission and the European Data Protection Supervisor a report on the technical functioning of the Central System, including the security thereof.

Amendment

4. Every **one year**, the Agency shall submit to the European Parliament, the Council, the Commission and the European Data Protection Supervisor a report on the technical functioning of the Central System, including the security thereof.

Or. en

Amendment 171

Sarah Ludford

Proposal for a regulation

Article 40 – paragraph 5

Text proposed by the Commission

5. Three years after the start of application of this Regulation as provided for in Article 46(2) and every four years thereafter, the Commission shall produce an overall evaluation of EURODAC, examining results achieved against objectives and assessing the continuing validity of the underlying rationale, and any implications for future operations, as well as make any necessary recommendations. The Commission shall transmit the evaluation to the European Parliament and the Council.

Amendment

5. Three years after the start of application of this Regulation as provided for in Article 46(2) and every four years thereafter, the Commission shall produce an overall evaluation of EURODAC, examining results achieved against objectives and assessing the continuing validity of the underlying rationale, ***including whether law enforcement access has led to the stigmatisation of applicants for international protection***, and any implications for future operations, as well as make any necessary recommendations. The Commission shall transmit the evaluation to the European

Amendment 172

Claude Moraes, Carmen Romero López, Birgit Sippel

Proposal for a regulation

Article 40 – paragraph 5

Text proposed by the Commission

5. Three years after the start of application of this Regulation as provided for in Article 46(2) and every four years thereafter, the Commission shall produce an overall evaluation of EURODAC, examining results achieved against objectives and assessing the continuing validity of the underlying rationale, and any implications for future operations, as well as make any necessary recommendations. The Commission shall transmit the evaluation to the European Parliament and the Council.

Amendment

5. Three years after the start of application of this Regulation as provided for in Article 46(2) and every four years thereafter, the Commission shall produce an overall evaluation of EURODAC, examining the results achieved against objectives ***and the impact on fundamental rights*** and assessing the continuing validity of the underlying rationale, and any implications for future operations, ***including whether the operation of the search functionality for law enforcement purposes will have led to the stigmatisation of persons seeking international protection***, as well as make any necessary recommendations. The Commission shall transmit the evaluation to the European Parliament and the Council.

Justification

Information of a group of vulnerable people is being specifically made available. All measures possible must be taken to ensure that their fundamental rights are protected and this regulation does not stigmatize them.

Amendment 173

Franziska Keller, Jan Philipp Albrecht

Proposal for a regulation
Article 40 – paragraph 5

Text proposed by the Commission

5. Three years after the start of application of this Regulation as provided for in Article 46(2) and every **four years** thereafter, the Commission shall produce an overall evaluation of EURODAC, examining results achieved against objectives and assessing the continuing validity of the underlying rationale, and any implications for future operations, as well as make any necessary recommendations. The Commission shall transmit the evaluation to the European Parliament and the Council.

Amendment

5. Three years after the start of application of this Regulation as provided for in Article 46(2) and every **three years** thereafter, the Commission shall produce an overall evaluation of EURODAC, examining results achieved against objectives and assessing the continuing validity of the underlying rationale, and any implications for future operations, as well as make any necessary recommendations. The Commission shall transmit the evaluation to the European Parliament and the Council.

Or. en

Amendment 174
Cornelis de Jong

Proposal for a regulation
Article 40 – paragraph 8

Text proposed by the Commission

8. Each Member State and Europol shall prepare annual reports on the effectiveness of the comparison of fingerprint data with EURODAC data for law enforcement access purposes, containing information and statistics on the exact purpose of the comparison, including the type of a terrorist offence or a serious criminal offence, number of requests for comparison, the number and type of cases which have ended in successful identifications and on the need and use made of the exceptional case of urgency as well as on those cases where that urgency was not accepted by the ex post verification carried out by the verifying authority. Such reports shall be

Amendment

deleted

transmitted to the Commission.

Or. en

Amendment 175

Franziska Keller, Jan Philipp Albrecht

Proposal for a regulation

Article 40 – paragraph 8

Text proposed by the Commission

Amendment

8. Each Member State and Europol shall prepare annual reports on the effectiveness of the comparison of fingerprint data with EURODAC data for law enforcement access purposes, containing information and statistics on the exact purpose of the comparison, including the type of a terrorist offence or a serious criminal offence, number of requests for comparison, the number and type of cases which have ended in successful identifications and on the need and use made of the exceptional case of urgency as well as on those cases where that urgency was not accepted by the ex post verification carried out by the verifying authority. Such reports shall be transmitted to the Commission.

deleted

Or. en

Amendment 176

Sarah Ludford

Proposal for a regulation

Article 40 – paragraph 8

Text proposed by the Commission

Amendment

8. Each Member State and Europol shall prepare annual reports on the effectiveness of the comparison of fingerprint data with

8. Each Member State and Europol shall prepare annual reports on the effectiveness of the comparison of fingerprint data with

EURODAC data for law enforcement access purposes, containing information and statistics on the exact purpose of the comparison, including the type of a terrorist offence or a serious criminal offence, number of requests for comparison, the number and type of cases which have ended in successful identifications and on the need and use made of the exceptional case of urgency as well as on those cases where that urgency was not accepted by the ex post verification carried out by the verifying authority. Such reports shall be transmitted to the Commission.

EURODAC data for law enforcement access purposes, containing information and statistics on the exact purpose of the comparison, including the type of a terrorist offence or a serious criminal offence, ***grounds given for reasonable suspicion***, number of requests for comparison, the number and type of cases which have ended in successful identifications and on the need and use made of the exceptional case of urgency as well as on those cases where that urgency was not accepted by the ex post verification carried out by the verifying authority. Such reports shall be transmitted to the Commission. ***Based on these annual reports and in addition to the overall evaluation provided for in paragraph 5, the Commission shall compile an annual report on law enforcement access to EURODAC and shall transmit the evaluation to the European Parliament, the Council and the EDPS.***

Or. en

Justification

The first change reflects the amendment in Article 20(d)(new). The second calls for the Commission to report annually on law enforcement access based on national and Europol reports.

Amendment 177 **Claude Moraes**

Proposal for a regulation **Article 40 – paragraph 8**

Text proposed by the Commission

8. Each Member State and Europol shall prepare annual reports on the effectiveness of the comparison of fingerprint data with EURODAC data for law enforcement access purposes, containing information

Amendment

8. Each Member State and Europol shall prepare annual reports on the effectiveness of the comparison of fingerprint data with EURODAC data for law enforcement access purposes, containing information

and statistics on the exact purpose of the comparison, including the type of a terrorist offence or a serious criminal offence, number of requests for comparison, the number and type of cases which have ended in successful identifications and on the need and use made of the exceptional case of urgency as well as on those cases where that urgency was not accepted by the ex post verification carried out by the verifying authority. Such reports shall be transmitted to the Commission.

and statistics on the exact purpose of the comparison, including the type of a terrorist offence or a serious criminal offence, ***grounds given for reasonable suspicion***, number of requests for comparison, the number and type of cases which have ended in successful identifications and on the need and use made of the exceptional case of urgency as well as on those cases where that urgency was not accepted by the ex post verification carried out by the verifying authority. Such reports shall be transmitted to the Commission. ***Based on these annual reports and in addition to the overall evaluation provided for in paragraph 5, the Commission shall compile an annual report on law enforcement access to EURODAC and shall transmit the evaluation to the European Parliament, the Council and the EDPS.***

Or. en

Justification

The first change reflects the amendment in Article 20(d)(new). The second calls for the Commission to report annually on law enforcement access based on national and Europol reports.

Amendment 178 **Cornelis de Jong**

Proposal for a regulation **Article 40 – paragraph 9**

Text proposed by the Commission

9. The Agency, Member States ***and Europol*** shall provide the Commission the information necessary to draft the evaluation reports referred to in paragraph 5. This information shall not jeopardise working methods nor include information that reveals sources, staff members or

Amendment

9. The Agency ***and*** Member States shall provide the Commission the information necessary to draft the evaluation reports referred to in paragraph 5. This information shall not jeopardise working methods nor include information that reveals sources, staff members or investigations of the

investigations of the designated authorities.

designated authorities.

Or. en

Amendment 179

Franziska Keller, Jan Philipp Albrecht

Proposal for a regulation

Article 43 – paragraph 1

Text proposed by the Commission

1. By [three months after the date of entry into force of this Regulation] at the latest each Member State shall notify the Commission of its designated authorities and shall notify without delay any amendment thereto.

Amendment

1. By [three months after the date of entry into force of this Regulation] at the latest each Member State shall notify the Commission of its designated authorities ***and the operation units referred to in Article 5(3)*** and shall notify without delay any amendment thereto.

Or. en

Amendment 180

Renate Weber

Proposal for a regulation

Article 43 – paragraph 1 a (new)

Text proposed by the Commission

Amendment

1a. Member States shall constantly update the information they have provided to the Commission. The Commission shall make this information available to the other Member States, Europol and the public via a constantly updated electronic publication.

Or. en

Amendment 181

Renate Weber

Proposal for a regulation
Article 43 – paragraph 2 a (new)

Text proposed by the Commission

Amendment

2a. Europol shall constantly update the information it has provided to the Commission. The Commission shall make this information available to the other Member States, Europol and the public via a constantly updated electronic publication.

Or. en

Amendment 182
Franziska Keller, Jan Philipp Albrecht

Proposal for a regulation
Article 43 – paragraph 4

Text proposed by the Commission

Amendment

4. The Commission shall publish information referred to in paragraphs 1, 2 and 3 in the Official Journal of the European Union on an annual basis.

4. The Commission shall publish information referred to in paragraphs 1, 2 and 3 in the Official Journal of the European Union on an annual basis, ***via a regularly updated electronic publication.***

Or. en

Anlage 7



**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 6 September 2012

13420/12

**Interinstitutional File:
2008/0242 (COD)**

EURODAC 17

COVER NOTE

from: Mr Peter HUSTINX, Supervisor, European Data Protection Supervisor
date of receipt: 5 September 2012
to: Mr Herman Van Rompuy, President of the Council of the European Union

Subject: Amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No [.../...] (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person) and to request comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (Recast version)
- Opinion of the European Data Protection Supervisor on the amended proposal

Delegations will find attached the opinion of the European Data Protection Supervisor on the above amended proposal.



PETER HUSTINX
SUPERVISOR

President of the Council of the European
Union
General Secretariat
Council of the European Union
Rue de la Loi 175
1048 Brussels

Brussels, 05 September 2012
PH/PDL/mch/ D(2012) 1747 C 2012-0473

Subject: Opinion of the European Data Protection Supervisor on the amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No [.../...] [...] (Recast version)

Dear Mr President,

With regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of data by the Community institutions and bodies and on the free movement of such data, and in particular its Article 41, I send you my opinion on the amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No [.../...] [...] (Recast version).

I have sent this opinion to the President of the European Commission and the President of the European Parliament as well.

Yours sincerely,



Peter HUSTINX

Annex: Opinion

Cc: Mr Uwe CORSEPIUS, Secretary-General
Mr Kornelios KORNELIOU, Permanent Representative of Cyprus to the European
Union
Mr Guy STESSSENS, Secretariat General of the Council

Postal address: rue Wiertz 60 - B-1047 Brussels

Offices: rue Montoyer 63

E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu

Tel.: 02-283 19 00 - Fax : 02-283 19 50



Opinion of the European Data Protection Supervisor on the amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No [.../...] [.....] (Recast version)

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular Articles 7 and 8 thereof,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data,¹

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data,²

Having regard to Council Framework Decision 2008/977/JHA of 27 November 2008³ on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters,

HAS ADOPTED THE FOLLOWING OPINION:

1. INTRODUCTION

1.1. Consultation of the EDPS

1. On 30 May 2012, the Commission adopted a proposal concerning a recast for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of

¹ OJ L281, 23.11.1995, p. 31.

² OJ L8, 12.1.2001, p. 1.

³ OJ L350, 30.12.2008, p. 60.

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 63
E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

Regulation (EU) No [...] (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person) and to request comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the Area of Freedom, Security and Justice (hereinafter: 'the Proposal').⁴

2. The Proposal was sent by the Commission to the EDPS for consultation on 5 June 2012, pursuant to Article 28(2) of Regulation (EC) No 45/2001. The EDPS recommends that reference to the present consultation be made in the preamble of the Proposal.
3. The EDPS regrets that the Commission services did not ask the EDPS to provide informal comments to the Commission before the adoption of the Proposal, according to the agreed procedure in relation to Commission documents relating to the processing of personal data.⁵
4. The Proposal was presented to the Home Affairs Ministers at the Justice and Home Affairs Council on 7-8 June 2012 and is currently under discussion within Council and the European Parliament with a view to adopt a regulation under the ordinary legislative procedure by the end of 2012. The present opinion of the EDPS intends to give input to this procedure.

1.2. Background

5. EURODAC was established in 2000 by Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of the Dublin Convention.⁶ The Commission presented proposals for amendment of this Regulation in 2008⁷ and in 2009.⁸ The 2008 Commission Proposal aimed at ensuring a higher degree of harmonisation and better standards of protection for the Common European Asylum System (CEAS), while the 2009 Commission Proposal sought to use asylum seekers' fingerprints for law enforcement purposes.
6. The EDPS delivered Opinions on both the 2008 Commission Proposal⁹ and the 2009 Commission Proposal.¹⁰ Especially in the second Opinion, the EDPS was very critical.

⁴ COM(2012)254 final.

⁵ The last time, the EDPS was informally consulted by the Commission on an amendment of the EURODAC Regulation was in 2008.

⁶ OJ L316, 15.12.2000, p. 1.

⁷ COM(2008)825 final.

⁸ COM(2009)342 final and COM(2009)344 final.

⁹ Opinion of 18 February 2009 on the Proposal for a Regulation concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No [...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] (COM(2008)825), OJ C229, 23.9.2009, p. 6.

7. Following the entry into force of the Treaty on the Functioning of the European Union (TFEU) and the abolition of the pillar structure, the Commission adopted a new proposal in 2010, replacing the earlier proposals.¹¹ With a view to progressing in the negotiations on the asylum package and facilitating the conclusion of an agreement on EURODAC, the 2010 Commission Proposal did no longer include provisions on access to EURODAC for law enforcement purposes.
8. The current Proposal withdraws and replaces the 2010 Commission Proposal using the recast procedure in order to:
 - take into account a resolution of the European Parliament and the results of negotiations in the Council;¹²
 - introduce the possibility for Member States' law enforcement authorities and Europol to access the EURODAC central database for the purposes of prevention, detection and investigation of terrorist offences and other serious criminal offences;
 - introduce the necessary amendments to Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the Area of Freedom, Security and Justice.¹³
9. According to the Explanatory Memorandum of the Proposal, it has become clear that including law enforcement access for EURODAC 'is needed as part of a balanced deal on the negotiations of the Common European Asylum System package'.¹⁴ No new consultation and impact assessment were conducted for the current Proposal since, according to the Explanatory Memorandum, the Impact Assessments of 2008 and 2009¹⁵ were still valid. Apparently, for the same reasons, the EDPS was not given the possibility to provide informal comments, as mentioned in point 3 above.

1.3. Reasons for and structure of this EDPS Opinion

10. In the present Opinion, the EDPS wishes to highlight the following main concerns:
 - the procedure followed does not do justice to the fundamental nature of the Proposal; a new impact assessment should have been performed;
 - the necessity and proportionality of access to EURODAC data for law enforcement purposes are not sufficiently demonstrated;
 - the Proposal does not consider sufficiently the implications of the use of EURODAC data for law enforcement purposes with regard to applicable data protection law aspects, nor does it consider the new legal

¹⁰ Opinion of 7 October 2009 on the proposals regarding law enforcement access to EURODAC, OJ C92, 10.4.2010, p. 1.

¹¹ COM(2010)555 final.

¹² See the Explanatory Memorandum p. 3.

¹³ OJ L 286, 1.11.2011, p. 1.

¹⁴ See the Explanatory Memorandum p. 3.

¹⁵ SEC(2008)2981 and SEC(2009)936.

basis for data protection since the entry into force of the Lisbon Treaty, and the ongoing data protection reform.

11. The Opinion is structured as follows:

- Section 2 provides critical remarks on the procedure followed by the Commission;
- Section 3 focuses on the general concerns with regard to the access to EURODAC data for law enforcement purposes;
- Section 4 contains comments on the applicable data protection law in the collection and processing of EURODAC data in a law enforcement perspective;
- Section 5 contains comments on more specific provisions in the proposal relating to EURODAC access for law enforcement purposes;
- Section 6 provides some comments on other provisions of the proposal;
- Section 7 lists the conclusions.

12. The Opinion builds on points of view expressed in earlier opinions relating to the EURODAC review (see point 5), as well as on other opinions in relevant areas. It also takes into account the experiences of the EURODAC Supervision Coordination Group, established to facilitate the supervision foreseen under Article 20 of the current EURODAC Regulation.¹⁶

2. THE PROCEDURE FOLLOWED BY THE COMMISSION

13. It appears that the Commission understands this Proposal as a technical exercise. From the Explanatory Memorandum it can be deduced that it mainly aims at reviving its older proposal, issued in 2009. However, in the last three years important institutional and substantive changes have taken place, for instance as a consequence of the entry into force of the Treaty of Lisbon. Moreover, the fact that in 2010 it was decided to take out provisions on law enforcement access in order to facilitate negotiations in Council and Parliament is a clear indication that the present proposal - including as a main objective law enforcement access - is not of a predominantly technical nature.

14. According to the Commission, the Proposal reinstates the provisions proposed in the lapsed proposal for a Council Decision of 2009. None of the elements introduced are considered new and all of them were assessed in the previous 2008¹⁷ and 2009¹⁸ Impact Assessments. Therefore, the Commission does not attach a new impact assessment, but uses the 2008 and 2009 impact assessments to justify the adoption of the present Proposal. The EDPS disagrees with this approach and still sees the need for a new Impact Assessment.

15. According to the EDPS there are two reasons why the two impact assessments carried out three and four years ago are not sufficient to demonstrate the actual necessity and consistency of the present Proposal.

¹⁶ See on this group: <http://www.edps.europa.eu/EDPSWEB/edps/cache/off/Supervision/Eurodac>.

¹⁷ SEC(2008) 2981, 3.12.2008.

¹⁸ SEC(2009) 936, 10.9.2009.

16. The first reason is that the results of the previous impact assessments were not relevant or not convincing. The 2008 Impact Assessment is irrelevant as it does not assess the introduction of law enforcement access to EURODAC. The 2009 Impact Assessment does evaluate the possibility to use EURODAC data for law enforcement purposes, but this assessment lacked comprehensive analysis¹⁹.
17. In the 2009 Impact Assessment four policy options were considered for regulating access to asylum seekers' data for law enforcement purposes.²⁰ The first option (maintaining the status quo) was ruled out without explanation. Two out of the three other options consisted of analysing the reasons why access to the EURODAC database would be essential in order to identify alleged criminals, as well as to prevent, combat and investigate a crime. However, the analysis failed to at least provide specific examples which justify a real necessity of this access.²¹ Moreover, the analysis failed to take into account that asylum seekers as such are a vulnerable group of people which would require assessing the need for additional protection.
18. The fourth policy option concerned the possibility to create a decentralised network that would allow each Member State to search the national asylum seekers databases of all other Member States in an automated manner. This option suggested that the new network would use only existing instruments such as the mechanism foreseen under Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime ('the Prüm Decision').²² This option was ruled out arguing that it would be complicated and costly.
19. The 2009 Impact Assessment repeatedly stated that existing law enforcement instruments are insufficient and not practical in comparing fingerprints for the investigation of a crime. In particular, the impact assessment pointed out that searching fingerprints through the national automated fingerprint identification systems ('AFIS')²³ of other Member States using the Prüm Decision was not fully reliable because some Member States may not store fingerprints of asylum seekers in their national AFIS unless they were related to crime.²⁴ Moreover, the impact assessment stressed that Council Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities²⁵ could only be used to collect data on asylum seekers if there were factual reasons to believe that the information was actually available in

¹⁹ For further details, see the 2008 and 2009 EDPS Opinions; see also the EDPS Opinion of 15 December 2010 on the establishment of 'EURODAC' for the comparison of fingerprints, OJ C101, p. 14.

²⁰ SEC(2009)936, p. 17-19.

²¹ The examples given in p. 11-12 of the impact assessment are too general and vague. They are not based on real and specific cases, but rather hypothetical situations in which the comparison of asylum seekers' fingerprints might be useful for law enforcement purposes. See also pt. 46-48 of the EDPS Opinion of 2009.

²² OJ L210, 6.8.2008, p. 1-11.

²³ See Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ L210, 06.08.2008, p. 12 ('the Prüm Implementing Decision').

²⁴ SEC(2009)936, p. 9.

²⁵ OJ L 386, 29.12.2006, p. 89.

a particular Member State.²⁶ Finally, the impact assessment noted that mutual legal assistance would require a request to be addressed to all Member States that are believed to have the relevant information, which was time consuming.²⁷

20. The EDPS considers that it should be demonstrated that the combination of these three instruments, and their simultaneous use would not cover all possible situations in which the identity of asylum seekers is needed for law enforcement purposes. Furthermore, in all the examples provided by the 2009 Impact Assessment, the Prüm Decision as well as other instruments were dismissed assuming that they would be insufficient because not all asylum seekers have their fingerprints recorded in other systems. Yet, the impact assessment failed to give consistent and justified arguments for an additional instrument especially focusing on asylum seekers²⁸, whereas comparable instruments are not foreseen and therefore presumably not necessary for other groups of individuals.
21. The second reason why a new impact assessment is needed is that the two previous Impact Assessments are out of date. They were written against a background where the Prüm Decision and the Prüm Implementing Decision were only partially applied in the Member States. The EDPS takes the view that the progress made since 2009 in the application of those decisions should be part of the assessment whether law enforcement access to EURODAC is actually needed.
22. Moreover, the Proposal does not include a Fundamental Rights Impact Assessment in accordance with the Commission's Communication 'Strategy for the Implementation of Fundamental Rights by the European Union' from 2010 which was adopted in light of the entry into force of the Lisbon Treaty which gave the Charter of Fundamental Rights of the European Union primary EU law status.²⁹ The Impact Assessment should examine the impact of the proposal on fundamental rights using the checklist provided in this Communication.³⁰
23. This checklist requires that answers be given to fundamental questions such as whether the impact is beneficial (promotion of fundamental rights) or negative (limitation of fundamental rights) or/and if the limitation of fundamental rights is necessary to achieve an objective of general interest or to protect the rights and freedoms of others, whether the measure is proportionate to the desired aim and preserves the essence of the fundamental rights concerned.
24. On the basis of the foregoing, the EDPS strongly recommends that the Commission provides a new impact assessment in which all four policy options are considered, in which solid evidence and reliable statistics are provided and which includes a fundamental rights assessment. This should all be done with due account to the practical and legal developments that took place since 2009.

²⁶ SEC(2009)936, p. 9.

²⁷ *Ibidem*, p. 9-10.

²⁸ See more in detail points 31-32.

²⁹ COM(2010)573.

³⁰ See also the Commission's Operational Guidance on taking account of Fundamental Rights in Commission Impact Assessments, SEC(2011)567, 06.05.2011.

3. ACCESS TO EURODAC DATA FOR LAW ENFORCEMENT PURPOSES

3.1. Purpose limitation and the risk of function creep

25. When the Regulation establishing EURODAC was adopted and the database became operational in 2003, it did not contemplate police access to its database. The fingerprints are collected and processed for purposes of determining which Member State is responsible for examining an asylum application, for preventing multiple asylum applications within the EU and, more in general, for facilitating the application of the Dublin Regulation.³¹ Specific safeguards are provided to ensure that the EURODAC database is *not* used for other purposes.
26. The Proposal suggests a new legal regime, in which data will still be collected for the purpose of examining asylum applications, but the data could - under certain circumstances - be used for another purpose, i.e. law enforcement outside the context of asylum and migration. This constitutes what is often described as "function creep", namely, a gradual widening of the use of a system or database beyond the purpose for which it was originally intended.
27. In general, the EDPS has strong reservations against this trend. He calls for a cautious approach as to initiatives with a view to possible use of data or systems for other unrelated purposes. It should not be easily accepted that since the data is already collected, it can just as well be used for other purposes which might have a bigger impact on the life of individuals. The assessment as to the necessity and proportionality of the creation of EURODAC would have been completely different if law enforcement access was envisaged from the outset.
28. Moreover, this widening of the use of an existing system is difficult to reconcile with the purpose limitation principle, which is one of the key principles of data protection law.³² Exceptions to the purpose limitation principle are possible, but only under strict conditions. First and foremost, the processing of the data for the other purpose should be necessary and proportionate.
29. The EDPS is not convinced that the necessity and proportionality that could justify an exemption to the purpose limitation principle has been sufficiently demonstrated. A better justification is needed. This is explained in the next sections.

3.2. Necessity of access for law enforcement purposes

30. The Proposal raises questions with regard to the necessity of granting access to EURODAC for law enforcement purposes, since, as indicated, there already exist a number of legal instruments which permit that one Member State

³¹ The Dublin Convention was in 2003 replaced by Council Regulation (EC) No 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national, OJ L 50, 25.2.2003, p. 1 ("Dublin Regulation").

³² The principle can be found in Article 5(b) of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS 108, 28.1.1981 ('Convention 108'), Article 6(1)(b) of Directive 95/46/EC and Article 3 of Framework Decision 2008/977/JHA.

consults fingerprints and other law enforcement data held by another Member State.³³

31. First, Member States can make use of the Prüm Decision, the aim of which is stepping up cross-border cooperation between EU countries in criminal matters, including through networking Member States' national databases³⁴. Under Article 8 of the Prüm Decision, Member States shall ensure availability of reference data from national AFIS established for the prevention and investigation of criminal offences. These reference data shall only include a reference number and dactyloscopic data (i.e 'fingerprint images, images of fingerprint latents, palm prints, palm print latents and templates of such images (coded minutiae), when they are stored and dealt with in an automated database³⁵).
32. Second, other instruments could be applied. Framework Decision 2006/960/JHA could be used for consultations of fingerprints. The measures foreseen in this instrument can be used subject to some conditions such as the need to give factual reasons to believe that the information is available in the other Member State, as well as the need of a prior authorisation by a judicial authority. Moreover, the European Convention on Mutual Assistance in Criminal Matters³⁶ could also be used by judicial authorities of Member States to seek access to criminal and non-criminal fingerprint collection, including asylum seekers. Finally, if a third-country national has applied for a Schengen visa, his or her fingerprints will already be stored in the Visa Information System as visa applicant,³⁷ and if the third-country national is wanted for arrest or an alert has been issued for the purpose of refusing entry, he/she will be in the Schengen Information System.³⁸
33. Therefore, the EDPS suggests that before creating a new instrument providing law enforcement authorities with access to asylum seekers' data, a thorough and more up-to-date evaluation should be carried out, in order to see whether a full implementation of the existing instruments would not be sufficient. The EDPS believes that there are sufficient reasons to assume that the existing instruments may already be effective and sufficient.
34. The state of play of the Prüm Decision and the Prüm Implementing Decision has recently been examined by the Council. The Council noted that some implementation difficulties still existed³⁹ and called in December 2011 on the Member States to finalise their domestic legal and technical implementation procedures in order to fully implement the Prüm Decisions.⁴⁰ Likewise, the Council invited Member States to prepare the assessment of the effectiveness

³³ See on this more in detail also the EDPS Opinion of 7 October 2009.

³⁴ See Article 1 and Recital 13 of the Prüm Decision.

³⁵ Article 2 (i) of the Prüm Implementing Decision.

³⁶ European Convention on Mutual Assistance in Criminal Matters, CETS No 030, 20.04.1959.

³⁷ On the basis of Art 8 of Regulation (C) No 767/2008 of the European Parliament and the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation). OJ L 218/60, 13.08.2008.

³⁸ On the basis of Art. 95 and 96 of the Schengen Convention.

³⁹ Council of Ministers, 18676/11, 20.12.2011.

⁴⁰ Council of Ministers, 17762/11, 5.12.2011.

and efficiency of the Prüm Decisions as an information exchange tool.⁴¹ This is also in line with the Stockholm programme, which points out that '*increased attention needs to be paid in the coming years to the full and effective implementation, enforcement and evaluation of existing instruments*'.⁴²

35. Furthermore, the EDPS is highly interested in this respect in the Commission Communication on the European Information Exchange Model which has been announced for 2012 and which will be based, amongst others, on the results of the Information Mapping Exercise launched by the Commission in 2010.⁴³ The objective of the latter was to analyse the current systems and channels of information to establish whether there is a need for new instruments and measures. As long as the implementation of current instruments is not fully in place and further analysed, the EDPS considers that granting access to EURODAC data for law enforcement purposes would be premature.

3.3. Proportionality of access for law enforcement purposes

36. The EDPS also has doubts as to whether access to EURODAC data by law enforcement authorities would comply with the requirement of proportionality.
37. It should be underlined that asylum seekers constitute a vulnerable group of people and, accordingly, their precarious position has to be taken into account when assessing the necessity and proportionality of the proposed action.⁴⁴ This has not been considered in the Proposal.
38. The net result of the proposed changes to the current system is that an asylum seeker can be identified from a crime scene if a finger print is found, while other individuals cannot, because similar data is not available for all other groups of the society. The Commission has not given any justification for a difference in treatment between asylum seekers and other individuals in this respect. Processing of EURODAC data for law enforcement purposes could therefore lead to a potential discrimination of asylum seekers, which, without justification, cannot be seen as a proportionate measure.
39. It should be underlined that the Court of Justice of the EU and the European Court of Human Rights ('ECtHR') have condemned databases which led to an unjustified unequal treatment of persons.⁴⁵ In *S. and Marper*, the ECtHR pointed at the risks of stigmatisation in this respect.⁴⁶
40. Proportionality also means that, would the necessity of access be demonstrated and the balance of rights and interests be respected, law enforcement access should be subject to strict conditions, as also highlighted in Recital 9 of the Proposal, including the condition that there should be a substantiated suspicion

⁴¹ *Ibidem*.

⁴² Stockholm Programme, point 1.2.2.

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

⁴⁴ See also de EDPS Opinion of 2009, pt. 29.

⁴⁵ See CJEU 16 December 2008, Case C-524/06, *Huber*, [2008] ECR I-09705 and ECtHR 4 December 2008, 30562/04 and 30566/04, *S. and Marper v. United Kingdom*.

⁴⁶ *Ibidem*, para 122.

that the perpetrator of a terrorist or other serious criminal offence has applied for asylum (see also point 56 below).

4. APPLICABLE DATA PROTECTION LAW

41. Currently, Directive 95/46/EC applies to all data processing operations carried out by the Member States within the framework of the EURODAC system. However, granting law enforcement authorities access to EURODAC data, leads to the applicability of the complicated legal framework adopted on the basis of the former third pillar. Processing of personal data by national competent authorities is covered by the provisions of Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters⁴⁷ in so far as it falls within its scope. Processing of personal data by Europol is covered by Council Decision 2009/371/JHA establishing the European Police Office (Europol)⁴⁸.
42. The Proposal contains several provisions specifying certain data protection rights and obligations. According to recital 32 of the Proposal, these are supplements or clarifications of Directive 95/46/EC. However, it remains unclear, how these specifications relate to Framework Decision 2008/977/JHA or to Council Decision 2009/371/JHA.⁴⁹ Article 33, which declares that both decisions are applicable to EURODAC data processing by law enforcement authorities and Europol respectively, does not provide further clarity on this. This leaves open the question whether certain specifications of the Proposal must also be seen as supplementing or clarifying these two decisions.
43. The main example is Article 35 which explicitly prohibits the sharing of personal data with third countries, international organisations or private entities. It is not made clear how this prohibition relates to the possibility of transferring personal data under Framework Decision 2008/977/JHA. In this respect it is relevant to point at the fact that Framework Decision 2006/960/JHA does not contain a prohibition on transferring of data to third countries.⁵⁰ The EDPS takes the view that the transfer of EURODAC data is indeed prohibited, also in case of use of EURODAC data for law enforcement purposes and recommends the legislator to clarify this in Article 35 of the Proposal.
44. Article 35 contains an exception to the prohibition. Member States have the right to transfer personal data to third countries to which the Dublin Regulation applies. According to the EDPS, it should be clarified in the recitals or in a substantive provision that this exception does not apply to transfer to those particular third countries in the context of law enforcement.
45. Another example concerns Article 29 of the Proposal which defines the rights of the data subject. If Article 29 would indeed constitute a supplement to or

⁴⁷ OJ L 350, 30.12.2008, p. 60.

⁴⁸ OJ L 121, 15.5.2009, p. 37.

⁴⁹ Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office ('EUROPOL'), OJ L121/37, 15.5.2009.

⁵⁰ OJ L386, 29.12.2006, p. 89-100.

clarification of Framework Decision 2008/977/JHA or Council Decision 2009/371/JHA, it should pay specific attention to the rights of data subjects in relation to law enforcement access and further use. For instance, on the basis of Article 29(1)(b), the data subject has the right to be informed of the purposes for which his or her data will be processed. However, this provision only mentions that a description of the aims of the Dublin Regulation will be included. If it is decided to grant access to Eurodac for law enforcement purposes, this should be added to the information communicated to the data subject.

46. The need for clarity on how the provisions of the Proposal relate to the Framework Decision 2008/977/JHA as well as Council Decision 2009/371/JHA is even stronger since the proposals for a new data protection framework of 25 January 2012 intend to keep the distinction between a general data protection instrument and a self-standing instrument for law enforcement purposes.⁵¹ Moreover, the proposed new rules do not touch the data protection rules for EU institutions, bodies and agencies as laid down in Regulation (EC) No 45/2001, nor the specific data protection rules such as the ones for Europol and the data protection rules under the Prüm Decision.⁵²

5. SPECIFIC PROVISIONS OF THE PROPOSAL RELATING TO LAW ENFORCEMENT ACCESS

47. As stated above, it should first be demonstrated that law enforcement access to EURODAC as such is necessary and proportionate. The conditions under which such access might be provided are part of a further analysis which should only take place in case the necessity and proportionality are sufficiently demonstrated. The comments made below should then be taken into account.

5.1. Designated and verifying authorities

48. Member States shall determine 'designated authorities' (Art. 5 of the Proposal), as well as 'verifying authorities' (Art. 6 and 7 of the Proposal). Both types of authorities must be responsible for the prevention, detection or investigation of terrorist offences and other serious criminal offences. However, their responsibilities are very different.
49. Under Article 5, the designated authorities shall be authorised to access Eurodac data pursuant to the proposed Regulation. To ensure unequivocally that such

⁵¹ COM(2012)11 final and COM(2012)10 final.

⁵² See the Opinion of the EDPS on the data protection reform package of 7.3.2012, para 26, available at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf. Asylum seekers are also protected by two other pieces of legislation. First, Directive 2011/95/EC (OJ L337, 20.12.2011, p. 9) enshrines the confidentiality principle (Article 37), and protects the collection, processing and circulation of information of unaccompanied minors (Article 31(5)). Second, Council Regulation (EC) No 343/2003 (OJ L50, 25.2.2003, p. 1) establishes that Member States' requests of personal data shall be appropriate, relevant and non excessive for examining the application for asylum (Article 21(1)), the information exchanged may only be used for the purpose of determining the Member State responsible for examining an application for asylum (Article 21(7)), and the asylum seeker has the right to be informed, in accordance with Directive 95/46/EC (Article 21(9)).

access is limited to law enforcement purposes, the EDPS recommends adding in Article 5(1) 'for the purposes referred to in Article 1(2)'.

50. The verifying authority referred to in Article 6 shall verify the lawfulness of the designated authorities' requests of access to Eurodac data. It will examine and validate⁵³ whether the conditions of such access are complied with. The EDPS considers the control mechanism as an essential safeguard to prevent unlawful access. He emphasises that the preferred option, from a fundamental rights perspective, would be the requirement of a prior judicial authorisation which offers appropriate and strong safeguards of independence and impartiality. In the absence of a requirement for a judicial authorisation, it is essential to ensure that the verifying authority must be effectively independent from the designated authority to guarantee a real and proper control, and create a proper system of checks and balances.
51. Therefore, the EDPS recommends as a minimum adding to Article 6 of the Proposal that the verifying authority shall perform its duties and tasks independently and shall not receive instructions as regards the exercise of the verification.
52. The same considerations apply to Article 7 of the proposal regarding access to EURODAC data by Europol.

5.2. Procedure and conditions for comparison and data transmission for law enforcement purposes

53. Under Article 19 of the Proposal a request for access to EURODAC data for law enforcement purposes shall be submitted to a prior check of the verifying authority which shall verify whether the conditions for access are fulfilled. Paragraph 3 provides an exception to this prior check in 'exceptional cases of urgency'. In such cases, ex-post verification shall be carried out without undue delay after the processing of the request. However, no guidance is provided about what qualifies as an exceptional case of urgency. This lack of clarity might lead to diverging interpretations and uncertainty about the scope of the exception. The EDPS recommends adding in Article 19 the criterion of the need to prevent an imminent danger associated with serious criminal or terrorist offences.⁵⁴
54. Moreover, Article 19(3) mentions that the ex-post verification shall be carried out 'without undue delay' after the processing of the request. The EDPS considers that the wording 'without undue delay' is too vague and recommends introducing a concrete time limit.
55. In accordance with Article 20, designated authorities may request comparison of fingerprints with those stored in the EURODAC Central Unit for law enforcement purposes only if comparisons of national fingerprint databases and of the

⁵³ See Article 19(2) of the Proposal.

⁵⁴ One could also think of alternative, more specific formulations, such as those mentioned in recital 26 of the proposal, in particular: "a specific and concrete danger associated with a terrorist or other serious criminal offence, or to specific persons in respect of whom there are serious grounds for believing that the persons will commit or have committed terrorist offences or other serious criminal offences".

Automated Fingerprints Databases of other Member States under Prüm Decision return negative results and where:

- the comparison is necessary for the purpose of the prevention, detection or investigation of terrorist offences or other serious criminal offences (Article 20(1)(a));
- the comparison is necessary in a specific case; systematic comparisons shall not be carried out (Article 20 (1) (b)) and;
- there are reasonable grounds to consider that it will contribute to the prevention, detection or investigation of any of the criminal offences in question (Article 20 (1) (c)).

56. The EDPS welcomes the requirement of a prior consultation of national databases and databases from other Member States through the mechanism set up by Prüm Decision. However, he considers that a prior check of the Visa Information System should also be required. Furthermore, he notes that the list of conditions does not include the requirement referred to in recital 9 of the Proposal and in the Explanatory Memorandum that there should be a substantiated suspicion that the perpetrator of a terrorist or other serious criminal offences has applied for asylum.⁵⁵ In light of what has been said before about the proportionality of law enforcement access to EURODAC data, the EDPS considers this condition as particularly important and strongly recommends the legislator to add it to the list of Article 20 of the Proposal. The reference in recital 9 is not sufficient to ensure compliance with this requirement.

57. The EDPS considers that the use of the wording in Article 20 (1) (c) 'contribute to' is too broad. As mentioned in the Explanatory Memorandum, the comparison of data should 'substantially' contribute to the prevention, detection or investigation of serious crimes in question.⁵⁶ The EDPS suggests amending Article 20 (1) (c) accordingly. In relation to the same provision, the EDPS recommends clarifying what is meant by 'reasonable grounds'.⁵⁷

58. As far as Europol is concerned, neither the explanatory memorandum nor the recitals explain the need for Europol to access EURODAC data. Recital 10 only refers to Europol's 'key role with respect to cooperation between Member States' authorities in the field of cross-border crime investigation in supporting Union-wide crime prevention, analyses and investigation' to justify its access to EURODAC data within the framework of its tasks. The 2009 impact assessment also provides little details on the concrete need of a direct access by Europol⁵⁸. In practice, a national law enforcement authority may (and most probably will) - prior to the sending of fingerprints to Europol - where relevant compare them with

⁵⁵ See especially Recital 9 and p. 7 of the Explanatory Memorandum.

⁵⁶ See p. 7 of the Explanatory Memorandum.

⁵⁷ See also the EDPS Opinion of 2010, point 49.

⁵⁸ The 2009 impact assessment mentions that: '(...) Europol is expected to provide national law enforcement authorities with the necessary tools to exchange information between them, such as exchange of information using the Europol National Units. It follows from the replies of Europol and the Member States to the questionnaire that the exchange of information between those units would benefit if information exchanged in relation to asylum seekers' fingerprints could form part of the information exchanged to them via Europol as part of a concrete file related to cross-border organised crime. Since Europol currently cannot access information on asylum seekers, it cannot ensure that this information be part of its analysis and investigation tasks'.

EURODAC data. The EDPS therefore recommends at least describing in a recital the kind of situations justifying a *direct* access by Europol to the EURODAC Central Unit.

59. Furthermore, the EDPS notes that the stringent criteria for access to EURODAC data by designated authorities do not apply to the access to EURODAC data by Europol. Requests for comparison by Europol are allowed for the purposes of a specific analysis or an analysis of a general nature and of a strategic type. The EDPS questions how the wider facilities for Europol comply with the reasoning provided by the Commission, namely that the access is necessary only for specific cases, under specific circumstances and under strict conditions. In the absence of any particular explanation, the EDPS recommends to align Article 21 with Article 20.

5.3. Comparison with latent fingerprints

60. Currently, by comparing fingerprints of a person with EURODAC data, EU countries can determine whether an asylum applicant or a foreign national found illegally present within an EU country has previously claimed asylum in another EU country or whether an asylum applicant entered the Union territory unlawfully. These situations require the person concerned to be physically present (at least at a given moment) to allow relevant national authorities to take his/her fingerprints with a view to compare them with EURODAC data. The carrying out of comparisons for law enforcement purposes is different in its approach since fingerprints can be taken at a crime scene or in another environment in the absence of the person concerned. This brings new concerns about the potential adverse effects it may have on innocent persons.
61. The EDPS has strong doubts as regards the possibility of searching latent fingerprints in the EURODAC system for law enforcement as considered in recital 12. Any search in EURODAC based on a latent fingerprint, particularly if found in public places, may lead to a high number of possible matches, given the wider range of possible correlations with partial or fragmentary prints. The consequences of a false match may be serious and may lead to the wrongful implication of innocent persons in criminal investigations. The rate of error may be influenced by the quality of the latent fingerprints which are often distorted, adding to the difficulty of matching these fingerprints to those stored in 'EURODAC' which are taken in better conditions.
62. Comparison of fingerprints for law enforcement purposes should in any case be subject to at least the same safeguards already foreseen especially in Article 25 (4) of the Proposal.

5.4. Access and retention of personal data for law enforcement purposes

63. Article 33(4) foresees that 'personal data obtained by a Member State or Europol pursuant to this Regulation from EURODAC shall be erased in national and Europol files after a period of one month, if the data are not required for a specific ongoing criminal investigation by that Member State, or Europol'. The EDPS welcomes the retention period for data retrieved from EURODAC for law enforcement purposes. However, he asks for clarification on the requirement of absence of specific ongoing criminal investigation for deleting the data. Access to EURODAC data should only be allowed when there is an existing ongoing criminal investigation. The EDPS therefore recommends specifying more clearly the framework of this exception or deleting it.

5.5. Nature of data accessed for law enforcement purposes

64. Articles 9 (5), 15 (2) and 17 (4) - which concern access to EURODAC in the context of the application of the Dublin Regulation - specify that when there is a hit (i.e. the existence of a match or matches by comparison between fingerprints data recorded in the Central System and those transmitted by a Member State), the Central System shall transmit for all data sets corresponding to the hit, the data referred in Article 11⁵⁹ along with where appropriate, the mark referred to in Article 18.1. However, the proposal does not contain similar provisions when comparison of fingerprints is requested for law enforcement purposes.

65. The explanatory memorandum (p.7) mentions that 'the comparison with EURODAC for law enforcement purposes will provide a result on a 'hit/no hit' basis - i.e. it will only determine if another Member State holds data on an asylum seeker. The proposal does not provide for new possibilities to process additional information in the follow-up to a 'hit' '. The EDPS wonders how effective it would be for the law enforcement authorities to only get 'hit/no hit' information, i.e. the existence or non existence of a matching. It can reasonably be presumed that the law enforcement authorities would need to know which Member State holds the data on the asylum seeker the fingerprints belong to.

66. This possible need for additional information should be clarified. In the event that the communication of additional information to the 'hit' (e.g. the identification of the Member State holding the data) is considered, the EDPS recalls that pursuant to the principles of necessity and proportionality, the information to be transmitted should be limited to the strict minimum necessary for the purpose for which access has been carried out.

⁵⁹ The proposal refers to the data mentioned in Article 8(a). However Article 8(a) concerns the statistics to be drawn up by the Agency. The EDPS deduces from the EURODAC Regulation, that the relevant provision is actually Article 11 of the proposal which lists the data recorded in the Central System. .

5.6. IT Agency and amendments to Regulation (EU) No 1077/2011

67. The EDPS wonders why the rules on professional secrecy contained in Article 17 (5) (g) of Regulation 1077/2011⁶⁰ have been withdrawn (see Article 38.4 (a) of the proposal) and recommends restoring them.
68. Article 38 (2) of the proposal introduces in Article 12(1)(t) the obligation for the Management Board to request comparisons with EURODAC data by Member States' law enforcement authorities for law enforcement purposes. The proposal does not provide for further explanation about this obligation. The EDPS understands that this is linked to reports and statistics to be provided by the Agency. He therefore recommends specifying in Article 38 (2) of the proposal amending Article 12(1)(t) of Regulation 1077/2011 the precise purposes of such request, as well as the anonymisation by law enforcement authorities of the data prior to their transmission to the Management Board.

6. OTHER SPECIFIC PROVISIONS OF THE PROPOSAL

69. The EDPS has commented on other provisions of the Proposal in his Opinions of 2008 and 2009, mentioned in point 6 above. These comments are not repeated here in full. This section will highlight the main concerns and address new amendments. Where relevant, reference is made to the more in-depth analysis in the previous EDPS Opinions.

6.1. Article 4: operational management

70. The EDPS welcomes the obligation to ensure that at all times the best available technology subject to a cost-benefit analysis is used for the Central System (Article 4(1)). However, he recommends replacing the expression 'Best Available Technologies' by 'Best Available Techniques' which include both the technology used and the way in which the installation is designed, built, maintained and operated. This is important because the concept of 'best available techniques' is broader and covers various aspects contributing to the application of 'data protection by design' which is considered a key principle in the review of the EU data protection legal framework.⁶¹
71. In Article 3(1), a Business Continuity System is foreseen. Furthermore, in Article 4(5), the availability of the platform is fixed to 24hours a day, 7 days a week. This shows the system is considered as critical. However, no details on this "Business Continuity System" or its security and data protection needs are provided.

⁶⁰ Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, OJ L 286, 1.11.2011, p.1.

⁶¹ See Article 23 of the Commission proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012) 11 final and paras 177-182 of the EDPS Opinion of 7 March 2012. See also EDPS Opinion of 15 December 2010 and EDPS Opinion of 18 February 2009.

72. A critical system should be covered by a sound and tested Business Continuity Plan (in case of major disruptions or disasters) which has repercussions on data protection, security and costs. Due care should be taken in defining the availability needs for the system which should take into account maintenance needs and unforeseen downtime. Additionally, requirements in terms of business continuity should be described. When defining business continuity measures, their impact on data protection should be taken into account. Impact may exist due to the existence of duplicates of the data, backup media and additional physical locations and systems at which data could be physically accessed. The EDPS recommends replacing the Business Continuity System by the need for a Business Continuity Plan in Article 3(1) and 4(5) and providing a legal basis for implementing measures containing the modalities of such plan.

6.2. Articles 9, 14 and 17: failure to enrol

73. The EDPS recalls the problem of so-called 'failure to enrol', i.e. the situation in which a person's fingerprints are not usable. It is important to ensure that 'failure to enrol' does not automatically lead to a denial of rights for asylum seekers. The Proposal already envisages partly the failure to enrol in Article 9(1) and 9(2). However, these provisions only envisage the hypothesis of temporary failure to enrol, whereas in some cases this impossibility will be permanent. Therefore, the EDPS recommends adding to Articles 9, 14 and 17 a provision stating that temporary or permanent impossibility to provide usable fingerprints shall not adversely affect the legal situation of the individual. In any case, it can not represent sufficient grounds to refuse to examine or to reject an asylum application.⁶²

6.3. Article 16: data retention

74. The EDPS welcomes the amendment in Article 16 establishing one year as the retention period for data (instead of two years in the current text of the Regulation). This constitutes a good application of the principle of data quality which stipulates that data should not be kept for longer than necessary to accomplish the purpose for which they are processed.⁶³

6.4. Article 29: right of information

75. The EDPS underlines that the information to the data subject should be provided in a way that enables the asylum seeker to fully understand his/her situation as well as the extent of the rights, including the procedural steps he/she can take as follow-up to the administrative decisions taken in his/her case. In that respect, the EDPS welcomes the additions made in Article 29(1), which are in line with the proposal for a general data protection regulation.⁶⁴

⁶² See EDPS Opinion of 15 December 2010 on the establishment of EURODAC for the comparison of fingerprints, Section IV, OJ C 101/14.

⁶³ See Articles 6(1)(e) of Directive 95/46 and 4.1 (e) of Regulation 45/2001. See also Article 4(2) of the Council Framework Decision 2008/977/JHA.

⁶⁴ See EDPS Opinion of 15 December 2010 and Art. 11 and 14 of the proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing

76. The EDPS welcomes the drawing up of a clear and simple common leaflet containing the information to be given to the data subject and the obligation for Member States to provide information in an age-appropriate manner when the person is a minor. This contributes to better harmonization and compliance with the EURODAC Regulation and follows recommendations of the EURODAC Supervision Coordination Group⁶⁵.

6.5. Articles 28 and 36: keeping of records, logging and documentation

77. For purposes of data protection monitoring and data security, the Agency, Member States and Europol shall keep records of all data processing operations within the Central Unit (Article 28) and in relation with requests for comparison with EURODAC (Article 36). However, although the aims are the same (data protection and data security), the wording used in both provisions differs (eg Article 28 mentions the unit *entering in or retrieving the data*, Article 36 refers to the name of the *authority having requested access* for comparison). In order to ensure consistency and allow proper supervision, the EDPS recommends merging both provisions in a single one using the wording of Article 36 which is more precise and complete.

78. Furthermore, Article 36 provides for additional logs/documentation to be kept by Member States and Europol in comparison to the records kept by the Agency. (e.g. the identifying mark of the official who carried out the search and of the official who ordered the search or supply). The EDPS welcomes this obligation which is in line with the principle of accountability and will help ensuring effective supervision.

79. Finally, the EDPS notes that while Article 36 refers to the access by the national supervisory authorities to these logs, there is no mention of a similar access for the EDPS and the Europol's supervisory authority to the records kept by the Agency and Europol respectively. The EDPS recommends amending Article 28 accordingly.

6.6. Articles 31 and 32: supervision model

80. The EDPS welcomes the supervision model laid down in Article 31 and 32 of the Proposal. This model is similar to the model for the Schengen Information System (2nd generation) and the Visa Information System.⁶⁶ It reflects the current practice

of personal data and on the free movement of such data (General Data Protection Regulation) COM (2012) 11 final.

⁶⁵ See Second coordinated inspection on information to data subjects and assessment of the age of young asylum seekers, available at

http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Eurodac/09-06-24_Eurodac_report2_EN.pdf.

⁶⁶ See Art. 41 to 43 of VIS Regulation, Art. 46 of Regulation (EC)No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJL381, 28.12.2006, p. 4 and Art. 62 of Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L265, 7.8.2007, p. 63.

which proved efficient and encouraged close collaboration between the EDPS and national DPAs. Therefore, the EDPS welcomes its formalisation in the Proposal and the fact that while providing for this, the legislator ensured consistency with the systems of supervision of other large-scale IT systems.

81. Recital 34 of the proposal explicitly refers to the monitoring of the lawfulness of data processing activities of Europol by the supervisory authority set up by the Europol Decision. Although the proposal contains specific provisions on supervision when data are processed by Member States or by the Agency (see Articles 31 and 32), the EDPS notes that the text does not contain a similar provision on the supervision of Europol's data processing activities, and recommends addressing this issue.

6.7. Article 34: data security

82. The EDPS has a number of suggestions in respect of Article 34 on data security.
- Article 34(2)(a) should not refer to general critical infrastructure but to the infrastructure required for the system. We suggest replacing "critical" by "*relevant*"
 - In Article 34(2)(f) the term "confidential access modes only" should be clarified.
 - In Article 34(2)(g) the EDPS recommend adding "*make their profiles and any other relevant information the authorities require for the purposes of carrying out supervision available*". The EDPS also recommends adding an explicit reference to Article 28 of Directive 95/46/EC as the requirements about data security provided for in Article 34 apply to transmission of data are performed for facilitating the application of Dublin Regulation, as well as to transmission for law enforcement purposes.
 - In Article 34(2)(i) it should be ensured that the logs, as well as the data they refer to, are protected.
 - In order to ensure the monitoring of the effectiveness of the security measures, the EDPS recommends including in Article 34(2)(k) not only auditing (i.e. providing a picture of the situation at a given point in time), but also near real-time observation of the system using specialised tools.
 - Article 34 should also mention the Business Continuity Plan⁶⁷. As regards security incidents, it should also include:
 - the necessity for Member States to inform the Agency of security incidents they detected on their system;
 - the necessity for the Agency to inform all stakeholders in case of security incidents;
 - the necessity for all parties to collaborate during a security incident;
 - the necessity to inform the national supervisory authorities and the EDPS.

⁶⁷ See paras 72-73 above.

6.8. Article 40: self-audit and annual report

83. Under Article 40(1), the Agency shall submit to the European Parliament and the Council an annual report on the activities of the Central System. The EDPS asks also to be included for the submission of the Agency's annual report.
84. Furthermore, Article 40(2) of the proposal provides for monitoring procedures. The EDPS takes the view that this monitoring should not only concern the aspects of output, cost-effectiveness and quality of services, but also compliance with legal requirements, especially in the field of data protection. Article 40 (2) should be amended accordingly.
85. In order to perform this self-auditing of the lawfulness of processing, the Commission should be enabled to make use of the records kept in accordance with Article 28 of the proposal. Accordingly, Article 28 should provide that these records shall not only be stored for monitoring data protection and ensuring data security, but also for conducting regular self-auditing of EURODAC. The self auditing reports will contribute to the supervisory task of the EDPS and the other supervisory authorities who will be better able to select their priority areas for supervision.

6.9. Article 43: publication of list of authorities

86. The EDPS welcomes the obligation for the Commission to publish the list of authorities having access to EURODAC data (Article 43). With a view to increase transparency and create an effective and practical tool for better supervision of the system (e.g. by the national DPAs), the EDPS recommends adding an obligation on Member States and Europol to constantly update the information they have provided to the Commission. Furthermore the EDPS recommends requiring that the Commission makes this information available to Member States, Europol and to the public 'via a constantly updated electronic publication'.

7. CONCLUSIONS

87. The EDPS notes that over recent years the need of accessing EURODAC data for law enforcement purposes was extensively debated within the Commission, the Council and the European Parliament. He also understands that the availability of a data base with fingerprints can be a useful additional instrument in the combat of crime. However, the EDPS also recalls that this access to EURODAC has a serious impact on the protection of personal data of the persons whose data are stored in the EURODAC system. To be valid, the necessity of such access must be supported by clear and undeniable elements, and the proportionality of the processing must be demonstrated. This is all the more required in case of an intrusion in the rights of individuals constituting a vulnerable group in need of protection, as foreseen in the proposal.
88. Evidence provided until now - also taking into account the specific context described above - is according to the EDPS not sufficient and up to date to demonstrate the necessity and proportionality of granting access to EURODAC

for law enforcement purposes. There are already a number of legal instruments which permit that one Member State consults fingerprints and other law enforcement data held by another Member State. A much better justification, as a precondition for law enforcement access is necessary.

89. In this context the EDPS recommends that the Commission provides a new impact assessment in which all relevant policy options are considered, in which solid evidence and reliable statistics are provided and which includes an assessment in a fundamental rights perspective.

90. The EDPS has identified several additional issues which are:

Applicable data protection law

91. The EDPS stresses the need for clarity on how the provisions of the Proposal specifying certain data protection rights and obligations relate to Council Framework Decision 2008/977/JHA as well as Council Decision 2009/371/JHA (see section 4).

Conditions for law enforcement access

As stated above, it should first be demonstrated that law enforcement access to EURODAC as such is necessary and proportionate. The comments made below should then be taken into account.

92. The EDPS recommends:

- clarifying that the transfer of EURODAC data to third countries is prohibited also in case of use of EURODAC data for law enforcement purposes (see points 43-44);
- adding the law enforcement purposes to the information communicated to the data subject (see point 45);
- ensuring unequivocally that access by designated authorities to EURODAC data is limited to law enforcement purposes (see point 49);
- submitting the access to EURODAC data for law enforcement purposes to a prior judicial authorisation or as a minimum providing that the verifying authority shall perform its duties and tasks independently and shall not receive instructions as regards the exercise of the verification (see points 50-51);
- adding the criterion of the 'need to prevent an imminent danger associated with serious criminal or terrorist offences' as exceptional case justifying the consultation of EURODAC data without prior verification by the verifying authority and introducing a concrete time limit for the ex-post verification (see points 53-54);
- as regards the conditions of access, adding the conditions of (i) a prior consultation of the Visa Information System, (ii) a 'substantiated suspicion that the perpetrator of a terrorist or other serious criminal offences has applied for asylum' and (iii) the 'substantial' contribution for law enforcement purposes and clarifying what is understood by 'reasonable grounds' (see points 56-57);
- describing in a recital the kind of situations justifying a *direct* access by Europol to the EURODAC Central Unit and providing that the strict conditions of access

applying to national designated authorities also apply to Europol (see points 58-59);

- ensuring that comparison of fingerprints for law enforcement purposes shall in any case be subject to at least the same safeguards foreseen for Dublin Regulation purposes (see point 62);
- specifying more clearly the rules on retention or deletion of data (see point 64);
- clarifying which additional information to the 'hit' will be communicated to EUROPOL if applicable (see points 65-66);
- specifying the precise purpose(s) of the request by the Agency's Management Board of the comparisons with EURODAC data by Member State's law enforcement authorities as well as the anonymisation by law enforcement authorities of the data prior to their transmission to the Management Board and restoring the rules on professional secrecyes (see points 67-68);
- providing an access for the EDPS and Europol's supervisory authority to the records kept by the Agency and Europol respectively as well as the obligation to store records also for conducting regular self-auditing of EURODAC (see points 79 and 85);
- clarifying the supervision of Europol's data processing activities (see point 81).

Other provisions

93. The EDPS recommends:

- replacing the Business Continuity System by the need for a Business Continuity Plan and providing a legal basis for implementing measures containing the modalities of such plan (see point 72);
- ensuring that temporary or permanent impossibility to provide usable fingerprints shall not adversely affect the legal situation of the individual and shall in any case represent sufficient grounds to refuse to examine or to reject an asylum application (see point 73);
- ensure consistency between the obligations of the Agency, the Member States and Europol to keep records and documentation of data processing activities (see point 77);
- improving provisions on data security (see point 82);
- including the EDPS for the submission of the Agency's annual report (see point 83);
- adding in Article 43 an obligation on Member States and Europol to constantly update the information they have provided to the Commission and requiring that the Commission makes this information available to Member States, Europol and to the public 'via a constantly updated electronic publication' (see point 86).

Done in Brussels, 5 September 2012



Peter HUSTINX
European Data Protection Supervisor

Anlage 8



BUNDESRECHTSANWALTSKAMMER

Stellungnahme Nr. 47 November 2012

zum Änderungsvorschlag der Europäischen Kommission vom 30.05.2012 zur EURODAC-Verordnung (COM(2012) 254)

Mitglieder des Ausschusses Asyl- und Ausländerrecht

Rechtsanwalt Dr. Stephan Hocks, Vorsitzender
Rechtsanwalt Michael Koch
Rechtsanwältin Ingvild Stadie, Berichterstatterin
Rechtsanwalt Manfred Weidmann

Rechtsanwältin Kristina Wiese, LL.M., Bundesrechtsanwaltskammer

Verteiler: **Europa**

Europäische Kommission
Europäisches Parlament
Rat der Europäischen Union
Ständige Vertretung der Bundesrepublik Deutschland bei der EU
Justizreferenten der Landesvertretungen
Rat der Europäischen Anwaltschaften (CCBE)

Deutschland

Bundesministerium des Innern
Bundesministerium der Justiz
Innenministerien und Senatsverwaltungen für Inneres der Länder
Beauftragte der Bundesregierung für Migration, Flüchtlinge und Integration
Innenausschuss des Deutschen Bundestages
Rechtsausschuss des Deutschen Bundestages
CDU/CSU-Fraktion im Deutschen Bundestag
SPD-Bundestagsfraktion im Deutschen Bundestag
FDP-Bundestagsfraktion im Deutschen Bundestag
Fraktion DIE LINKE im Deutschen Bundestag
Fraktion Bündnis 90/Die Grünen im Deutschen Bundestag
Arbeitsgruppen Recht der im Bundestag vertretenen Parteien
Rechtsanwaltskammern
Arbeitsgruppe Migration und Integration der SPD-Bundestagsfraktion
UNHCR Deutschland

Bundesrechtsanwaltskammer

The German Federal Bar
Barreau Fédéral Allemand
www.brak.de

Büro Berlin – Hans Litten Haus

Littenstraße 9
10179 Berlin
Deutschland
Tel. +49.30.28 49 39 -0
Fax +49.30.28 49 39 -11
Mail zentrale@brak.de

Büro Brüssel

Avenue des Nerviens 85/9
1040 Brüssel
Belgien
Tel. +32.2.743 86 46
Fax +32.2.743 86 56
Mail brak.bxl@brak.eu

Katholisches Büro in Berlin
Bevollmächtigter des Rates der EKD bei der Bundesrepublik Deutschland
Diakonisches Werk der EKD
Deutscher Caritasverband
Deutsches Rotes Kreuz
Deutscher Anwaltverein
Deutscher Richterbund
Bund Deutscher Verwaltungsrichter
PRO ASYL, Bundesweite Arbeitsgruppe für Flüchtlinge e. V.
Deutscher Gewerkschaftsbund (Bundesvorstand)
Neue Richtervereinigung (NRV)
Präsidentin des Bundesverwaltungsgerichts
Neue Zeitschrift für Verwaltungsrecht (NVwZ)
ZAR
Asylmagazin
ANA-ZAR
Informationsbrief Ausländerrecht

Die Bundesrechtsanwaltskammer ist die Dachorganisation der anwaltlichen Selbstverwaltung. Sie vertritt die Interessen der 28 Rechtsanwaltskammern und damit der gesamten Anwaltschaft der Bundesrepublik Deutschland mit zurzeit rund 159.000 Rechtsanwältinnen und Rechtsanwälten gegenüber Behörden, Gerichten und Organisationen - auf nationaler, europäischer und internationaler Ebene.

Stellungnahme

Die Bundesrechtsanwaltskammer bedankt sich für die Gelegenheit zur Stellungnahme und möchte folgende Überlegungen zu bedenken geben:

I.

Sinn und Zweck der EURODAC-Verordnung ist die effektive Anwendung der Verordnung (EG) Nr. 343/2003 des Rates vom 18. Februar 2003 zur Festlegung der Kriterien und Verfahren zur Bestimmung des Unterzeichnerstaates, der für die Prüfung eines von einem Drittstaatsangehörigen in einem Unterzeichnerstaat gestellten Asylantrags zuständig ist (Dublin II-Verordnung).

EURODAC liefert den Asylbehörden bei der Prüfung ihrer Zuständigkeit Anhaltspunkte dafür, ob der betreffende Antragsteller bereits in einem anderen Mitgliedstaat einen Asylantrag gestellt und/oder wann und wo er illegal die Außengrenzen des Geltungsbereichs der Verordnung überschritten hat.

Die Ausdehnung des Anwendungsbereichs auf die Nutzung der erhobenen Daten zum Zweck der Verhütung, Aufdeckung und Untersuchung terroristischer und sonstiger schwerer Straftaten widerspricht dem Kerngedanken dieser Verordnung (Erwägungsgrund (1) bis (3)) und steht mit der Vergemeinschaftung der Asylpolitik und der Schaffung eines gemeinsamen europäischen Asylsystems in keinem Zusammenhang. Die EURODAC-VO ist ein Regelwerk in einem Verbund weiterer Verordnungen und Richtlinien, die miteinander korrelieren und der Harmonisierung und Vergemeinschaftung des Asylsystems dienen. Die geplanten Änderungen lösen die EURODAC-Verordnung aus diesem strukturellen Zusammenhang und laufen damit der Zielsetzung eines gemeinsamen europäischen Asylsystems insgesamt zuwider.

Die Anlegung einer Datenbank und Verwendung personenbezogener Daten zum Zweck der Verhütung, Aufdeckung und Untersuchung terroristischer und sonstiger schwerer Straftaten bedürfte einer vom Asylsystem losgelösten Gesetzesgrundlage, die in einer gemeinsamen Strafverfolgungspolitik der Europäischen Gemeinschaft ihre Grundlage finden sollte und für alle Gesellschaftsgruppen gleichermaßen gelten muss.

Es kann nicht sein, dass nur die Daten einer bestimmten Personengruppe, deren Daten nun einmal bereits gesammelt worden sind, für einen solchen weit reichenden Zweck verwendet werden dürfen.

II.

Die Erhebung der Daten im Asylprozess und deren sachfremde Verwendung dürfte im Hinblick auf Art. 2 Abs. 1 GG bzw. Art. 7 und Art. 8 Europäischen Grundrechte Charta (GRC) problematisch sein und ebenso gegen Art. 3 Abs. 1 GG bzw. Art. 20 GRC verstoßen.

1.

Es ist nicht ersichtlich, weshalb Daten von Asylsuchenden umfassend in allen Mitgliedstaaten für die Verbrechensbekämpfung zur Verfügung stehen dürfen, wohingegen es derlei Datenbestände für andere gesellschaftliche Gruppen nicht gibt. Ein Nachweis, der diese Ungleichbehandlung in der Verbrechensbekämpfung rechtfertigt, ist nicht erbracht.

Die vorzeitige Löschung der Daten aus EURODAC, wenn vor Ablauf der 10-Jahresfrist die Staatsangehörigkeit eines Mitgliedstaats erworben wird (Art. 13 VO-Änderung), war bei ursprünglicher Zwecksetzung der EURODAC-VO – Durchsetzung eines gemeinsamen Asylsystems - folgerichtig. Bei der nun angestrebten Änderung – der Nutzung der Daten für die Strafverfolgung – ist eine solche Löschung der Daten bei Wechsel der Staatsangehörigkeit unter dem Gesichtspunkt des Gleichheitsgrundsatzes wohl nicht mehr zu rechtfertigen, sondern ein weiteres Indiz für die Ungleichbehandlung und Stigmatisierung der Asylsuchenden.

2.

Das Haager Programm sieht zwar die Stärkung der Zusammenarbeit der Strafverfolgungsbehörden der Mitgliedstaaten, insbesondere durch besseren Informationsaustausch, vor. Diese Zielsetzung ist aber mit der Freigabe der EURODAC-Daten nicht im Einklang, denn bei den vorliegenden Änderungen geht es nicht um die Verbesserung der Zusammenarbeit der Strafverfolgungsbehörden, sondern um die Nutzung von fachfremd erhobener Daten einer einzigen Personengruppe durch eine für strafrechtliche Ermittlungen unzuständige Asylbehörde und deren Bedienstete.

3.

Der rechtsstaatliche Verhältnismäßigkeitsgrundsatz bzw. Art. 52 GRC ist bei einem Eingriff in das Grundrecht der Privatsphäre und des Datenschutzes zu beachten, insbesondere wenn es sich um Eingriffe in die Rechte von besonders Schutzbedürftigen, wie hier von Personen, die vor Verfolgung fliehen und grundsätzlich keiner Straftat verdächtigt werden, handelt. Die Wahrung des Verhältnismäßigkeitsgrundsatzes bedeutet, dass die Maßnahme wirksam sein muss und das Ziel nicht mit den schon bestehenden Instrumenten erreicht werden kann. Dies ist sorgfältig zu prüfen, bevor zusätzliche Maßnahmen eingeführt werden. Überdies geht es um Daten, die für Zwecke erhoben wurden, die nicht im Zusammenhang mit der Bekämpfung von Kriminalität stehen. Die Fingerabdruckinformationen werden für andere Zwecke erhoben. Es besteht die Gefahr der

Stigmatisierung. Asylbewerber, die keines Verbrechens überführt worden sind und bei denen die Unschuldsvermutung gilt, werden wie Verdächtige behandelt.

III.

Die vorgesehene künftige bloße Markierung der Daten von Personen, die internationalen Schutz erhalten haben (Art. 18 des Änderungsvorschlags), wird der besonderen Schutzbedürftigkeit dieser Personen nicht gerecht. Daten dieser Sondergruppe müssen mit besonderer Sorgfalt verwahrt und geschützt werden. Denn bei diesen Personen ist bereits festgestellt, dass ihnen in ihrem Herkunftsland eine akute, ernsthafte Gefahr für Leib, Leben und Gesundheit droht. Insofern sollten deren Daten auch - wie bislang - gesperrt werden, so dass ein Zugriff – und damit die Gefahr eines Missbrauchs der Daten - wirksam vermieden werden kann.

Die Markierung der Daten statt deren bisherige Sperrung soll den Zweck erfüllen, dass für die Mitgliedstaaten erkennbar ist, wenn eine Person, die bereits in einem anderen Mitgliedstaat internationalen Schutz erhalten hat, erneut versucht, einen Asylantrag zu stellen. Diesem Zweck ist jedoch bereits durch die Informationsaustauschmöglichkeit des Art. 21 Dublin II-Verordnung ausreichend Rechnung getragen.

IV.

Der Datenmissbrauch durch Weitergabe dieser empfindlichen Daten an Drittstaaten, die die Bestimmungen der Genfer Konventionen nicht achten, ist durch Art. 35 des Änderungsvorschlags nicht ausreichend gesichert.

Denn über die Daten, die einmal über die Neuregelungen der EURODAC-Verordnung an strafrechtliche Ermittlungsbehörden eines Mitgliedstaats gelangt sind, besteht dann keine Kontrolle mehr. Die Änderung der EURODAC-Verordnung regelt weder das Verbot der Weitergabe der Daten auch durch die Ermittlungsbehörden und Europol, noch ist gewährleistet, dass die Daten bei diesen so verwahrt und kennzeichnet werden, dass sie auch noch nach Jahren als EURODAC-Daten erkennbar sind und damit einem besonderen Schutz unterliegen. Es ist somit nicht auszuschließen, dass diese sensiblen Daten über die Strafverfolgungsbehörden im Rahmen von internationalen Abkommen an Drittstaaten und Verfolgerstaaten weitergegeben werden.

V.

Art. 19 Abs. 3 VO-Änderung, der die Ausnahme einer vorherigen Prüfung der Voraussetzungen für die Datenweitergabe in „dringenden Fällen“ regelt, ist zu unbestimmt gefasst. Es bedürfte in jedem Fall einer weiteren Konkretisierung des Begriffs „dringende Fälle“. Im Hinblick darauf, dass die Datennutzung nur für die Bekämpfung des Terrorismus und schwerer Straftaten möglich ist, dürfte wohl überwiegend ein „dringender Fall“ gegeben sein, so dass die Datenweitergabe in einer Vielzahl von Fällen ohne vorherige Prüfung der Voraussetzung möglich sein wird und die Ausnahme somit zur Regel wird.

Dies entspricht nicht den Vorgaben des Art. 8 Abs. 1 i. V. m. Art. 52 Abs. 1 der GRC. Hiernach muss jede Einschränkung des Rechts auf den Schutz personenbezogener Daten gesetzlich vorgesehen und so bestimmt und präzise sein, dass der Einzelne sein Verhalten danach richten kann, vor Willkür der Behörden geschützt ist und der Handlungsspielraum, den die Behörden haben und die Art und Weise, wie dieser genutzt wird, muss klar festgelegten Regeln folgen. Einschränkungen dieses Rechts dürfen nur unter Wahrung des Verhältnismäßigkeitsgrundsatzes erfolgen. Die in der Ordnungsänderung vorgesehenen Schutzklauseln für den Einzelnen werden aber dann ausgehöhlt, wenn die von den

Voraussetzungen für die Beantragung eines Abgleichs mit den EURODAC-Daten zugelassenen Ausnahmen nicht eindeutig definiert sind.

Durch die nachträgliche Löschung zu Unrecht weitergegebener Daten wird der vorhergehende Grundrechtseingriff nicht geheilt.

Fraglich ist ferner, wie die ordnungsgemäße Löschung ungerechtfertigt erhaltener Daten von der Prüfstelle in den Mitgliedstaaten durchgesetzt wird.

VI.

Probleme dürfte es ferner mit dem Schutz der Daten von Kindern ab dem 14. Lebensjahr geben, die ebenfalls im EURODAC-Datensystem gespeichert werden. Minderjährige in diesem Alter können nicht in allen Mitgliedstaaten belangt werden. Die Ausführungen in Erwägungsgrund (27) gehen diesbezüglich nicht weit genug. Es muss sichergestellt sein, dass Daten der betroffenen Minderjährigen nicht zu Strafverfolgungszwecken an diese Mitgliedstaaten weitergegeben werden. Dem Kinderschutz ist diesbezüglich Vorrang einzuräumen. Es ist auch nicht zu erkennen, weshalb gerade der antragstellende Staat ein Interesse haben sollte, die Minderjährigkeit nachzuweisen (Erwägungsgrund (27)).

Problematisch ist in diesem Zusammenhang auch der Altersnachweis. Der Großteil der um internationalen Schutz Suchenden ist nicht im Besitz von Identitätspapieren. Aus diesem Grund findet oft eine Altersfestsetzung von Behördenseite statt, die oft über dem von den Schutzsuchenden angegebenen Alter liegt.

VII.

Art. 21 VO-Änderung: Es ist nicht ersichtlich, weshalb die strengen Kriterien für den Zugriff der benannten Behörden auf EURODAC nicht für den Zugriff von Europol gelten (vgl. Art. 20 und 21 VO-Änderung). Gründe hierfür werden nicht benannt.

VIII.

Die Tatsache, dass bei Personen, deren Fingerkuppen beschädigt sind - aus welchen Gründen auch immer - und eine Erfassung der Fingerabdruckdaten daher nicht möglich ist, darf nicht zu Beeinträchtigungen bei der Bearbeitung des Asylantrages führen (vgl. Art. 9 VO-Änderung geht nur von vorübergehenden Schwierigkeiten aus, nicht geregelt ist der Dauerzustand).

IX.

Art. 29 Abs. 1 VO-Änderung: durch die bloße mündliche Unterrichtung der von der Datenverarbeitung betroffenen Personen – auch wenn diese in der entsprechenden Landessprache erfolgt - ist das Recht auf Schutz der personenbezogenen Daten sowie der wirksame Rechtsschutz hiergegen nicht hinreichend gewährleistet. Es ist nicht davon auszugehen, dass alle Schutzsuchenden, die oft wenig oder gar keine Schulbildung besitzen, ihre Rechte und die Tragweite der Datenverarbeitung verstehen. Ohne entsprechende schriftliche Mitteilung ist es diesen Personen aber auch nicht möglich, unterstützende (anwaltliche) Beratung einzuholen.

Es bestehen erhebliche Bedenken, dass die Änderungen der EUODAC-Verordnung einer verfassungsgerichtlichen Überprüfung standhalten und der besonderen Schutzbedürftigkeit dieser sensiblen Personengruppe gerecht werden.

Anlage 9

Meijers Committee

Standing committee of experts on international immigration, refugee and criminal law

Secretariat

p.o. box 201, 3500 AE Utrecht/The Netherlands
phone 0031 30 297 43 28
fax 0031 30 296 00 50
e-mail cie.meijers@forum.nl
<http://www.commissie-meijers.nl>

To (by email) European Parliament
Civil Liberties, Justice and Home Affairs Committee
Rue Wiertz
BE-1047 Bruxelles

Reference CM1216
Regarding Note Meijers Committee on the EUODAC proposal (COM(2012) 254)
Date 10 October 2012

Dear Members of the Civil Liberties, Justice and Home Affairs Committee,

Please find attached a note by the Meijers Committee on the amended proposal for a Regulation on the establishment of Eurodac. The new draft provides for the possibility to request comparison with Eurodac data by Member States law enforcement authorities and Europol. This was also proposed in 2009 but lapsed as a consequence of the Treaty of Lisbon.

The Meijers Committee strongly opposes this access to law enforcement authorities, because it breaches fundamental rights of asylum seekers, including their right to privacy and data protection, the right to asylum and protection against torture and inhuman treatment. Furthermore, the extended use of Eurodac data involves the risk of stigmatisation of a particular group of persons, namely asylum seekers (see section 1 of the accompanying note).

For this reason, the Meijers Committee advises the members of the European Parliament to vote against this proposal.

If the European Parliament decides to accept access for law enforcement authorities and Europol to Eurodac data, the Meijers Committee urges to take into account the comments in the accompanying note (see section 2).

We hope you will find these comments useful. Should any questions arise, the Meijers Committee is prepared to provide you with further information on this subject.

Yours sincerely,



Prof. dr. C.A. Groenendijk
Chairman

Note on the proposal for a Regulation on the establishment of Eurodac (COM(2012)254)

1. Access by law enforcement authorities and Europol: a breach of fundamental rights.

The Meijers Committee emphasizes that the proposal by which law enforcement authorities and Europol are permitted access to the information in Eurodac violates fundamental rights of the asylum seekers, including the right to privacy and data protection, the right to asylum and protection against torture and inhuman treatment, and will lead to stigmatisation of this particular group. In earlier comments, the Meijers Committee already expressed its concerns with regard to this access.¹ The Committee is of the opinion that the proposal violates:

- **the right to data protection (Article 8 Charter of Fundamental Rights).**

The proposed use of Eurodac for law enforcement authorities is originally based on the Regulation (EC) No2725 concerning the establishment of Eurodac for the comparison of fingerprints for the effective application of the Dublin Convention.² The proposal to give law enforcement authorities and Europol access to Eurodac will change this database into a criminal law investigation tool which is contrary to the limited purpose of this system, namely the assessment of the state which is responsible for an asylum application under the Dublin Regulation. There would not seem to be a justified exception to the breach of the purpose limitation principle, as the necessity and proportionality of access for law enforcement authorities and Europol have not been demonstrated.

In this context, the Meijers Committee refers to preliminary questions which have been recently submitted by national courts in Germany and the Netherlands to the Court of Justice of the European Union (CJEU) on the implementation of the Regulation(EC) No 444/2009 on standards for security features and biometrics in passports and travel documents issued by Member States.³ In these questions, the national courts voice their concerns about the proportionality of the central storage of biometric data in passports and travel documents and their use for other purposes and about the relationship of the Regulation with the rights to privacy and protection of personal data safeguarded under Article 7 and 8 of the Charter of Fundamental Rights and Article 8 ECHR. If the CJEU comes to the conclusion that this use is disproportional, access for law enforcement authorities and Europol to Eurodac must most likely also be considered disproportional, considering that these fingerprints are used for another purpose than for which they were stored and that it concerns the systematical storage of fingerprint data of a particularly vulnerable group, asylum seekers.⁴

- **the right to privacy (Article 8 ECHR)**

The underlying proposal gives law enforcement authorities of 31 states and Europol access to a Europe-wide database with the fingerprints of asylum seekers, including minors, who are not suspected of any crime. The presumption that access contributes to the prevention, detection or investigation of the criminal offences is not sufficient to limit the right to privacy and data protection of asylum seekers; a fair balance has to be struck between the competing public interests and the protection of rights of a highly vulnerable group.⁵ The Meijers Committee is of the opinion that the European Commission has not given convincing reasons why such a serious infringement is justified. Further, there are insufficient guarantees that data are no longer stored than necessary and that the national authorities of the country of origin of the person who is granted international protection are prevented from accessing the data. Aside from the provision in Article 29, according to which the asylum seeker will be informed on the recipients of his data, he has no means available to challenge the transfer of his fingerprints, initially provided on an obligatory basis for administrative purposes only, to the law enforcement authorities and Europol. The Meijers Committee

¹ See CM0712, CM0714 and CM0910, available on our website www.commissie-meijers.nl.

² OJ L 50/1, 25.2.2003. Meanwhile the Dublin Convention has been replaced by the Council Regulation 343/2003 (Dublin II) of 18 February. This Regulation is now under consideration (COM(2008) 820).

³ Dutch Council of State, case 201205423/1/A3, 28 September 2012 and Verwaltungsgericht Gelsenkirchen, C-291/12 *Schwarz v. Stadt Bochum*, 15 May 2012.

⁴ In the case of *M.S.S. v. Belgium and Greece*, it was explicitly underlined that asylum seekers are a highly vulnerable group (application no. 30696/09, 21 Januari 2011).

⁵ *S. and Marper v. the United Kingdom*, applications nos. 30562/04 and 30566/04, 4 December 2008.

therefore agrees with the opinion of the EDPS that “to intrude upon the privacy of individuals and risk stigmatising them requires strong justification and the Commission has simply not provided sufficient reason why asylum seekers should be singled out for such treatment”.⁶

- **the right to asylum and right to protection against torture and inhuman treatment (Article 18 Charter of Fundamental Rights and Article 3 ECHR)**

Extension of the use of data in Eurodac to other authorities not dealing with asylum applications implies the risk that the information will be shared with foreign authorities as well. This risk is enhanced because the information will, through the extended use of Eurodac data, become available to a far wider range of authorities in Member States who have no experience with the specific risks of asylum related information. The mere knowledge that his or her data may be used by law enforcement authorities in the EU and possibly later become accessible to the authorities of the state of origin may already sort detrimental effects on the asylum seeker’s right to request asylum or subsidiary protection. In this context the Meijers Committee is also worried about a comment in the recently published note of the Council explaining the need for Europol to be able to request the comparison with Eurodac.⁷ According to this note, Europol may use information from third countries, received on the basis of operational agreements according to Article 23 of the Europol Decision (2009/371/JHA), as an indication of ‘proving reasonable grounds to consider that a comparison with Eurodac data will lead to the identification of a victim or suspect of serious crime in a specific case’. This use of information by Europol involves the risk that asylum seekers will be labeled as terrorists or suspected criminals by their countries of origin, just to prevent them to obtain asylum in Europe.

- **prohibition of discrimination (Article 14 ECHR)**

The use of fingerprints of asylum seekers for law enforcement purposes and in the fight against terrorism will lead to stigmatisation and discrimination of this group of individuals. This risk of stigmatisation is recognized by the European Court of Human Rights in *S. & Marper v. the UK*.⁸ The fact that by this extended use of their information, asylum seekers are de facto considered as suspected persons, may influence the way this group of persons will be treated in society as well.⁹ It would have the highly questionable effect of increasing the probability of prosecution of a segment of the population on the mere basis that its members have made use of their fundamental right to seek asylum. A divide will be erected as regards the presumption of innocence between asylum seekers and other parts of the population, which amounts to unequal treatment on the basis of nationality for which no reasonable justification has been advanced.

2. Comments on the new Eurodac proposal

As has been stated above, the Meijers Committee is of the opinion that the comparison and data transmission of fingerprints in Eurodac for law enforcement purposes breaches fundamental rights. The Committee therefore strongly rejects this possibility and advises the LIBE-members to reject the proposal of the European Commission.

⁶ Press release Opinion of the European Data Protection Supervisor on the amended proposal for a Regulation on the establishment of EURODAC, 5 September 2012. The recently published note explaining the need for Europol to be able to request the comparison with Eurodac changes nothing to this conclusion, as it is only explained why access contributes to the prevention, detection or investigation of criminal offences but fails to explain why this outweighs the interest of the individuals registered in Eurodac (Note explaining the need for Europol to be able to request the comparison with Eurodac data for the purposes of preventing, detecting and investigating terrorist offences and other serious criminal offences, Council doc. 14081/12, 21 September 2012.)

⁷ Note explaining the need for Europol to be able to request the comparison with Eurodac data for the purposes of preventing, detecting and investigating terrorist offences and other serious criminal offences, Council doc. 14081/12, 21 September 2012.

⁸ *S. and Marper v. the United Kingdom*, applications nos. 30562/04 and 30566/04, 4 December 2008, also judgment of the Bundesverfassungsgericht, 4 April 2006, 1 BvR 518/02 published on 23 May 2006.

⁹ In this context, the Meijers Committee also refers to the case *Huber v. Germany* by the CJEU which has been discussed in an earlier note by the Meijers Committee, see CM0910 accessible through www.commissie-meijers.nl.

If the LIBE Committee decides not to reject the proposal, the Meijers Committee advises to take into account the following comments and suggestions.

1. Designated authorities (Article 5)

According to Article 5(1) Member States shall designate the authorities which are authorised to access Eurodac data pursuant to this Regulation. Designated authorities shall be authorities of the Member States which are responsible for the prevention, detection or investigation of terrorist offences and other serious criminal offences. The Meijers Committee finds that this definition is too wide as it allows Member States to appoint several different national authorities having access to the data in Eurodac. In this context, the Meijers Committee recalls the standard case law of the European Court on Human Rights stating that the transmission of data to and their use by other authorities, which enlarges the group of persons with knowledge of the personal data intercepted and can lead to investigations being instituted against the persons concerned, constitutes a further separate interference with the applicants rights' under Article 8.¹⁰ The possibility in Article 5 (1) for Member States to designate a large number of "designated authorities" authorised to have access to the Eurodac data will hamper the effective control on the use and further storage of the fingerprints of asylum seekers. The obligation of Member States to notify the Commission of the lists of the designated authorities is insufficient in this respect (Article 43 of the proposal).

The wide definition of "designated authorities" leads to a further interference of Article 8 ECHR. The Meijers Committee strongly advises to limit the possibility for Member States to designate law enforcement authorities who may access Eurodac, by developing limitative lists in the Regulation itself, or in an annex, of the national authorities authorized to have access to Eurodac data.

2. Data storage and advance data erasure of applicants for international protection (Article 12, Article 13)

Data of applicants for international protection shall be stored for ten years from the date on which the fingerprints were taken. When a person acquires citizenship before the ten-year period has lapsed, his data shall be erased from the Central System "as soon as the Member State of origin becomes aware that the person has acquired such citizenship". The Meijers Committee finds that this provision gives too much discretion to the Member State. It is necessary that Member States keep track of changes in the situation of the persons registered in Eurodac as there is an implementation deficit in the advance deletion of data. In the Eurodac Activity report the EDPS mentions "that inspections were carried out and results made clear that some Member States still lacked appropriate procedures for dealing with advance deletion".¹¹ This indicates that data remain to be stored in Eurodac while they should have been erased. The Meijers Committee is particularly concerned about this in the context of access by law enforcement authorities and Europol: if data are stored longer than necessary it gives them even wider access to data of persons who are not suspected of any crime. With regard to this problematic issue and in line with the recommendations of the European Data Protection Supervisor, the Meijers Committee proposes the following:

- **efficient procedures for automatic advance deletion of data by Member States should be established;**
- **if law enforcement agencies and Europol should gain access to Eurodac data, the Regulation should include strict and short time limits for the storage of the data on asylum seekers.**

3. Comparison of fingerprint data (Article 17)

From an inspection report by the EDPS of the EU's Eurodac Central Unit it appears that comparisons of fingerprint data of a third country national or a stateless person found illegally staying within its territory with the fingerprints registered in Eurodac are not deleted once these comparisons have been transmitted to

¹⁰ ECHR *Leander v. Sweden* appl.no. 9248/81, 26 March 1987 and ECHR *Weber and Saravia v. Germany*, appl.no.54934/00, 28 October 1994.

¹¹ European Data Protection Supervisor "Coordinated Supervision of Eurodac Activity Report 2010-2011", p. 6, 4 July 2012.

relevant Member States, contrary to the obligation under Article 11(5) of the current Eurodac regulation.¹² This is a clear violation of the obligation to ensure that data are not stored longer than is necessary for the purposes for which data were collected. The Meijers Committee therefore questions the decision to delete the obligation for the Central Unit to erase the results of the comparison in the new Article 17. Especially now that access for law enforcement authorities and Europol is allowed and data become available for a large group of authorities it should be guaranteed that the Central Unit will delete the results of the comparison immediately after it has been transmitted. The Meijers Committee urges that comparisons as regulated in Article 17 must be deleted immediately after these data have been transmitted to the Member States. Therefore, this obligation that is provided in Article 11(5) of the current Eurodac Regulation (2725/2000/EC) should be maintained:

Once the results of the comparison have been transmitted to the Member State of origin, the Central Unit shall forthwith:

- (a) erase the fingerprint data and other data transmitted to it under paragraph 1; and**
- (b) destroy the media used by the Member State of origin for transmitting the data to the Central Unit, unless the Member State of origin has requested their return.**

4. Marking of data (Article 18)

Article 12 of the current Eurodac Regulation (2725/2000/EC) regulates that data relating to an asylum applicant are blocked in the central database if that person is recognised and admitted as a refugee in a Member State. Hits concerning these persons are not transmitted and the Central Unit should send a negative result to the Member State. Although the data remain in the Central Database, these data are not accessible by the Member States as long as the person is recognized as a refugee. If the refugee lost his status as a refugee, his data would be unblocked. Under the new proposal, data of persons who are granted international protection are marked: “this mark shall be stored in the Central System in accordance with Article 12 for the purpose of transmission under Article 9(5)”. This means that data are no longer blocked, but can be transmitted to the Member States, even if the applicant has been granted international protection. The Committee wonders whether “for the purposes of transmission under Article 9(5) (application for international protection)” means that data shall not be transmitted when these data are requested by law enforcement authorities and Europol. The Meijers Committee suggests the following amendment, in the line of Article 12 of the current Eurodac Regulation:

Data relating to an applicant for asylum which have been recorded pursuant to Article 11 shall be blocked in the central database if that person is recognised and granted international protection in a Member State. Such blocking shall be carried out by the Central Unit on the instructions of the Member States of origin.

Hits concerning persons who have been recognised and granted international protection in a Member State shall not be transmitted. The Central Unit shall return a negative result to the requesting Member State.

Furthermore, the question whether “for the purpose of transmission under Article 9(5)” in the new Article 18(1) means that data shall not be transmitted when these data are requested by law enforcement authorities and Europol should be clarified.

5. Conditions for access to EURODAC data by designated authorities and Europol (Article 19 to Article 22).

The Meijers Committee emphasizes the vulnerable position of asylum seekers and the obligation of Member States to protect the right to asylum under Article 18 of the EU Charter on Fundamental Rights and their right of non-refoulement under the Geneva Convention and Article 3 ECHR. It is therefore even more important that the conditions for access to Eurodac by designated authorities and Europol are strictly and clearly defined. For this reason, the Meijers Committee is worried about the possibility regulated in Article 19(3) that “in exceptional cases of urgency, the verifying authority may transmit the fingerprint data immediately to the requesting authority, and only verify ex-post whether all the conditions of Article 20 or Article 21 are fulfilled.

¹² EDPS Eurodac Central Unit Inspection report June 2012, Council doc. 11660/12.

“Exceptional cases of urgency” is too vague and should be clarified. The Meijers Committee supports the suggestion by the EDPS to add the criterion ‘of the need to prevent an imminent danger associated with serious criminal or terrorist offences’.

The Meijers Committee has noticed that in Article 20 (1) (c) the word “substantially” is no longer mentioned, which makes the condition for access broader and less clear than in the Eurodac proposal of 2009. In the Council Decision concerning access for consultation of the Visa Information Systems (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences access is only possible when “there are reasonable grounds to consider that consultation of VIS data will *substantially* contribute to the prevention, detection or investigation of any of the criminal offences in question”. Eurodac contains information of vulnerable persons and conditions to access this data should be at least as strict as access to VIS. The Meijers Committee suggests to amend Article 20 (1)(c) as follows:

There are reasonable grounds to consider that such comparisons with Eurodac data will *substantially* contribute to the prevention, detection or investigation of any of the criminal offences in question.

The Meijers Committee is concerned that the conditions for access to Eurodac data by Europol are broader than the conditions for access by designated authorities. The Committee welcomes the suggestions by the Presidency to align the conditions for access by Europol with the conditions for access by designated law enforcement agencies. This was also suggested by the EDPS in its opinion.¹³

6. Role national supervisory authority (Article 29 to Article 32)

The Meijers Committee supports the explicit role given to the European Data Protection Supervisor and the National Supervisory Authorities in the supervision of data processing activities concerning Eurodac. The access for law enforcement authorities to the sensitive data of asylum seekers in Eurodac must be strictly supervised. However, the Committee is worried that the supervision of access for law enforcement authorities and Europol means a further extending of their tasks. With the adoption of various data processing instruments in the last decennium there has been an increasing workload, which has not been accompanied by an increase of financial means and capacity. The Committee therefore recommends that:

It should be guaranteed that both the national and European supervisory authorities are provided with sufficient financial and personal resources to be able to supervise the use and access to Eurodac data adequately.

7. Exchange of data with third countries (Article 35)

In Article 35 it is stated that personal data obtained by a Member State or Europol from the Eurodac database shall not be transferred or made available to any third country or international organisation or a private entity established in or outside the European Union. This provision does not prevent that Eurodac data, when stored in the national data bases of EU or Dublin States will be transferred to third states outside the framework of the Dublin Regulation. The Meijers Committee therefore proposes to add to Article 35 (in italics):

Personal data obtained by a Member State or Europol pursuant to this Regulation from the Eurodac central database shall not be transferred or made available to any third country or international organisation or a private entity established in or outside the European Union. This prohibition shall be without prejudice to the right of Member States to transfer such data to third countries to which the Dublin Regulation applies. *Personal data obtained by a Member State or Europol and processed further in national databases, shall not be transferred or made available to any third country or international organisation or a private entity established in or outside the European Union.*

¹³ Presidency compromise suggestions, 13884/12, 20 September 2012 and opinion of the EDPS, paragraph 59, 5 September 2012.

Anlage 10



An efficient and protective Eurodac

UNHCR comments on the Commission's amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No [.../...] (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person) and to request comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (Recast version)

Introduction

'Eurodac' was created in 2000 by Regulation (EC) 2725/2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention (hereafter 'Eurodac' Regulation).¹ On 3 December 2008, the European Commission proposed² to recast both the 'Eurodac' Regulation (hereafter 2008 proposal), as well as Council Regulation 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a Third Country National (hereafter the 'Dublin II' Regulation).³ Those proposals set out to remedy a number of shortcomings in the application of these instruments, as identified in the Commission's report on the evaluation of the Dublin System (hereafter 'Evaluation

¹ Council of the European Union, *Council Regulation (EC) No 2725/2000 of 11 December 2000 Concerning the Establishment of 'Eurodac' for the Comparison of Fingerprints for the Effective Application of the Dublin Convention*, 11 December 2000, Official Journal of the European Communities; 15 December 2000, available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000R2725:EN:HTML>

² European Commission, *Proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] (Recast version)*, 3 December 2008, COM(2008) 825 final, available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0825:FIN:EN:PDF>; and European Commission, *Proposal for a Regulation of the European Parliament and of the Council establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person (Recast)*, 3 December 2008, COM(2008) 820 final, available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0820:FIN:EN:PDF>.

³ *Council Regulation (EC) No 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national*, Official Journal ('OJ') L 050, 25/02/2003, p. 1-10, available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32003R0343:EN:NOT>

Report') published in June 2007.⁴ The European Parliament completed its first reading of the two proposals on 7 May 2009.⁵

Withdrawal of the proposal of law enforcement access to 'Eurodac' data

On 10 September 2009, the European Commission adopted two proposals: firstly, a proposal for a Council Decision on requesting comparisons with 'Eurodac'⁶ data by Member States' law enforcement authorities and Europol for law enforcement purposes;⁷ and secondly, an amended proposal for a recast of the 'Eurodac' Regulation (hereafter September 2009 proposals).⁸ The proposals aimed at taking into account the position of the co-legislators, the Council and the European Parliament, and to introduce the possibility for law enforcement authorities and Europol to have access to 'Eurodac' data.

With the entry into force of the Treaty on the Functioning of the European Union (TFEU),⁹ the September 2009 proposals lapsed. Consequently, on 11 October 2010, the European Commission presented another amended proposal for a recast of the 'Eurodac' Regulation (hereafter October 2010 proposal).¹⁰ In order to accelerate the negotiations on the asylum package and agreement on 'Eurodac' in particular, the European Commission decided to withdraw the proposal for law enforcement authorities' access to 'Eurodac' data and proposed two further

⁴ European Commission, *Report from the Commission to the European Parliament and the Council on the evaluation of the Dublin System COM(2007)299*, 6 June 2007, available at:

http://ec.europa.eu/justice_home/news/intro/doc/com_2007_299_en.pdf

⁵ European Parliament, *Legislative resolution of 7 May 2009 on the proposal for a regulation of the European Parliament and of the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No (.../...) [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] (recast)*, available at:

<http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P6-TA-2009-0378&language=EN&ring=A6-2009-0283> ; and European Parliament legislative resolution of 7 May 2009 on the proposal for a regulation of the European Parliament and of the Council establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person (recast), available at:

<http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P6-TA-2009-0377&language=EN&ring=A6-2009-0284>.

⁶ 'Eurodac' refers to the database established under the 'Eurodac' Regulation.

⁷ European Commission, *Proposal for a Council Decision on requesting comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes*, 10 September 2009, COM(2009) 344 final, available at:

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0344:FIN:EN:PDF> .

⁸ European Commission, *Amended proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EC) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person]*, 10 September 2009, COM(2009) 342 final, available at:

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0342:FIN:EN:PDF>

⁹ European Union, *Consolidated version of the Treaty on the Functioning of the European Union*, 13 December 2007, 2008/C 115/01, available at: <http://eur-lex.europa.eu/JOHtml.do?uri=OJ:C:2010:083:SOM:EN:HTML>

¹⁰ European Commission, *Amended proposal for a Regulation of the European Parliament on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EC) No [.../...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] (Recast version)*, 11 October 2010, COM(2010)555 final, available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0555:FIN:EN:PDF>.

technical amendments. The European Parliament supported this revised approach on the part of the Commission in its report adopted by the Committee on Civil Liberties, Justice and Home Affairs in February 2011.¹¹

**New 2012
proposal
including law
enforcement
access**

In May 2012, the Commission presented a new proposal for an Amended 'Eurodac' Regulation which merges into a single regulation on the one hand the proposed amendments for the better functioning of 'Eurodac', and on the other hand law enforcement access to 'Eurodac' (hereafter the 2012 proposal).¹² The European Commission explains this new proposal by the fact that since 2010 it has become clear that "including law enforcement access for Eurodac is needed as part of a balanced deal on the negotiations of the Common European Asylum System (CEAS) package with a view to completing the package by the end of 2012".¹³

**UNHCR's
Mandate**

UNHCR, pursuant to its supervisory function for the 1951 Convention and consultative role on EU asylum matters, puts forward comments and observations on EU legislative and policy proposals related to asylum and refugee protection.

In March 2009, UNHCR published its observations on the initial 2008 proposals. The comments below should be read in conjunction with this set of observations.¹⁴ The aim of the recast of the CEAS standards is first and foremost to ensure the adoption of higher legislative standards than those put in place under the first generation asylum instruments. Principled agreements should therefore be sought which reflect international refugee and human rights law, as well as good practice and high quality standards.

¹¹ European Parliament, *Report on the amended proposal for a regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EC) No [...] [establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] (recast)*, (COM(2010)0555 – C7-0319/2010 – 2008/0242(COD)), available at: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-450.875+01+DOC+PDF+V0//EN&language=EN>.

¹² European Commission, *Amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No [...] (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person) and to request comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (Recast version)*, COM (2012)254 final, 30 May 2012, available at: http://ec.europa.eu/home-affairs/doc_centre/asylum/docs/COM%202012%20254%20final%201_EN_ACT_part1_v13.pdf.

¹³ *Ibid.*, p. 3.

¹⁴ UNHCR, *Comments on the European Commission's Proposal for a recast of the Regulation of the European Parliament and of the Council establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third country national or a stateless person ("Dublin II") (COM(2008) 820, 3 December 2008) and the European Commission's Proposal for a recast of the Regulation of the European Parliament and of the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of [the Dublin II Regulation] (COM(2008) 825, 3 December 2008), 18 March 2009*, available at: <http://www.unhcr.org/refworld/docid/49c0ca922.html>

UN principles of lawfulness and fairness

The 1990 UN General Assembly Guidelines for the Regulation of Computerized Personal Data Files¹⁵ set out the principles of *lawfulness* and *fairness*, and the principle of *purpose-specification* as key principles of data protection regimes. In adopting this Resolution, the UN confirmed that data protection and privacy are central to its protection and human rights principles. Similarly, Article 8 of the European Convention on Human Rights¹⁶ and Article 8 of the European Charter of Fundamental Rights¹⁷ require that data collection be necessary and “*processed fairly for specified purposes*”.

Necessity and proportionality Eurodac is not demonstrated

‘Eurodac’ was established to facilitate the application of the ‘Dublin II’ Regulation. Extending access to ‘Eurodac’ for law enforcement authorities therefore constitutes a significant change in the original purpose. The proportionality, necessity and utility of this proposal for combating terrorism and other serious crime should be examined and confirmed before it can be agreed.¹⁸

Change to ‘Eurodac’'s original purpose

In addition, in UNHCR’s view, this change may lead not only to interference with the right to privacy and family life of asylum-seekers and refugees, but it may also place a refugee and his/her family at significant risk of harm, if the information is shared with countries of origin. It may also result in stigmatisation of asylum-seekers as a group by associating them with criminal activity. Furthermore, UNHCR takes note that the proposal to include the possibility to search latent fingerprints relies on technology in which the risk of error has not been fully examined and eliminated (latent fingerprints). The original purpose of ‘Eurodac’, as set out in the ‘Eurodac’ Regulation, is to facilitate the operation of the ‘Dublin II’ Regulation with the aim of determining the Member State responsible for examining the asylum application. Based on this, UNHCR considers that ‘Eurodac’ should be used for its original purpose.

¹⁵ UN General Assembly, *Guidelines for the Regulation of Computerized Personal Data Files*, 14 December 1990, available at: <http://www.unhcr.org/refworld/docid/3ddcafaac.html>.

¹⁶ Council of Europe, *Convention for the Protection of Human Rights and Fundamental Freedoms*, available at : <http://www.echr.coe.int/nr/rdonlyres/d5cc24a7-dc13-4318-b457-5c9014916d7a/0/englishanglais.pdf>

¹⁷ European Union, *Charter of Fundamental Rights of the European Union*, available at: http://www.europarl.europa.eu/charter/pdf/text_en.pdf

¹⁸ The necessity for proportionality of access for law enforcement authorities to fingerprint data of asylum-seekers and refugees in the EU is not fully demonstrated. The 2009 impact assessment referred to the fact that “*access should be limited to designated authorities and only on a case-by-case basis*”, but did not include any justification demonstrating how the proposals meet any of the data protection requirements stated above. Expert sources have questioned whether the use of ‘Eurodac’ may enable law enforcers more effectively to find and convict criminals, or whether ‘Eurodac’ access would yield useful outcomes in terms of detecting more criminals, given the mismatches and errors that can occur between imperfect traces of fingerprints and fingerprints in ‘Eurodac’. More data and consultation may be useful on all of these issues.

**UNHCR
recommends
further
safeguards**

UNHCR recommends that as a minimum, several safeguards are put in place.

In particular, UNHCR recommends that:

- **the possibility of error in matching fingerprints and the wrongful implication of asylum-seekers in criminal investigations is fully examined and eliminated to the greatest extent possible before the possibility to search ‘Eurodac’ with latent fingerprints is introduced;**
- **the provisions on the prohibition of transfer of information on asylum-seekers or refugees to third countries are reinforced and clarified to eliminate any gaps in the protection of data;**
- **the potential for stigmatisation of asylum-seekers as a particularly vulnerable group is evaluated;**
- **the scope of the instruments is limited to cases where there is substantial suspicion that the perpetrator or suspect has applied for asylum; and**
- **the applicant is informed that his/her data may be used for the purpose of criminal investigations.**

Risk of Error

**Searching
latent
fingerprints**

The European Commission proposes the possibility for law enforcement authorities to search ‘Eurodac’ based on latent fingerprints (article 2(1)(l)). A latent fingerprint is a fingerprint left on a surface touched by an individual which may be found at a crime scene. UNHCR notes that the 2012 proposal does not provide a detailed definition of what a latent fingerprint is. Usually latent fingerprints are limited to one or two fingers and are fragmentary or partial. UNHCR understands that assessing the possibility of error in matching latent fingerprints and fingerprints stored in ‘Eurodac’ (false match and false non matches) requires a high level of technical expertise. Any search in ‘Eurodac’ based on a latent fingerprint may lead to a high number of possible matches, given the wider range of possible correlations with partial or fragmentary prints. These would then have to be examined by a human investigator. The Commission seeks to reduce risks of error by clarifying that all automated hit results should be checked by a fingerprint expert (article 18(4)) – a requirement which UNHCR welcomes. Nevertheless, UNHCR notes that latent fingerprints require even greater interpretation than other prints matched in the automated process. This will be resource-intensive as it requires high technical expertise, and is not error-free. The consequences of a false match may be very serious and may lead to the wrongful implication of innocent persons in criminal investigations. In addition, the rate of error may be influenced by the quality of the latent fingerprints (which are often blurred or distorted by other matter, adding to the difficulty of matching these

fingerprints to those stored in 'Eurodac' which are taken in "clean" conditions). Other factors which may influence error rates include technology issues (varying software, algorithms), as well as variations in the law enforcement authorities' methodology. The high risk of error raises questions about how a possible match based on a latent fingerprint will be treated in any subsequent investigation.

Damaging consequences of a possible false match

UNHCR is particularly concerned about the potential consequences for innocent asylum-seekers of being wrongfully implicated in a criminal investigation as a result of a false match of a latent fingerprint in 'Eurodac'. Asylum-seekers often have limited knowledge of the language and legal culture of the country where they are seeking asylum, and are therefore at a significant disadvantage in seeking to assert their innocence. Furthermore, they are particularly vulnerable due to their provisional legal status as asylum-seekers, and their ongoing asylum application processes. These factors may make it difficult for asylum-seekers to challenge law enforcement bodies, even if they are innocent of the alleged crimes.

UNHCR takes note that no independent external expertise on the technical aspects of the suggested use of 'Eurodac' was sought ahead of the 2009 proposals or since.¹⁹ In 2009, the Commission recognized that the current 'Eurodac' Regulation does not provide the possibility to search the database on the basis of latent fingerprints, and that such facility would be added later.

Recommendation

UNHCR suggests deleting the possibility to search 'Eurodac' data based on latent fingerprints from article 2(1)(l) until independent technical expert opinions are available confirming that the risk of error of matching between latent fingerprints and fingerprints stored in 'Eurodac' is eliminated to the greatest extent possible. This is particularly important considering the significant prejudice an asylum-seeker may face if wrongfully implicated in a criminal investigation.

Protection risks linked to data sharing

Prohibition of sharing data with third countries

UNHCR welcomes the explicit prohibition of the sharing of personal data with third countries, organizations or entities (article 35). Sharing of personal data of asylum-seekers with third parties, such as the authorities in the country of origin, which may be the agents of persecution or human rights violations, could seriously jeopardize the safety, not only of the asylum-seeker, but also of his/her family or associates. As underlined by the Commission in its evaluation on the compliance of the proposal with the right to asylum guaranteed by Article 18 of the Charter of Fundamental Rights,²⁰ insufficient guarantees could deter refugees from applying for asylum in the EU, thus denying them the necessary protection from harm to which they are entitled under international and regional protection regimes.

¹⁹ See footnote 7, p. 5.

²⁰ See footnote 12, Explanatory Memorandum, p. 6

Only “hits” are covered by prohibition

UNHCR considers it vital to retain this prohibition on data transfer in a broader, unqualified form, and fears that the proposed safeguard is insufficient to ensure that all asylum-related information is not shared in a manner that places asylum-seekers and their families at risk. UNHCR shares the concern raised by the European Data Protection Supervisor (EDPS) that the proposal does not clearly specify that this prohibition extends to all possibilities of transferring personal data including for law enforcement purposes under Framework Decision 2006/960/JHA.²¹

In this respect, the prohibition only covers fingerprint data obtained from a hit in ‘Eurodac’. The ‘hit’/‘no hit’ system is put forward as a major safeguard in law enforcement access to ‘Eurodac’ data as “it will only determine if another Member State holds data on an asylum-seeker”²² and prevent mass comparison of data. While UNHCR welcomes this safeguard, it cautions that it is likely that after a ‘positive hit’ on a fingerprint stored in ‘Eurodac’, authorities would make requests for further ‘underlying’ information from the concerned Member State. This could possibly include all information in the asylum claim file of the individual concerned, which may be sensitive and confidential, having been gathered for the specific purpose of assessing a person’s need for international protection.

Data shared following a hit may be shared with third countries

The 2012 proposal does not define what data may be shared following a hit in ‘Eurodac,’ proposing only that such information may be exchanged under the existing rules of instruments on information-sharing for law enforcement purposes.²³ However, the Framework Decision 2008/977/JHA on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union²⁴ and the proposed Directive which will replace the Framework Decision,²⁵ do not contain a prohibition on transferring data to third countries. The foreseen prohibition in Article 35 on transferring the data to third countries may therefore have little practical impact, and fail to fully protect asylum-seekers. This means that sensitive information, including data

²¹ European Data Protection Supervisor, *Opinion of the European Data Protection Supervisor on the amended proposal for a Regulation of the European Parliament and of the Council on the establishment of 'EURODAC' for the comparison of fingerprints for the effective application of Regulation (EU) No [.../...] [...] (Recast version)*, 5 September 2012, p. 10, available at:

http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-09-05_EURODAC_EN.pdf.

²² See footnote 12, Explanatory Memorandum, p. 7

²³ See footnote 12, Explanatory Memorandum, p. 7 “the proposal does not provide for new possibilities to process additional personal information in the follow up to a ‘hit’”.

²⁴ European Union: *Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union*, available at:

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:386:0089:0100:EN:PDF>

²⁵ European Commission, *Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data*, COM (2012) 10 final, 25 January 2012, available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:EN:PDF>.

concerning his/her asylum claim, can potentially be shared with third parties, including the country of origin of the asylum-seeker. UNHCR shares the concerns raised by the EDPS on the lack of clarity with Framework Decision 2008/977/JHA which does not provide a prohibition of transferring data to third countries,²⁶ and recommends that this is clarified in Article 35.

Recommendation

UNHCR recommends that article 35 is amended in order to ensure that the prohibition of transfer of data to third countries extends to all data and information exchanged between Member States on the basis of a 'positive hit' in Eurodac:

Personal data obtained by a Member State or Europol pursuant to this Regulation, *including personal data obtained by a Member State and processed further in national databases for law enforcement purposes*, from the EURODAC central database shall not be transferred or made available to any third country or international organisation or a private entity established in or outside the European Union. This prohibition shall be without prejudice to the right of Member States to transfer such data to third countries to which the Dublin Regulation applies.

Procedure for comparisons with 'Eurodac' data for law enforcement purposes

Two-step approach for searches

UNHCR welcomes the fact that a number of safeguards have been included in the 2012 proposal with the stated intention of mitigating the limitation of the right to protection of personal data. These safeguards include a two-step approach whereby comparisons with 'Eurodac' data are only authorized after searches in national databases and in the Prüm databases have returned negative decisions (article 20(1)). UNHCR notes that in cases where Member States may not have yet implemented Council Decision 2008/615/JHA²⁷ (Prüm Decision), they will not be able to conduct searches in 'Eurodac' for law enforcement purposes.²⁸

²⁶ See footnote 21, para. 43

²⁷ Council of the European Union, *Council Decision 2008/616/JHA of 26 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime*, available at:

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:210:0012:0072:EN:PDF>

²⁸ See footnote 12, Explanatory Memorandum, p. 7.

Limiting searches to cases where there is a substantiated suspicion that the person has applied for asylum

The proposed scope envisages that ‘Eurodac’ data may be searched for the purposes of the “prevention, detection and investigation of terrorist offences and other serious criminal offences” (article 1(2)). This scope is of some concern insofar as it does not restrict searches of fingerprint data to persons who are suspects, increasing the risk of implicating innocent persons. UNHCR recommends that the ‘Eurodac’ database may only be searched in relation to a specific criminal offence, where there is substantiated suspicion that the suspect is an asylum-seeker or has entered the territory irregularly, in the framework of an investigation under judicial control. UNHCR notes that Recital 9 refers to the need for law enforcement authorities to have access to ‘Eurodac’ data in well-defined cases “when there would be a substantiated suspicion that the perpetrator of a terrorist or other serious criminal offence has applied for asylum”. UNHCR would recommend that this safeguard is reflected in the conditions for access to ‘Eurodac’ data by designated authorities in Article 20.

Recommendations

- ✓ UNHCR recommends that ‘Eurodac’ data searches by law enforcement authorities should be permitted in limited circumstances only, as part of an ongoing criminal investigation and in cases where there is a substantiated suspicion that the perpetrator or suspect has applied for asylum. UNHCR therefore recommends amending Article 20(1) to add a new subparagraph (d):

(d) there is substantiated suspicion that the suspect or perpetrator of a terrorist or other serious criminal offence has applied for asylum.

Information regarding the rights of the data subject

Information in a language that the person understands

UNHCR welcomes the inclusion in Article 29 the requirement to include information on ‘Eurodac’ in the leaflet given to persons seeking international protection falling under the Dublin system. UNHCR notes however with concern that the person affected by the ‘Eurodac’ Regulation should receive information about his/her rights in a language which s/he understands “or may reasonably be presumed to understand.” It is particularly important that the person should fully understand his/her rights in the framework of the Regulation, if personal data might be used by law enforcement authorities. In addition, UNHCR considers that persons seeking international protection should be informed both of the aims of the ‘Dublin II’ Regulation, but also of the possibility that their fingerprints may be used for the purpose of the prevention, detection and investigation of terrorist offences and serious crimes.

Recommendations

- ✓ UNHCR considers that Article 29(1) should be amended so that information is made available in “a language that the applicant understands” rather than one that s/he “is reasonably presumed to understand”. This change should also be made in the 4th indent with regards to be information contained in the leaflet:
- ✓ UNHCR recommends that article 29(1)(b) is amended to include the requirement to inform the asylum-seeker on the possibility of law enforcement access to Eurodac data:

(b) regarding the purpose for which his or her data will be processed within EURODAC including *the purposes in Article 1(2) and* a description of the aims of the Dublin Regulation, in accordance with Article 4 of that Regulation.

Risk of stigmatisation of persons seeking international protection

Asylum-seekers’ whose fingerprints are stored are at increased exposure to investigation

UNHCR is concerned that access for law enforcement authorities to ‘Eurodac’ data could lead to increased stigmatisation of asylum-seekers. People registered in ‘Eurodac’ with no criminal record would face greater likelihood of being subject to criminal investigation than other members of the community whose fingerprints are not collected or stored on a systematic basis. This increased exposure of asylum-seekers to investigation, simply because their fingerprints are in an accessible database, could fuel misperceptions that there is a link between asylum-seekers and crime, and feed xenophobia and racism. Where police records of such investigation are kept, even when the person is found to be innocent, this may further hamper the person’s integration into society if s/he is subsequently granted protected status. This is because police records are consulted for a range of purposes in many Member States, including in connection with possible employment, rental of housing– including important steps in the process of integration and participation in society.

In this regard, UNHCR recalls that many persons in need of international protection, including those granted status and those still in the asylum procedure, may have suffered persecution, violence and human rights abuses inflicted by authorities in their countries of origin. In some cases, this may have been at the hands of police. Increased scrutiny by law enforcement authorities may therefore cause disproportionate pressure and potentially harm to people whose data is available, although they are not suspected of nor charged with any crime.

Evaluation of stigmatisation after the fact is insufficient

In its evaluation of the compliance of the proposal with the Charter on Fundamental Rights, the Commission considers *inter alia* the issue of stigmatisation when assessing if the 2012 proposal limits the right to asylum as guaranteed by Article 18 of the Charter.²⁹ The Commission concludes that the right to asylum is not limited as the extensive evaluation and monitoring mechanism included in Article 40 “will include whether the operation of the search functionality for law enforcement purposes will have led to the stigmatisation of persons seeking international protection.”³⁰ However, evaluating stigmatisation after it has occurred would not protect or assist persons who have already suffered from such stigmatisation. UNHCR considers that this issue should have been the subject of a comprehensive evaluation before law enforcement access to ‘Eurodac’ data was introduced, and that evaluating stigmatisation after its introduction is a minimum requirement. UNHCR would recommend that the evaluation of stigmatisation should be specifically referred to in the areas for evaluation in Article 40(5).

Non-discrimination

Non-discrimination is a key human rights principle applicable also to the collection of personal data of groups of persons. It is specifically highlighted in the UN General Assembly Guidelines for the Regulation of Computerized Personal Data Files³¹ as an important principle for which there are strict conditions and limits to possible exceptions. Discrimination concerns arise in relation to ‘Eurodac’ as the database contains fingerprints only of certain groups of persons, including asylum-seekers. Similar information is however not available to law enforcement bodies for other groups of persons in the EU. This distinguishes the ‘Eurodac’ proposal from the Visa Information System (VIS) and the Schengen Information System (SIS), which already provide for law enforcement access to personal information on Third Country Nationals in general, including asylum-seekers, and therefore does not single them out as a group for particular scrutiny.

²⁹ See footnote 17.

³⁰ See footnote 12, Explanatory Memorandum, p.6.

³¹ UN General Assembly, *Guidelines for the Regulation of Computerized Personal Data Files*, 14 December 1990, available at: <http://www.unhcr.org/refworld/docid/3ddcafaac.html>

Recommendation

UNHCR recommends that Article 40(5) is amended in order to include stigmatisation as one of the issues to be evaluated:

Three years after the start of application of this Regulation as provided for in Article 46(2) and every four years thereafter, the Commission shall produce an overall evaluation of EURODAC, examining results achieved against objectives and assessing the continuing validity of the underlying rationale, and any implications for future operations, ***including whether the operation of the search functionality for law enforcement purposes will have led to the stigmatisation of persons seeking international protection***, as well as make any necessary recommendations. The Commission shall transmit the evaluation to the European Parliament and the Council.

Conclusion

UNHCR appreciates the importance attached by Member States to law enforcement access to 'Eurodac' data, as well as the effort of the European Commission to achieve a balance between the Member States' positions and concerns raised by UNHCR, the European Data Protection Supervisor and civil society during the 2008 consultation process. UNHCR considers however that law enforcement access to 'Eurodac' data would make a significant change to the purpose of 'Eurodac'; and would create a risk that the data on asylum-seekers may be transferred to countries of origin, which could have serious consequences for the life and safety of refugees and their families. It would further risk putting persons seeking international protection at risk of stigmatisation. UNHCR considers that the lack of technical certainty could create further obstacles and risks for people seeking asylum in the European Union.

UNHCR
Bureau for Europe
November 2012