



university of
 groningen

ACCESS TO EURODAC BY LAW ENFORCEMENT AUTHORITIES

-

AN ASSESSMENT

June 2011

This paper was written and researched by Vincent Eeclaudt,
under the supervision of dr. H.D. Wolswijk (Groningen University).

For more information concerning this paper, feel free to contact

Vincent Eechaudt
Vincent.Eechaudt@UGent.be
Vincent.Eechaudt@gmail.com

The views in this report are the author's own and do not necessarily reflect those of the European Council on Refugees and Exiles or Groningen University. This paper is distributed in the form submitted by the author. There has been no additional copyediting or typesetting.

Reproduction is authorised provided the source is acknowledged.

“Justice cannot be for one side alone, but must be for both.”

Eleanor Roosevelt

Many thanks go out to my parents, sister and partner,
who gave me a compass
to orient myself in life.

I would also like to thank Dr. Hein Wolswijk at Groningen University,
Kris Pollet at the European Council for Refugees and Exiles,
Els De Busser at the Max Planck Institute For Foreign and International Criminal Law,
the people at the Institute for International Research on Criminal Policy
(Ghent University), particularly Wendy De Bondt
and Cornelia Riehle at the Academy of European Law,
for making this research possible and for assisting me in this paper's process.

TABLE OF CONTENTS

Table of contents	p 7
Abstract	p 9
List of abbreviations.....	p 10

1. Introduction

1. Aim, context and relevance of the study	p 11
2. Methodology	p 14
3. The various chapters at a glance.....	p 14

2. The EU policy on irregular migration and the link with its security policy

1. Globalisation and migration	p 16
2. The EU policy on irregular migration and asylum.....	p 17
3. The use of databases and the link with the EU security policy	p 20

3. On the access by law enforcement authorities and Europol to Eurodac

1. A short history of the proposal concerning LEA's access to Eurodac.....	p 23
2. What do the proposals say?.....	p 25
3. Motivating the proposals	
Prevent, detect and investigate terrorism and other serious crime.....	p 26
Existing access to national asylum databases.....	p 30
4. Concerns on data protection	
The principle of legality, purpose limitations and function creep.....	p 33
The principles of proportionality and necessity	p 38
Effective control on the data	p 44
5. Stigmatising asylum seekers?.....	p 48
6. The need for a complete, qualitative database and correct identifications.....	p 50

4. Conclusions	p 52
----------------------	------

Bibliography	p 55
--------------------	------

Annexes p 67

1. Proposal for a Council Decision on access to Eurodac, COM(2009) 344
2. Proposal for a Regulation establishing Eurodac, COM(2009) 342

ABSTRACT

In 2009 the European Commission presented a proposal to open up Eurodac for law enforcement purposes, as part of the bigger reform of the Dublin system. However, this proposal has been heavily criticised by different stakeholders. This paper analyses the different comments given on the proposal and gives arguments pro or contra. More particularly, the reasons for this proposal, concerns of data protection, the stigmatisation of asylum seekers and the false recognition rates are assessed. This paper thus tries to establish a balance between law enforcement on the one hand and legal safeguards and human rights on the other hand.

Keywords: Eurodac, law enforcement authorities, data protection, asylum seekers.

LIST OF ABBREVIATIONS

AFSJ:	Area of Freedom, Security and Justice
CEAS:	Common European Asylum System
CFREU:	Charter of Fundamental Rights of the European Union.
Council:	Council of the European Union
EC:	European Commission
ECHR:	European Convention of Human Rights of the Council of Europe.
ECJ:	European Court of Justice
ECtHR:	European Court of Human Rights
EDPS:	European Data Protection Supervisor
LEA access:	Law enforcement authorities' access to Eurodac. Depending on the stage of the negotiations, this includes access by Europol to Eurodac. It will be made sufficiently clear in the paper when Europol is not yet involved.
SIS (II):	Schengen Information System (II). This system also contains information on illegally apprehended persons. It was originally conceived for 18 member states, however SIS II is now under development.

1. INTRODUCTION

“[There is] the need to ensure that the police exercise their powers to control and prevent crime in a manner which fully respects [human rights] guarantees which legitimately place restraints on the scope of their action to investigate crime and bring offenders to justice”
 - *European Court of Human Rights, Osman v. UK, 1999*

1. Aim, context and relevance of the study

This study seeks to provide insight into the European Commission proposals for granting the member states’ law enforcement authorities and Europol access to Eurodac for law enforcement purposes. Hence, different points of controversy will be critically assessed. The emphasis will be placed on whether or not there is a substantial benefit for law enforcement and if there will be enough safeguards against misuse and other detrimental consequences of the proposal for its target group: refugees and migrants. In other words, the basic research question raised in the following paper is **whether the proposals to open up Eurodac for law enforcement purposes can be seen as balanced measures to combat terrorism and serious crime or if the proposals neglect human rights concerns in the field of migration and justice**. To have a good understanding of the discussed topics however, the proposal on LEA access will first be contextualised in the current EU policy in the area of freedom, security and justice. The added value of this research lies in approaching migration issues from a criminal law perspective and whether or not the proposed measures take into account the specific sensitivities when dealing with asylum seekers.

Co-operation in the field of justice, security and migration (commonly referred to as the Area of Freedom, Security and Justice) has already been taking place a few decades on the European Union level. Since the Maastricht Treaty¹ was signed in 1992, co-operation was formalised with the creation of the so-called third pillar², which was characterised by an intergovernmental decision-making process and thus only minor democratic control. With the adoption of the Amsterdam Treaty³ in 1997 and its entry into force in 1999, the asylum and migration policy was transferred to the first pillar, the result of which reflected in the fact that the European Parliament had the right to participate in the decision-making process. This is why the European Commission presented two separate proposals on law enforcement authorities’ access to Eurodac⁴ (further: LEA’s access) as it was a combination of first and third pillar policy measures. Since the entry into force of the Treaty of Lisbon⁵ the pillar

¹ Treaty on European Union, 29 July 1992, OJ C 191.

² Its competencies were defined in Title VI of the Maastricht Treaty.

³ Treaty of Amsterdam, 10 November 1997, OJ C 340.

⁴ Commission of the European Communities, COM(2009) 342, 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] (Recast version), 10 September 2009, 74 p. and Commission of the European Communities, COM(2009) 344 final, 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, 21 p.

⁵ Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, 17 December 2007, OJ C 306.

structure has been abolished and more powers have been granted to the European Parliament, which now has to give its approval to all new legislation concerning migration, judicial co-operation in criminal matters, etc. However, certain subjects such as operational police co-operation and passports are still subject to a unanimous decision of the European Council with the European Parliament only being consulted for advice.⁶ Concerning the proposals for LEA's access to Eurodac, much of its preparation was done under the former three-tier structure, with the result that this paper may often refer to the pre-existing EU structure.

To assure a consistent policy in the area of freedom, security and justice, there have been different multi-annual programs in which the Council unveils what measures it wants to take to strengthen international co-operation.⁷ For example, after the Tampere-top in 1999, the ministers of all EU member states decided to focus on mutual recognition in criminal matters. As such, member states would recognise and execute each other's judicial decisions without the formalities formerly needed to ensure that EU citizens were guaranteed fair criminal proceedings. European judicial and police co-operation steadily developed, not in the least after the terrorist attacks on 11 September 2001 in the US and the Madrid and London bombings in 2004 and 2005. For the 2005-2009 period, the fight against terrorism became an absolute priority for the EU as exemplified by the Hague Programme.⁸ This policy document asked for the 'principle of availability' to be applied across the EU member states. The principle of availability was defined in the Hague Programme as follows:

With effect from 1 January 2008 the exchange of [...] information should be governed by the principle of availability, which means that, throughout the Union, a law enforcement officer in one Member State who needs information in order to perform his duties can obtain this from another Member State and that the law enforcement agency in the other Member State which holds this information will make it available [...].⁹

It implied that member states should make their police and judicial information available to all other member states without any of the usual obstacles. The exchange of information between member states indeed has to be improved, the principle of availability however equally abolished legal safeguards for the individual.¹⁰ It is this principle of availability that underlies the proposal for access of law enforcement authorities to Eurodac. Eurodac is a EU-wide database used for comparing fingerprints of asylum seekers and certain categories of irregular immigrants.¹¹ It facilitates the application of the Dublin II Regulation (see *infra*), which makes it possible to determine the EU country responsible for examining an asylum application. If law enforcement authorities would be granted access to Eurodac, police agencies would be able to compare their data with biometrics which were stored on the EU

⁶ General Secretariat of the Council of the EU, *The Lisbon Treaty's impact on the Justice and Home Affairs (JHA) Council: More co-decision and new working structures*, Brussels, December 2009, p. 2, WWW <http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/111615.pdf>.

⁷ On how the different programmes came about: Eechaudt, V., *De voorbereidingen van het Stockholm Programma geanalyseerd*, Gent, 2010, WWW <http://lib.ugent.be/fulltxt/RUG01/001/458/143/RUG01-001458143_2011_0001_AC.pdf>. (Master dissertation).

⁸ Council of the European Union, *The Hague Programme: strengthening freedom, security and justice in the European Union*, 3 March 2005, OJ C 53.

⁹ *Ibid.*, OJ C 53/7.

¹⁰ Commissioner for Human Rights, *CommDH/IssuePaper(2008)3, Protecting the Right to privacy in the fight against terrorism*, Strasbourg, 4 December 2008, p. 10.

¹¹ Council of the European Union, "Eurodac" system, WWW <http://europa.eu/legislation_summaries/justice_freedom_security/free_movement_of_persons_asylum_migration/l33081_en.htm>.

level for the purpose of processing asylum claims. This puts the LEA access proposal at the forefront of an expanding interpretation of the principle of availability, especially because the principle of availability is not limited anymore to police and judicial measures (the former third EU pillar), but expands to areas which are not primarily set up for security reasons (the former first pillar), concerning the querying of data from people with a clean criminal record. As such it was received very critically by civil society. Further comments have been made on different legal aspects of the proposal (data protection rules, legal basis of the proposal), as well as on the impact the proposal might have on a particularly vulnerable group in society (e.g. the stigmatisation of asylum seekers). The policy programme for 2010-2014, the so-called Stockholm Programme¹², recalls a number of basic principles for the use of data by public authorities (purpose limitation, proportionality, legitimacy of processing, etc.) and underscores the balance between security and fundamental rights.¹³ This renewed attention to human rights and legal safeguards seems promising. As the Council plans to propose LEA access to Eurodac again in 2012, their new proposal might depart from the one proposed in 2009, and take into account the comments given by civil society and the principles enumerated in the Stockholm Programme.¹⁴

This essay is particularly **relevant for criminology and international criminal law and policy**, as it will explore the way policy makers wish to combat crime, more specifically terrorism and serious crimes. It will therefore explore the intertwining of the EU migration policy with the EU security policy, which are seen as two different aspects by a significant part of civil society, but seem to be two different sides of the same coin for the European Union. EU co-operation in criminal matters has been increasingly important during the last decade and has proven to be essential in a borderless European Union. While the exchange of information concerning criminal cases only seems beneficial for victims, society, falsely accused persons and law enforcement agencies, EU measures in this area sometimes lack attention for human rights, at which point they are being criticised by an active civil society (e.g. the commotion regarding the PNR agreements or Swift).¹⁵ This is particularly true for anti-terrorism measures. Terrorism is not a passing phenomenon, and measures taken to prevent, detect and investigate terrorism tend to become semi-permanent. Data protection, the right to privacy, anti-discrimination measures, etc. are frequently seen as an obstacle to effective anti-terrorist measures, and are all too often restricting fundamental democratic values. This means that decisions made in the context of anti-terrorism have a permanent implication on legal systems. The debate is now exploring the topic of immigrants, and which measures should be taken to prevent crimes committed by the latter. The argument that asylum seekers, and immigrants more in general, are more involved in crime, drives policy makers to focus on measures towards this specific group. Looking at a specific proposal - opening the EU asylum database for law enforcement purposes - this paper will try to consider whether or not due attention is paid to the needs of law enforcement and criminal

¹² Council of the European Union, The Stockholm Programme - An open and secure Europe serving and protecting citizens, 4 May 2010, OJ C 115.

¹³ Lodge, J., *Quantum surveillance and 'shared secrets' - a biometric step too far?*, Centre for European Policy Studies, 13 July 2010, p. 3, WWW <www.ceps.eu> and Council of the European Union, The Stockholm Programme - An open and secure Europe serving and protecting citizens, 4 May 2010, OJ C 115.

¹⁴ Council of the European Union, Outcome of proceedings of CATS on 25 and 26 October 2010, 16006/10, Brussels, 9 November 2010, p. 2.

¹⁵ The US-EU PNR (Passengers Name Record) agreement dealt with the exchange of information between the US and EU on passengers between both countries. It has been contested on data protection grounds caused by a lower level of data protection for EU citizens in the US. Swift is a worldwide financial messaging network. In 2006 it was revealed that the US accessed information on financial transactions. Again, privacy concerns formed the basis of the commotion.

investigations on the one hand, and whether or not human rights have been taken into account on the other hand.

In the light of the above, this study devotes particular attention to the following aspects of the LEA's access proposal:

- The merging of the EU asylum policy with the EU security policy;
- The motivation behind the proposals;
- Concerns of data protection;
- The stigmatisation of asylum seekers;
- The quality of the data in Eurodac and the recognition of fingerprints.

1.2 Methodology

The study is mainly descriptive, explaining contemporary evolutions in the field of EU justice and home affairs. More specifically, a mix of sources has been used, ranging from recent scientific research to laws and case-law, and from EU policy documents (as far as access to those documents has not been restricted) to advisory reports and other contributions made by related actors, such as NGO's, national parliaments and international organisations. The initial findings were then later fine-tuned by discussing certain sub-topics with experts at an ERA conference¹⁶ or e-mailing them.

The legislative proposal to open up Eurodac for law enforcement purposes is related to multiple policy areas, mainly combating crime and regulating asylum, but equally concerns data protection and technical matters, such as the quality of dactyloscopic data. Therefore, the different aspects have all been given some attention in this research by dealing with each subject separately. However, as this is a legal research, the main pro or contra arguments have been taken from legislation and jurisprudence. Although technical facts are also significant (e.g. the percentage of wrongly identified fingerprints), their interpretation has been taken mainly from jurisprudence (e.g. when those numbers are balanced against the principle of proportionality).

1.3 The various chapters at a glance

Chapter two provides a general overview of the two main policy areas related to the LEA's access to Eurodac proposal, asylum and the EU security policy. It also discusses the links between them and takes a closer look at the use of databases to control migration and crime. Thereafter, in chapter 3, the proposals for LEA's access are examined based on their possible consequences and merits for the actors involved. Different categories of problems are distinguished, and each category is given due attention. The paragraphs focus on the motivation of the proposal, concerns of data protection, the stigmatisation of asylum seekers and the need for a qualitative database and the correct identification of fingerprints. Chapter four presents the conclusions and recommendations deduced from this research. Two annexes are attached to this paper: the third pillar Council Decision on LEA's access and the

¹⁶ "SIENA, Prüm, SIS II, VIS, Eurodac - Law enforcement and information exchange in the EU today", Organised by ERA, the Academy of European Law in Trier on May 19th and 20th 2011. More information see: <http://www.era.int>.

first pillar Regulation concerning the reform of Eurodac, which contains stipulations on LEA's access.

* *

*

2. THE EU POLICY ON IRREGULAR MIGRATION AND THE LINK WITH ITS SECURITY POLICY

2.1 Globalisation and migration

Migration is far from being a new phenomenon. However, the number of migrants, the routes they use and the ways in which people migrate have changed considerably. This implies that the impact migration has on societies has changed significantly too.

Today, more people are living outside their homeland than at any previous time in history.¹⁷ More and more countries are crucially affected by migratory movements of all kinds, not only by labour migration, but also by refugee movements and people seeking permanent settlement.¹⁸ It is no surprise that exactly industrialised countries attract many of these foreigners. Global news channels like CNN, Al-Jazeera and many others disseminate images of the luxurious lifestyle of wealthy Westerners, leaving many foreigners with feelings of relative poverty. One of the effects of globalisation is that people increasingly get the perception that the world is becoming a global village. People are connected with others thousands of kilometres away, and events happening at the other side of the world can have a local impact. This has been extensively described by David Harvey as the 'time-space compression'.¹⁹ However, the increasing display of security, development and wealth in other parts of the world also leads to escalating feelings of relative deprivation. As a consequence, this leads, inter alia, to people migrating and wanting to achieve the same level of prosperity.²⁰ Apart from the pull-factors described above, migration can also be a result of push-factors such as war, persecution or the destructive effects of the EU common agricultural policy on local third-world markets. It's no coincidence that the main countries of origin for asylum seekers in the industrialised world are Afghanistan, Iraq and Somalia, countries torn by (civil) war.²¹

Parallel with the growth of migratory flows, most developed countries have placed greater limits on migration and permanent settlement. Consequently, there has also been an increase in illegal migration.²² EU member states have been known to unilaterally restrict their asylum systems, as such causing asylum seekers to knock on other member states' door.²³ As the EU limited access to its markets in the 1990's, there was a decrease in regular immigration, whereas the number of illegal immigrants had steadily risen in the same period.²⁴ Taking this

¹⁷ Papastergiadis, N., *The turbulence of migration: globalization, deterritorialization, and hybridity*, Polity Press, Cambridge, 2000, p. 10.

¹⁸ Castles, S. and Miller, M.J., *The age of migration: international population movements in the modern World*, Fourth edition, Palgrave Macmillan, Basingstoke, 2009, p. 7.

¹⁹ Harvey, D., *The condition of postmodernity: an enquiry into the origins of cultural change*, Blackwell, Oxford, 1990, 392 p.

²⁰ For more information on culture, structure and the concept of 'anomie', see Robert Merton's 'Social structure and anomie'.

²¹ UNHCR, *Asylum levels and trends in industrialized countries 2009 - statistical overview of asylum applications lodged in Europe and selected non-European countries*, Geneva, 2010, p. 10, WWW <<http://www.unhcr.org/4ba7341a9.html>>.

²² Aas, K.F., *Globalization & crime*, Sage publications, Thousand Oaks, 2007, p 30.

²³ Thieleman, E., Why asylum policy harmonisation undermines refugee burden-sharing, *European journal of migration and law* (1) 2004, pp. 47-65.

²⁴ APAP, J. and INCERTI, M., *Trust and co-operation in judicial, extradition, immigration and asylum matters - proceedings of a CEPS-SITRA network meeting*, Brussels, 23 March 2002, p. 6.

into account, globalisation has made the world borderless for some, while it has made others (or, one could say, the largest part of the human population) dependant on clandestine travel, excluded from regular forms of migration.²⁵ Although there are legitimate aims for controlling migratory flows, rendering migration illegal has not yet proven to be an effective measure to reduce it.²⁶ It is more likely that a punitive attitude towards migration only leads to a displacement of the phenomenon, translocating immigration routes to places where the least resistance is expected (also known as the waterbed-effect).²⁷

2.2 The EU policy on irregular migration and asylum

With the Schengen Agreement abolishing internal frontiers, member states agreed to strengthen police and judicial co-operation and to intensify the control at their external borders. This way they wished to better control transnational crime and fluxes of irregular migrants as both now had a potential impact on all of the Schengen states. Policymakers feared that the abolishment of internal border controls would be an incentive for asylum shoppers: once inside the territory of the EU it would have been possible for asylum seekers to apply for asylum in those member states with the most generous procedures.²⁸ The incorporation of the Schengen Agreement into the ‘acquis communautaire’ was done by the Amsterdam Treaty in 1999, which aimed for an EU-wide internal market, being an area with minimal controls on movement. At the same time the EU created an area of freedom, security and justice.²⁹ During the treaty’s preparations, the member states also agreed on establishing the Common European Asylum System (CEAS)³⁰, which was formally adopted at the Tampere-top in 1999. The CEAS’ goal was to harmonise the member states’ asylum procedure and to offer asylum seekers the same protection in every EU member state. Nevertheless, it progressed much slower than expected, which stands in contrast with the measures taken to ‘fight irregular migration’. The lack of interest from part of the member states to pursue a CEAS is mainly due to the fact that states do not wish to lose any autonomy on this politically sensitive matter.³¹ Meanwhile, some countries have restricted the conditions for admitting migrants on their territory, and less restrictive countries have had to deal with an increase of irregular immigrants³², making the latter also consider more stringent criteria. This evolution has been criticised as it has pushed immigrants further into illegality and has made

²⁵ Bauman, Z., *Globalization: the human consequences*, Polity Press, Cambridge, 1998, p. 88.

²⁶ For a comprehensive study on the criminalisation of migration and its effects, see: Commissioner for Human Rights, CommDH/IssuePaper(2010)1, Criminalisation of Migration in Europe: human rights implications, Strasbourg, February 2010, 51 p.

²⁷ Besters, M. and Brom, F.W.A., ‘Greedy’ information technology: the digitalization of the European Migration Policy, *European Journal of Migration and Law* (12) 2010, p. 461 and European Council on Refugees and Exiles, *Comments from the European Council on Refugees and Exiles on the European Commission proposal to recast the Dublin Regulation*, Brussels, April 2009, p. 3-4.

²⁸ Boeles, P., Den Heijer, M., Lodder, G. and Wouters, K., *European Migration Law*, Intersentia, Mortsel, 2009, p. 316.

²⁹ Guild, E., The Europeanisation of Europe’s asylum policy, *International journal of refugee law* (3-4) 2006, p. 640.

³⁰ Art. 63 of the Treaty of Amsterdam.

³¹ Although the immigration policy had fallen under the shared competence of the EU and the member states, the latter kept holding on to their chief role in the management of admissions, stay and inclusion of non-EU nationals. See also Guild, E., Carrera, S. and Eggenschwiler, A., *Informing the immigration debate*, May 2009, 4 p., WWW <www.ceps.eu>.

³² UNHCR, *The application of the “safe third country” notion and its impact on the management of flows and on the protection of refugees - background paper no. 2*, Geneva, May 2001, p. 2 and Vincent, E., Les nouvelles routes de la Méditerranée, *Le Monde*, 24 June 2010.

them prone to exploitation and crime.³³ A vicious circle is thus being created whereby irregular migrants are being involved in illegal activities, which additionally encourages member states to be even more restrictive towards migrants.³⁴ Thus, European asylum law took off primarily as a ‘flanking measure’, trying to manage the influx of migrants, while not necessarily improving the protection of refugees.³⁵ Although vast efforts have been made to improve migrants’ rights, EU states have by no means been always consistent with their human rights obligations in this field.³⁶

To regulate asylum claims, the EU developed the Dublin System as part of the CEAS. It consists of the Dublin and Eurodac Regulations and their two implementing regulations. Its goal is to determine the member state responsible for considering an asylum application and to apply the first safe country principle to asylum seekers within Europe. As such, an irregular migrant can be sent back to the member state which is designated to process his asylum claim, usually the country of first arrival.³⁷ By allowing detailed information exchange on the asylum claimant through use of the Eurodac database, the system prevents ‘asylum shopping’. EU officials stated at the start of the Dublin System that asylum claims in different countries would “flatten out over time” as asylum seekers realise that it is no longer possible to do ‘asylum shopping’. This has however proven to be untrue, as numbers of multiple asylum claims in EU member states have been rising steadily year after year, thus confuting the Dublin goals at least partially.³⁸ The Dublin System should also guarantee adequate protection to refugees and a fair burden on all member states.³⁹ This means that, where a member state already has examined or began examining an asylum application, it may be requested to take back the asylum seeker who finds himself irregularly in another member state.⁴⁰ The country where asylum seekers claim international protection is usually the first country through which they have entered the EU. As a result, member states which are at the external border of the EU have a higher chance of dealing with immigrants. This leads to individual member states making it more difficult to reach their territory⁴¹ or member states being unable to cope with

³³ European Council on Refugees and Exiles, *Comments from the European Council on Refugees and Exiles on the European Commission proposal to recast the Dublin Regulation*, Brussels, April 2009, p. 3-4.

³⁴ Broeders, D., *The new digital borders of Europe: EU databases and the surveillance of irregular migrants*, *International sociology* (22) 2007, p. 88 and Fortescue, A., *Combating illegal migration: from Tampere via Seville*, 2003, p. 1.

³⁵ Boeles, P., Den Heijer, M., Lodder, G. and Wouters, K., *European Migration Law*, Intersentia, Mortsel, 2009, p. 316.

³⁶ Guild, E., *The Europeanisation of Europe’s asylum policy*, *International journal of refugee law* (3-4) 2006, p. 643.

³⁷ Because all member states have ‘mutual trust’ in each other’s law system, EU member states presume each of them can be assumed to be a safe third country’. As such, they can send an irregular migrant back to the country of first arrival without checking the claim on its merits. However, in *T.I. v. the United Kingdom*, the European Court of Human Rights emphasised that sending T.I. back to Germany was a case of indirect refoulement and could expose him to inhuman treatment as opposed to art. 3 ECHR.

³⁸ Whereas in 2005, 16% of all asylum claims were cases of ‘asylum shopping’, this number rose to 17% in 2006, 17,5% in 2008 and 23,3% in 2009. Only in 2007 there was a 1% drop compared to the numbers in 2006.

³⁹ Council of the European Union, 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, 25 February 2003, OJ C 50/1.

⁴⁰ Although humanitarian considerations and asylum seekers’ preferences do play a role, EU member states clearly wanted to prevent asylum seekers travelling through Europe in order to seek asylum in the country of their choice.

⁴¹ For example, Italy signed a readmission agreement with Libya and the EU signed a readmission agreement with Ukraine, while conditions for refugees in Libya and Ukraine have been reported to be

the high number of migrants.⁴² These evolutions have put vast pressure on the Dublin System, forcing the European Commission to propose amendments to the Dublin and Eurodac Regulation to enhance the system's efficiency⁴³ and to ensure that the needs of applicants for international protection are better addressed.⁴⁴ These are currently still being discussed.

As the Dublin II Regulation lays down the criteria for determining the member state responsible for an asylum claim, there has to be an objective mechanism for ascertaining whether or not another member state is obliged to take care of an asylum claim, and this is where Eurodac comes into play. The Eurodac legislative process was decisively influenced by the Schengen group's ad hoc response to the refugee crisis of the end of the nineties, when thousands of Kurds from Iraq and Turkey crossed the external EU borders irregularly. The members of the Schengen Task Force expected that the Kurdish refugees were planning secondary movements within the Schengen area.⁴⁵ By means of the Eurodac regulations⁴⁶ a central European fingerprint database was set up, for the purpose of storing and comparing the fingerprints of all persons who apply for asylum and who irregularly cross borders. For people apprehended illegally in a member state, fingerprints are not stored in Eurodac, but only compared with the data already available in the database.⁴⁷ The system ultimately became operational in 2003. Eurodac is a hit/no-hit system, which means that sent data is automatically checked against other prints stored in the Eurodac Central Unit and that a notification will be given whenever there is a match. On the basis of this hit, member states may ask another member state to take over the irregular migrant. Eurodac is not only limited to EU member states, but is also being accessed by Iceland, Norway, Denmark and Switzerland. In addition to fingerprints of all persons of at least 14 years of age, Eurodac also stores information on the sex of a person, the EU country of origin, their reference number, the place and date of the asylum application or the apprehension of the person, the date on which the fingerprints were taken and the date on which they were transmitted to the Central Unit. This information is then kept for ten years in case of asylum applicants, or for two years in case of irregular border-crossers, unless they obtain citizenship or if, in case of the former

inhumane. See i.a. Human Rights Watch, *Buffeted in the Borderland - The Treatment of Asylum Seekers and Migrants in Ukraine*, 16 December 2010, 124 p., WWW <www.hrw.org>.

⁴² See European Court of Human Rights, *M.S.S. v. Belgium and Greece*, judgment, 21 January 2011, WWW <<http://cmiskp.echr.coe.int/tkp197/search.asp>>. Belgium was convicted for expelling an asylum-seeker to Greece as the conditions in Greece's detention centres among others violated article 3 (prohibition of inhuman and degrading treatment or punishment).

⁴³ For example, of the more than 55300 requests for transfer in 2006 only 16842 asylum applicants were actually transferred by the member states.

⁴⁴ Commission of the European Communities, COM(2008) 820, 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, p. 2.

⁴⁵ Aus, J.P., *EU governance in an area of freedom, security and justice: logics of decision-making in the justice and home affairs council - working paper No. 15*, October 2007, 50 p., WWW <www.arena.uio.no/publications>.

⁴⁶ 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, 15 December 2000, OJ L 316 and Council of the European Union, 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, 5 March 2002, OJ L 62.

⁴⁷ The Eurodac database was originally meant to cover asylum applicants only. However, during the negotiations i.e. Germany and Austria managed to broaden the scope *ratione personae*. For more information on the negotiations: Aus, J.P., *Eurodac: a solution looking for a problem?*, *European Integration online papers* (10) 2006, WWW <<http://www.eiop.or.at/eiop/index.php/eiop>> .

group, they receive a residence permit or have left the EU. Compliance with these rules is being monitored by the European Data Protection Supervisor on the EU level and by national supervisory bodies in the participating states themselves. The Eurodac database filled up rather quickly with fingerprints of asylum seekers, which made it able to contribute substantially to its primary goal: determine the member state responsible for an asylum seeker. Very noticeably, in practice the use of Eurodac has widened to include irregular border-crossers in a significant way. In the first years the Commission was disappointed that member states did not send much information to Eurodac concerning this category, whereas nowadays those transactions have increased faster than the ones concerning asylum seekers. As such, the Eurodac system is of increasing importance for the European fight against illegal immigration.⁴⁸ All in all, the Commission considers the Eurodac project very successful in terms of security, cost-effectiveness, speed, output and the prevention of asylum-shopping, year after year. However, Eurodac has been criticised on many points, not the least on data protection grounds, due to the fact that the Eurodac regulation does not take into account European data protection standards.⁴⁹ As a consequence, there has been disapproval of the fact that the EU is more concerned with preventing the leakage of information than ensuring that the records are correct and accurate.⁵⁰

2.3 The use of databases and the link with the EU security policy

The metaphor of Fortress Europe is often used to describe the multitude of measures taken to close the borders of the European Union for unwanted immigrants. Substantial investments like Frontex⁵¹ and the constant monitoring of the external borders prevent illegal migrants from entering European soil. However, because of the gradual realisation that borders alone cannot halt irregular migration, there has been a shift to internal migration control, using large-scale electronic surveillance systems such as the Schengen Information System (SIS), Eurodac and the Visa Information System.⁵² As identity papers are often absent, the EU counts on technology and the use of biometric data for identification. The inclusion of biometrics (primarily fingerprints) in databases and travel documents is often presented as the tool for numerous purposes: preventing illegal immigration, visa shopping, combating terrorism, etc.⁵³

Since there has been a substantial growth in the number of databases, the Commission is now pleading for the establishment of a supranational agency. This way productivity could be

⁴⁸ Broeders, D., The new digital borders of Europe: EU databases and the surveillance of irregular migrants, *International sociology* (22) 2007, p. 83 and the different reports from the Commission on the activities of the Eurodac central unit (SEC(2005) 839, SEC(2006) 1170, SEC(2007) 1184, COM(2009) 13, COM(2009) 494 and COM(2010) 415)

⁴⁹ Chalmers, D., Hadjiemmanuil, C., Monti, G. and Tomkins, A., *European Union Law*, Cambridge University Press, Cambridge, 2006, p. 642.

⁵⁰ Statewatch, *Statewatch bulletin vol. 3 no 1*, January-February 1993, p. 9, WWW <www.statewatch.org>.

⁵¹ Frontex is a European Union agency responsible for coordinating the activities of national border guards, thus ensuring the EU external borders' security. It has been criticised for not taking into account asylum and human rights concerns.

⁵² Broeders, D., *Ibid.*, p. 72.

⁵³ Brouwer, E., Data surveillance and border control in the EU - balancing efficiency and legal protection, in: Balzacq, T. and Carrera, S. (eds.), *Security versus freedom?: a challenge for Europe's future*, Ashgate, Aldershot, 2006, p. 139.

improved and costs could be reduced.⁵⁴ Although the Commission does not refer to it literally anymore, the original impetus for bringing different databases together was to ‘exploit the added value of the synergy between existing and future information systems as SIS II, VIS and Eurodac in the prevention and fight against terrorism’.⁵⁵ As biometric information is increasingly present in databases⁵⁶, the Commission also defends - completely in line with the Hague Programme⁵⁷ and again referring to the fight against terrorism and organised crime - the interoperability of the different systems and the access of security agencies to those systems. Even if it is recognised that databases like Eurodac and VIS hold personal information irrespective of real or suspected behaviour in the past, the querying of these databases to combat organised crime and terrorism is deemed justified, even if it concerns databases that have registered people with a clean criminal record.⁵⁸ The mere existence of the data stored in these systems tempts politicians and policy makers, especially in law enforcement, to use them for goals other than for which they have been constructed.⁵⁹ Essentially, there is an evolution towards the establishment of multiple databases and the intention to make them available later to security agencies, even though they originally served a different purpose (also often referred to as ‘mission creep’). As Florian Geyer points out, even though these systems are related to the area of freedom, security and justice, they address substantially different issues: migration, asylum and free movement on the one hand, and police and judicial cooperation in criminal matters, including counter-terrorism, on the other. A distinction between these issues is not only mandatory in terms of content (e.g. the movement of persons across borders is by itself neither a threat nor a crime), but also in regard to the institutional EU order under which these decisions were made.⁶⁰ Critical researchers like Guild argue that there is no direct relationship between refugees and asylum seekers coming to Europe and the risk of terrorism. If there were such a relationship, it would be indirect, a result of displacement of linkages made at the political level about security and

⁵⁴ Commission of the European Communities, COM(2009) 292 final, Communication from the Commission - Legislative package establishing an agency for the operational management of large-scale IT systems in the area of freedom, security and justice, 24 June 2009, p. 3.

⁵⁵ Council of the European Union, Draft council conclusions on access to Eurodac by Member State police and law enforcement authorities, 8688/07, Brussels, 20 April 2007, p. 1..

⁵⁶ Not only are the fingerprints being registered of an increasing number of categories of people, member states also wish to lower the minimum age from when fingerprints have to be taken. For example, the Council already requested to lower the age to six year old. The debate goes further as technology makes it increasingly possible to take reliable fingerprints from a younger age. On how technological means shapes policy instead of the other way around: Besters, M. and Brom, F.W.A., ‘Greedy’ information technology: the digitalization of the European Migration Policy, *European Journal of Migration and Law* (12) 2010, pp. 455-470.

⁵⁷ Council of the European Union, The Hague Programme: strengthening freedom, security and justice in the European Union, 3 March 2005, OJ C 53/7

⁵⁸ Commission of the European Communities, COM(2005) 597 final, Communication from the Commission to the Council and the European Parliament - on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs, 24 November 2005, p. 10.

⁵⁹ Broeders, D., The new digital borders of Europe: EU databases and the surveillance of irregular migrants, *International sociology* (22) 2007, p. 87 and 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 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], and on the Proposal for a Council Decision on requesting comparisons with EURODAC data by Member States’ law enforcement authorities and Europol for law enforcement purposes, 10 April 2010, OJ C 92/4.

⁶⁰ GEYER, F., *Taking stock: databases and systems of information exchange in the area of freedom, security and justice*, Centre for European Policy Studies, May 2008, p. 4, WWW <www.ceps.eu>.

borders.⁶¹ Because of this, official EU discourses often put irregular immigration into the same basket as a whole series of diverse insecurities, threats and criminalities, frequently justifying the adoption of policies calling for repressive responses centred on expulsion, detention and criminalisation measures.⁶² The increasing use of migration policies for counter-terrorism purposes has thus shifted the primary use of the criminal justice system for security purposes towards more administrative systems, which has been noted to provide insufficient protection for human rights.⁶³ Equally, privacy rights have been put under pressure to benefit extensive gathering and exchange of data.⁶⁴ It is within the framework of those two evolutions that a proposal for LEA access to Eurodac is possible.

* * *

*

⁶¹ Guild, E., International terrorism and EU immigration, asylum and borders policy: the unexpected victims of 11 September 2001, *in*: Carr, F. and Massey, A. (eds.), *Public policy and the new European Agendas*, Edward Elgar Publishing, Cheltenham, 2006, p. 233.

⁶² Carrera, S. and Merlino, M., *Assessing EU policy on irregular immigration under the Stockholm Programme*, Centre for European Policy Studies, 14 October 2010, p. 2, WWW <www.ceps.eu>.

⁶³ European Parliament - Directorate-general for external policies of the Union, *Current challenges regarding respect of human rights in the fight against terrorism*, Brussels, April 2010, p 3, 5.

⁶⁴ *Ibid.*, p. 5.

3. ON THE ACCESS BY LAW ENFORCEMENT AUTHORITIES AND EUROPOL TO EURODAC

“This is not a technical question, it is a political question of balance between security and the rights of individuals.”

- *Andrej Grošelj, Permanent Representation of the Republic of Slovenia to the EU*

“It is not only about balancing, it is also about legality and consumer rights. Security has a price.”

- *Paul De Hert, Professor at Vrije Universiteit Brussel*

The larger framework of the EU migration policy was given in the chapter above as to understand the complexity of migration and security measures within the European Union. The Commission’s proposal to open up Eurodac for law enforcement purposes is only one particular act in the light of the above and is said to be a political question rather than a technical one. This is because implementing the proposal is technically feasible, however a lot of criticism has been given on whether or not it would be detrimental to fundamental rights or undermine the positions of migrants. As such, it fits within the larger debate on security versus individual rights. In order to obtain a full picture and to test its compliance with existing legislation and jurisprudence, the proposal will be discussed on several grounds and will assess the merits of the critique given. First, an overview of how the proposal came to be will be given.

3.1 A short history of the proposal concerning LEA’s access to Eurodac

The proposal for access to Eurodac by law enforcement authorities and Europol is the result of a relatively long political process. As to better understand the dynamics behind the Commission’s proposals to open Eurodac for law enforcement purposes, a short look will be given at the negotiations concerning the proposals. Drawing up the proposal for LEA’s access took quite a while and it ran parallel to a more general reform of the Dublin II and Eurodac system which has equally been under discussion.

Every so often, the Ministers of the Interior of the six largest EU states - the G6 - meet informally to discuss further responses to terrorism, organised crime and illegal immigration. The idea behind this is that new proposals can be discussed more easily in a small committee. Subjects on which a common agreement is reached can then be put on the EU agenda. Therefore, the member states involved can substantially affect EU legislative process. At the G6-meeting of 22 and 23 March 2006 in Heiligendamm, the idea to grant police access to Eurodac was launched for the first time. Equally, the proposal to grant authorities responsible for internal security full access to VIS was advocated.⁶⁵ This is in line with the Hague Programme, which called for extending the access of law enforcement authorities to existing data filing systems of the European Union. Noticeable is that back at Heiligendamm, there is only a reference to police authorities and not to law enforcement authorities in general, the latter encompassing a much broader array of agencies. It is also remarkable that the Ministers

⁶⁵ House of Lords - European Union Committee, Behind closed doors: the meeting of the G6 Interior Ministers at Heiligendamm - Report with evidence - 40th report of session 2005-06, London, The Stationery Office, 19 July 2006, p 25.

do not yet regard data protection issues as important when discussing the exchange of information.⁶⁶ It is not clear which country was the driving force behind the proposal, as the G6 has no transparency obligation nor does it publish reports. However, during the first half of 2007 the German presidency lobbied strongly for a proposal to be drafted, while it also extended the scope of the proposal to law enforcement authorities and Europol⁶⁷. Although Belgium and Sweden expressed reservations (among others concerning data protection and timing) to the policy proposal, there was a clear political commitment of the member states. Consequently, the JHA Council asked the Commission to set up a legislative proposal as soon as possible in June 2007.⁶⁸

As time elapsed, the Commission drafted three proposals⁶⁹ amending the Eurodac Regulation, framing in the broader reform of the Dublin II system. While all three concerned the more general reform of Dublin II and Eurodac, only one of them contained provisions for granting LEA's access to Eurodac.⁷⁰ The first proposal for an amended Eurodac regulation was presented by the Commission in December 2008, which then referred it to the European Parliament. The latter then adopted a resolution in which it directed the Commission to take into account a number of amendments. The second Eurodac proposal of the Commission took into account some of the proposals of the European Parliament, but also introduced the possibility for member states' LEA's to access Eurodac in relation to 'the prevention, detection and investigation of terrorist offences and other serious criminal offences'. The arrangement for LEA's access was however received critically by the European Parliament

⁶⁶ *Ibid.*, p. 10-11.

⁶⁷ After discussing the German proposal in the Article 36 Committee (CATS), all subsequent documents refer to 'access to Eurodac by law enforcement authorities and Europol'.

⁶⁸ Council of the European Union, Draft council conclusions on access to Eurodac by Member State police and law enforcement authorities, 8688/07, Brussels, 20 April 2007, 3 p., Council of the European Union, Policy document concerning access to Eurodac by Member State's police and law enforcement authorities, 16982/06, Brussels, 20 December 2006, 3 p. and Council of the European Union, Draft council conclusions on access to Eurodac by Member State police and law enforcement authorities as well as Europol, 10002/07, Brussels, 25 May 2007, 3 p.

⁶⁹ Commission of the European Communities, Proposal for a regulation of the European Parliament and 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, 60 p., Commission of the European Communities, COM(2009) 342, 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] (Recast version), 10 September 2009, 74 p., Commission of the European Communities, COM(2009) 344 final, 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, 21 p. and Commission of the European Communities, COM(2010) 555, Amended proposal for a regulation of the European Parliament and 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), 11 October 2010, 70 p.

⁷⁰ The other main changes proposed in the new Eurodac Regulations are 1) the extension of the scope of Eurodac to cover applications for subsidiary protection (parallel to the provisions in the European Qualification Directive, part of the CEAS, also regulating the applications for subsidiary protection), 2) provisions for the operational management of Eurodac by a new IT management authority, 3) strict 72-hours deadlines for transmitting fingerprint information and 4) additional data protection safeguards.

(which recently asked the Commission on February 11th to confirm that Eurodac would not be used for other purposes than originally intended), national parliaments and numerous NGO's. This led the ministers of justice and home affairs to '*voice their disappointment that the provisions for law enforcement access to the Eurodac data had been omitted from the latest Commission proposal*'.⁷¹ Nevertheless, the Council never substantially refuted the arguments made by the parliaments and NGO's. Not to jeopardise the general reform of the Dublin II system, the European Commission left out the provisions on LEA's access from the third Eurodac reform proposal.⁷² This omission is however not permanent: Austria (backed by 9 other member states) insisted that LEA's access to Eurodac should be presented again as it saw the important tool to combat crime.⁷³ The Commission agreed to propose it again by 2012. By then the European Parliament will have full co-decision powers over the proposal, which makes it rather unlikely that the proposal, as it is now envisaged, will be accepted in its current form.

3.2 What do the proposals say?

The proposals to open up Eurodac for law enforcement purposes were a combination of first and third pillar policies. The Commission therefore drafted both a regulation (COM(2009) 342) as well as a council decision (COM(2009) 344). While the proposed regulation only contains minimal references to law enforcement agencies (mainly article 3 and some statements in the preamble), most of the details have been elaborated in the council decision as it concerns co-operation in criminal matters. The first pillar regulation introduces a 'bridging clause'⁷⁴ to allow access for law enforcement purposes by providing a link with the third pillar council decision. Both proposals will be scrutinised further, although the council decision will get most of the attention as it contains most of the provisions on LEA's access.

The proposals basically allow law enforcement agencies and Europol to access Eurodac's database for the comparison of fingerprints. As a result, when a fingerprint is in their possession, they can retrieve information concerning that fingerprint from Eurodac, for instance a person's reference number, sex, member state of origin, the date on which the fingerprints were taken, etc. If a fingerprint is recognised in Eurodac, a person consulting Eurodac should be able to identify the person to whom it belongs. As this means that information is retrieved from people with a clean criminal record, the proposal contains certain thresholds. Consequently, it can only be consulted if querying Prüm⁷⁵ returns no result and only for the prevention, detection and investigation of 32 offences, listed in the European

⁷¹ Council of the European Union, Press release - 3043rd Council meeting - Justice and Home Affairs, 15848/10, Brussels, November 2010, p. 9.

⁷² House of Commons - European Scrutiny Committee - Seventh Report of Session 2010-11, HC 428-vii, The stationery Office, London, 23 November 2010, p. 33.

⁷³ Council of the European Union, Outcome of proceedings of CATS on 25 and 26 October 2010, 16006/10, Brussels, 9 November 2010, p. 2.

⁷⁴ Article 3 of the 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] (Recast version), COM(2009) 342, 10 September 2009, 74 p.

⁷⁵ The Prüm agreement enables member states to automatically exchange data (fingerprints, DNA, vehicle registration data) by directly accessing each other's databases. As such, when one query is launched, the databases of all other member states are searched.

Arrest Warrant framework decision.⁷⁶ In spite of efforts taken by the Commission, the proposal has met criticism from different international organisations, parliaments and NGO's. Those comments have been made due to conflicts of legal origin, such as non-conformity with the principle of legality. Equally, some comments stem from different perspectives on the matter taken by the actors involved: police organisations are more concerned with crime-fighting whereas refugee organisations prioritise the integration of refugees in society.

The following paragraphs will examine the critique given on the proposal, finding a balance between the different points of view given by the stakeholders involved. Four main issues arise regarding the proposal to grant LEA's access to Eurodac: (1) motivation, (2) data protection, (3) stigmatisation of asylum seekers and (4) the quality of Eurodac data.

(1) *Motivation*: the Commission, law enforcement agencies and the Council have given reasons to open up Eurodac for law enforcement purposes. A closer look will be taken at the factual basis of these arguments.

(2) *Data protection*: the handling of personal data is prone to data protection rules. The proposal will be checked against a.o. the principle of necessity and proportionality, the purpose limitation rule and effective control on the data. This is especially relevant considering that an updated EU data protection regime will be established soon, with an even stricter purpose limitation approach.

(3) *The stigmatisation of asylum seekers*: asylum seekers have become linked with terrorism and serious crime in popular perception. Jurisprudence has nonetheless stressed that this link has not sufficiently been established and that similar actions which focus on asylum seekers have a stigmatising effect. The arguments of the Commission will be weighed against those previous court rulings.

(4) *Quality of Eurodac Data*: the usefulness of fingerprints to combat crime has been acknowledged. However, this is only the case if the data is of sufficient quality and if false recognition rates are low. This paragraph will examine whether or not this applies to Eurodac.

3.3 Motivating the proposal

The motives for granting LEA's access to Eurodac have been enumerated in the Commission proposal and have been elaborated to some extent in the impact assessment⁷⁷

⁷⁶ These are: participation in a criminal organisation; terrorism; trafficking in human beings; sexual exploitation of children and child pornography; illicit trafficking in narcotic drugs and psychotropic substances; illicit trafficking in weapons, munitions and explosives; corruption; fraud; laundering of the proceeds of crime; counterfeiting; computer-related crime; environmental crime; facilitation of unauthorised entry and residence; murder; grievous bodily injury; illicit trade in human organs and tissue; kidnapping; illegal restraint and hostage-taking; racism and xenophobia; organised or armed robbery; illicit trafficking in cultural goods; swindling; racketeering and extortion; counterfeiting and piracy of products; forgery of administrative documents and trafficking therein; forgery of means of payment; illicit trafficking in hormonal substances and other growth promoters; illicit trafficking in nuclear or radioactive materials; trafficking in stolen vehicles; rape; arson; crimes within the jurisdiction of the International Criminal Court; unlawful seizure of aircraft/ships; sabotage.

⁷⁷ Commission of the European Communities, SEC(2009) 936, Commission staff working document - Accompanying document to the amended proposal for a regulation of the European Parliament and 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) and to the proposal for a Council Decision on requesting comparisons with EURODAC data by Member States' law enforcement

accompanying the proposal. They will be further discussed hereunder, complementing the arguments with irrefutable or negative evidence.

The overarching reason to open up Eurodac for law enforcement purposes is its necessity to **prevent, detect and investigate terrorism and other serious criminal offences**.⁷⁸ Additionally it is positioned as the only timely, accurate, secure and cost-efficient way to do this. This was previously pointed out at the JHA Council of 12-13 June 2007, where access to Eurodac was defined as necessary to fully achieve the aim of improving security and to enhance the fight against terrorism. Similar conclusions can be drawn based on the results of a questionnaire that was sent to Europol and all states participating in Eurodac, in which a great majority of respondents confirmed that *'access to Eurodac, even only on the basis of ten finger prints, would be of great use for police [...]'*.⁷⁹ An efficient exchange of information is indeed essential to investigate transnational crime in the European Union. This is especially the case when addressing serious crime, such as listed in the European Arrest Warrant, because this has a more significant impact on people's life. It's an established fact that access by law enforcement authorities to any significant and reliable biometrical database would lead to a more efficient way of identifying persons related to a criminal case.

There are however two points of discussion regarding this motivation for the LEA's access to Eurodac: (1) if fingerprints regarding only a certain group of people are checked, there have to be compelling reasons why this certain group is targeted or the proposal would be discriminatory and (2) similar databases have not yet proven to be cost-efficient, nor have they demonstrated that they are able to significantly reduce serious crime, including terrorism.

(1) If LEA's would only like access to the identity data of a specific group of people, there should be convincing reasons for only addressing that group, *in casu* asylum seekers. If it cannot be proven that this group is more likely to be involved in terrorism or serious crime, one cannot argue that access to their biometrics is more necessary than of any other group. As such, a differential treatment is allowed, but it has to be based on concrete facts. Otherwise law enforcement authorities should advocate access to information from every individual, regardless of the fact that he or she is an asylum seeker.

Data on crime and asylum seekers point in different directions. A report⁸⁰ of the British Association of Chief Police Officers, which coordinates the direction and development of the police service, has found no evidence that asylum seekers are more likely than anyone else in the community to commit criminal offences, and that asylum seekers are more prone to be the victims of crime than to be the perpetrators. These data do not indicate that asylum seekers are any more likely to be terrorists than non-asylum seekers. David Blunkett, Secretary of State for the Home Department, said that *"we should not assume that asylum seekers are any more likely to be terrorists than anyone else"*. Similarly, the European Commission declared in a 2005 communication that: *the claiming of asylum [does not indicate] in any way that a hitherto innocent individual will commit a criminal or terrorist act. [...] whilst the storage of*

authorities and Europol for law enforcement purposes - Impact assessment, Brussels, 10 September 2009, p. 59 p.

⁷⁸ Preamble (2) and article 1 of the Proposal for a Council Decision on requesting comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes, COM(2009) 344, 21 p.

⁷⁹ Commission of the European Communities, SEC(2009) 936, *o.c.*, p. 41.

⁸⁰ Association of Chief Police Officers of England, Wales and Northern Ireland, Asylum Seekers Policing Guide, 2001.

*personal data in criminal databases is justified due to past and real or suspected behaviour of the individual (which must be substantiated), this is not the case for EURODAC [...].*⁸¹ On the other hand countries like Germany, Austria and the Netherlands indicate that there is a significant crime rate of asylum seekers.⁸² In a discussion on those numbers with an Austrian official, I have been informed that those numbers do not only concern terrorism or serious crimes, but all forms of crimes, which means that no conclusions can be drawn from the numbers reported by Austria on whether or not access to Eurodac would be legitimate for terrorism and serious crimes. It seems as if no conclusive evidence can be given as to induce whether or not asylum seekers would be involved more in terrorism and serious crime. The European Data Protection Supervisor, a EU institution which monitors and advises EU bodies on the lawful processing of individuals' personal data, highlights that the sharing of personal information should always be based on clear and irrefutable arguments.⁸³ This does not seem to be the case and it is therefore difficult to state that only the fingerprints of asylum seekers are necessary, without demanding those of other people. In its Hüber-case⁸⁴, the European Court of justice dealt with similar facts, with this difference that it regarded the discrimination of other EU states' citizens compared to a state's own nationals. The case concerned a centralised German register, which contained certain personal data relating to foreign nationals – both EU citizens and non-EU citizens alike. These data were used to different ends, *inter alia* to apply the legislation relating to the right of residence, for statistical purposes and for the purposes of fighting crime. There was no comparable database for German nationals. The systematic processing of personal data relating only to nationals of other Member States for the purposes of fighting crime was ruled to be discrimination on the ground of nationality which is prohibited by Article 12 EC. Advocate General Maduro declared *“Indeed, law enforcement and the combating of crime could, in principle, be a legitimate public policy [...]. What member states cannot do, though, is to invoke it selectively, that is, against EU nationals living in their territory, but not against their own citizens. If a central register is so important for effective general policing, it should obviously include everyone living within a particular country regardless of his/her nationality. It is not open to national authorities to say that fighting crime requires the systematic processing of personal data of EU citizens but not of that relating to nationals. This would be tantamount to saying that EU nationals pose a greater security threat and are more likely to commit crimes than citizens, which, as the Commission points out, “is completely unacceptable”.* Similar fingerprint information as contained in Eurodac on non-suspect individuals is however not available on any other group in society⁸⁵, while information on criminal foreigners will already be accessible by other means (e.g. via SIS II or Prüm). EU measures or policies in the

⁸¹ Commission of the European Communities, COM(2005) 597 final, Communication from the Commission to the Council and the European Parliament - on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs, 24 November 2005, p. 10.

⁸² Commission of the European Communities, SEC(2009) 936, Commission staff working document - Accompanying document to the amended proposal for a regulation of the European Parliament and 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) and to the proposal for a Council Decision on requesting comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes - Impact assessment, Brussels, 10 September 2009, p. 8.

⁸³ European Data Protection Supervisor, *o.c.*, OJ C 92/3.

⁸⁴ European Court of Justice, Case C-524/06 (Heinz Huber v. Bundesrepublik Deutschland), preliminary ruling, 16 December 2008, WWW

<<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62006J0524:EN:NOT>>.

⁸⁵ European Data Protection Supervisor, *o.c.*, OJ C 92/5.

field of Freedom, Security, and Justice should not be based on the general presumption that migrants within the EU are to be treated as suspected terrorists. Such a policy would run against the general accepted principles in EU law of non-discrimination and equality.⁸⁶ The Meijers Committee also points out that access of LEA's to Eurodac could be deemed unlawful by the European Court of Human Rights under article 14 of the ECHR, which points out that 'enjoyment of the rights and freedoms [...] shall be set forth without discrimination on any ground such as race, [...], national or social origin, [...] or other status'. The exclusive storage and use for law enforcement purposes of fingerprints of individuals who apply for asylum in one of the EU member states is to be considered contrary to article 14.⁸⁷

(2) Multiple studies have indicated that using similar databases for law enforcement purposes is not a cost-efficient way for lowering terrorism and serious crime. Hobbing & Koslowski, for example, have examined the US-VISIT programme, which registers incoming travellers to the US. When it became known in the USA that several terrorists were non-US citizens whose legal residence in the US had expired, the US-VISIT programme was developed and law enforcement agencies gained access thanks to the approval of the US Patriot Act. When measuring the results it had produced against its purpose, they found that between 2004 and 2008 about 113 million immigrants had been registered in the information system. In this period, more than 1800 individuals were stopped entering the USA with the help of US-VISIT. Taking into consideration that throughout the year 2009 the US-VISIT programme had cost about \$ 2 billion, each suspect that was stopped at the border cost over \$ 1 million. They concluded that the system has only proven to be expensive, with no apparent security gain.⁸⁸ Similar observations have been made with regard to SIS: the number of hits based on third country nationals is considered relatively small compared to the storing of information on such a large group.⁸⁹ It has been argued that the expected positive effects of biometrics should be more explicitly balanced against the estimated rate of false recognition and the possibility of misuse. Nevertheless, it must be said that the results of SIS and the US-VISIT programme can also be attributed to the poor quality of the data, while the content of Eurodac is considered to be superior. SIS I holds incorrect identities and other data and additionally contains no photos or fingerprint information, which makes identification rather difficult, e.g. in case someone holds the same name or if identity theft has taken place.⁹⁰ On the other hand, the US-VISIT programme has been criticised for using 'bloated and inaccurate' watch lists. Contrary to this, Eurodac is regarded as a quality database.⁹¹

⁸⁶ Standing Committee of experts on international immigration, refugee and criminal law, Note on the proposal of the JHA Council to give law enforcement authorities access to Eurodac, CM0712-IV, Utrecht, 18 September 2007, p. 1.

⁸⁷ Standing Committee of experts on international immigration, refugee and criminal law, The amended proposal for the Eurodac Regulation (COM (2009) 342) and the Decision on requesting comparisons with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (COM (2009) 344), CM0910, Utrecht, 30 December 2009, p. 8.

⁸⁸ Besters, M. and Brom, F.W.A., 'Greedy' information technology: the digitalization of the European Migration Policy, *European Journal of Migration and Law* (12) 2010, p. 467-468 and Bigo, D., Carrera, S. and Guild, E., *What future for the area of freedom, security and justice? Recommendations on EU migration and borders policies in a globalising world*, March 2008, p. 2, WWW <www.ceps.eu>.

⁸⁹ Brouwer, E., Data surveillance and border control in the EU - balancing efficiency and legal protection, in: Balzacq, T. and Carrera, S. (eds.), *Security versus freedom?: a challenge for Europe's future*, Ashgate, Aldershot, 2006, p. 150.

⁹⁰ For an image of SIS I data extracts: see the slides presented at the ERA conference on information exchange of Reinhard Schmid, working at the Austrian Ministry of the Interior: <http://www.era.int/upload/dokumente/12315.pdf>, p. 78.

⁹¹ House of Lords - European Union Committee, *The Treaty of Lisbon: an impact assessment - volume II: evidence - 10th report of session 2007-08*, The Stationery Office, London, 13 March 2008, p. E47.

An additional remark has been made regarding planned terrorist offences or serious crimes. Although it concerns established law enforcement practices in the US, it similarly applies to the proposal to open up Eurodac for law enforcement purposes. LEA's access to Eurodac will be an additional obstacle to foreign terrorists wishing to enter the EU, but is unlikely to catch many of them. 'Established terrorists' who suspect that they may become involved in a criminal investigation are unlikely to provide their biometric data that may lead to their apprehension. Those are more likely to try to circumvent Eurodac, e.g. by travel document or ID fraud.⁹²

LEA's access to Eurodac also raised suspicion on whether or not data mining techniques could be applied in order to find 'matches' against certain suspicious profiles, similar as was envisaged by the EU-PNR system.⁹³ These methods inevitably lead to actions against large numbers of innocent people and are non-democratic due to the high numbers of false positives and false negatives.⁹⁴ Although initially ten member states were in favour of mass comparisons⁹⁵, this technique has been expressly forbidden in the proposal⁹⁶: the Commission's proposal only allows for fingerprint data to be checked in specific cases (although this requirement is less strict for Europol) and on a hit/no-hit basis.

The proposal also mentions a second reason for granting LEA's access to Eurodac. The explanatory memorandum states that **law enforcement authorities already have direct or indirect access to their own national databases containing fingerprints of asylum seekers** for the purpose of fighting crime. Granting LEA's access to Eurodac therefore only extends the territorial application of an existing practice. 13 participating states notified the European Commission through the questionnaire that their LEA's had access to fingerprints of asylum seekers. Three of them keep those fingerprints in a database together with other third country nationals, while eight states keep them in their national fingerprint database.⁹⁷ Regrettably, no

⁹² Koslowski, R., *Real challenges for virtual borders: the implementation of US-VISIT*, Migration Policy Institute, June 2005, p. 25.

⁹³ European Parliament, Resolution on the fight against terrorism, P6_TA(2007)0612, 12 December 2007, Strasbourg, WWW. <<http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P6-TA-2007-0612&language=EN>>.

⁹⁴ False positives are innocent people identified as suspects, where false negatives are real criminals which are not identified. See Commissioner for Human Rights, CommDH/IssuePaper(2008)3, Protecting the Right to privacy in the fight against terrorism, Strasbourg, 4 December 2008, p. 4-5.

⁹⁵ Commission of the European Communities, SEC(2009) 936, Commission staff working document - Accompanying document to the amended proposal for a regulation of the European Parliament and 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) and to the proposal for a Council Decision on requesting comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes - Impact assessment, Brussels, 10 September 2009, p. 42.

⁹⁶ Preamble (11) of the Proposal for a Council Decision on requesting comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes, COM(2009) 344, 21 p.

⁹⁷ Commission of the European Communities, SEC(2009) 936, Commission staff working document - Accompanying document to the amended proposal for a regulation of the European Parliament and 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) and to the proposal for a

further details have been given on which states are concerned as to examine the conditions under which access is allowed. Access to those documents has been refused by the Commission.⁹⁸ Research by Vogel et. al. and French parliamentary documents reveal that Germany has the most developed system regarding access to immigrants data, including asylum seekers status databases. A certain number of data is readily accessible, while more detailed data can be obtained under certain conditions.⁹⁹ Other countries such as France prohibit access to asylum seekers data by law enforcement authorities, as this has been deemed unconstitutional by the Constitutional Council.¹⁰⁰ The latter stated in a 1997 decision that “*The confidential treatment of information held [...] on applicants for refugee status in France is a vital guarantee of the right of asylum, a principle of constitutional status. [Access to this information] thus removes this constitutional guarantee [...]*”.¹⁰¹ Even though a large number of countries allow access to their asylum database, conditions for this differ between states. Although the threshold for access to Eurodac would be limited to serious crime, this might lower the minimum standards applicable in some EU countries for access to its asylum seekers’ data. In the case of France there are even greater complications, as this access has been prohibited as a matter of constitutional guarantees. Action taken at the EU level would thus undermine legal guarantees offered to asylum seekers, granted to them as they are a group in need of special protection.¹⁰² If no action is taken on the EU-level, it is likely that only a certain number of member states will share their data on asylum seekers. According to prof. Paul De Hert, the principle of subsidiarity should be complied with more stringently, therefore preventing that everything is put on the EU agenda, while those measures too often do not accord with national legislation.¹⁰³ Priority could be given at transnational projects, only encompassing a ‘coalition of the willing’. The Commission does not agree with this opinion though, as it states that “*action undertaken by member states alone is likely to be prohibitively expensive and disproportional*”.¹⁰⁴

Concrete: The reasons enumerated in the proposal certainly both have their merits. Nonetheless, the question is whether or not those arguments have been compared enough with other legitimate interests. Firstly, the use of Eurodac to prevent, detect and investigate

Council Decision on requesting comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes - Impact assessment, Brussels, 10 September 2009, p. 47.

⁹⁸ Under Regulation No 1049/2001 (OJ L 145, 31 December 2001) the public can request access to European Parliament, Council and Commission documents. Access to the documents has been denied under art. 4(3) for the reason that “*disclosure of this information would seriously undermine the Commission's decision-making process*”.

⁹⁹ Vogel, D., McDonald, W., Düvell, F., Jordan, B., Kovacheva, V. and Vollmer, B., Police Cooperation in Internal Enforcement of Immigration Control: Learning from International Comparison. In: McDonald, W. (ed.), *Immigration, Crime and Justice. Sociology of Crime, Law and Deviance* (13) 2009, Emerald, p. 207-244 and Assemblée Nationale - Commission des affaires européennes, Rapport d'information sur la deuxième phase de mise en œuvre du régime d'asile européen commun, 15 December 2009, p. 23-24.

¹⁰⁰ Assemblée Nationale - Commission des affaires européennes, *o.c.*, p. 23-24.

¹⁰¹ French Constitutional Council, Decision 97-389, Act making various provisions in respect of immigration, No. 26, 22 April 1997, WWW <<http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/97389DCa97389dcpdf>>.

¹⁰² Assemblée Nationale - Commission des affaires européennes, *o.c.*, p. 24.

¹⁰³ Speech by prof. Paul De Hert on the subject ‘No access for law enforcement to Eurodac - A lost opportunity?’ at “SIENA, Prüm, SIS II, VIS, Eurodac - Law enforcement and information exchange in the EU today”, conference organised by ERA, the Academy of European Law in Trier on May 19th and 20th 2011.

¹⁰⁴ Explanatory memorandum of the 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, p. 7.

terrorism and other serious crimes could pay off. However, the proposals do not bring forward sufficient proof to allow a differential treatment of asylum seekers compared to non-asylum seekers. Indeed, the Commission declared that an asylum claim does not indicate in any way that a hitherto innocent individual will commit a criminal or terrorist act. Only allowing access to asylum seekers' biometrics but not equally demanding access to regular citizens' fingerprints is in contrast with the principle of non-discrimination and equality. The remarks on the cost-efficiency of LEA's access to Eurodac are more nuanced. Although similar databases have proven to be resource intensive, Eurodac should be more efficient as it is a more qualitative database. Nonetheless, terrorists and criminals might quickly find ways to evade Eurodac, diminishing the use of LEA's access to Eurodac quickly. Secondly, the fact that law enforcement authorities already have access to asylum seekers' fingerprints in certain countries should not be a reason to impose this on others, certainly when this has been deemed unconstitutionally earlier. A stricter interpretation of the subsidiarity rule has been advocated.

3.4 Concerns on data protection

Data protection is a broad concept and linked with the right to privacy, thus with article 8 of the European Convention on Human Rights (ECHR) and article 6 of the Charter of Fundamental Rights of the European Union (CFREU), which now has binding legal status due to the ratification of the Lisbon Treaty.¹⁰⁵ The latter also accounts for the fact that the pillar structure has been abandoned. Because ever-developing technology changes the way data can be collected, processed and protected, the European Commission is preparing a uniform data protection regime for the whole European Union, ensuring that all legislation has to respect the same data protection standards.¹⁰⁶ Data protection is also increasingly seen as a *sui generis* right¹⁰⁷, as illustrated by article 8 of the CFREU (protection of personal data). Collecting and processing personal data interfering with an individual's private life can therefore only be conducted within the limits of these provisions, meaning that the data should be accurate, adequate, relevant and not excessive in relation to the purpose for which they are stored.¹⁰⁸ Further, personal data should be obtained fairly and lawfully, which means no privacy infringing methods should be used, unless legally allowed and necessary to protect a certain interest. Neither should it be processed for undefined or unspecific aims, nor for purposes incompatible with the purpose the data were gathered for originally. Finally, the storage of the data should not be used longer than necessary for the purpose the data were stored for.¹⁰⁹

¹⁰⁵ European Union Agency for Fundamental Rights, *Data Protection in the European Union: the role of national data protection authorities - strengthening the fundamental rights in the EU II*, Publications Office of the European Union, Luxembourg, 2010, p. 18.

¹⁰⁶ Commission of the European Communities, COM(2010) 609 final, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of Regions - A comprehensive approach on personal data protection in the European Union, 4 November 2010, p. 13.

¹⁰⁷ Commissioner for Human Rights, CommDH/IssuePaper(2008)3, Protecting the Right to privacy in the fight against terrorism, Strasbourg, 4 December 2008, p. 5.

¹⁰⁸ Article 5 of the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data, ETS No. 108, Strasbourg, 28 January 1981.

¹⁰⁹ Article 2, c), *Ibid.* and De Busser, E., *Data Protection in EU and US Criminal Cooperation, a substantive law approach to the EU internal and transatlantic cooperation in criminal matters between judicial and law enforcement authorities*, Maklu, Antwerpen, 2009, p. 22.

Data protection encompasses different rules which have to be followed when collecting and processing personal data, i.e. the proportionality, necessity and subsidiarity of provisions on the use and collection of personal data, effective control on the access to this data and purpose limitations on the use of the data. The provisions on LEA's access in the proposals specifically refer to the Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters, the data protection framework applicable in the former third pillar.¹¹⁰ Nevertheless, when the new proposal for LEA's access will be presented by the Commission, a different legal instrument will be referred to as the old one denotes pillar-specific data protection rules.

3.4.1 The principle of legality, purpose limitations and function creep

The purpose limitation rule has been recognised as being part of a sound data protection regime. It can be found from as early as 1981 in art. 5 of the Council of Europe's Data Protection Convention¹¹¹, and has been repeated in subsequent agreements, including on the EU level, such as the Data Protection Directive¹¹² or the Framework Decision 2008/977/JHA mentioned above. It defines what can be done with personal data that have been collected for the purpose of a particular procedure or action. It is possible that the use of these data remains within the original set of rules for which the data have been collected. Personal data gathered for a specific purpose can also be used for different purposes, governed by other privacy standards. Because the conflicting data protection rules can result in a decline of the (privacy) protection offered to the data subject, the use for other purposes than those the data were collected for, should be limited.¹¹³ Particularly, the collection of personal data for administrative purposes and subsequently using them in the context of criminal proceedings means the data subject loses the protection normally received under article 6 of the European Convention on Human Rights, which ensures him or her a fair trial when data has been collected for the purpose of criminal proceedings.¹¹⁴ As such, when personal data are used for judicial purposes, more specifically in a criminal procedure, additional safeguards should enter into force.

To begin with, a change of purpose can only be permitted if there is sufficient legal basis allowing the new purpose. The Eurodac Regulation currently contains **no sufficient legal basis** to allow LEA's access to the Eurodac database. The European Commission itself recognised, when it developed SIS II, that it is necessary to identify the appropriate legal

¹¹⁰ Preamble (12) and article 10 of the 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, 21 p.

¹¹¹ Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data, Council of Europe, 28 January 1981, ETS no. 108. Article 5 reads as follows: '*Personal data undergoing automatic processing shall be: a) obtained and processed fairly and lawfully; b) stored for specified and legitimate purposes and not used in a way incompatible with those purposes; c) adequate, relevant and not excessive in relation to the purposes for which they are stored; d) accurate and, where necessary, kept up to date; e) preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.*'

¹¹² 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, 23 November 1995, OJ L 281.

¹¹³ De Busser, E., *Data Protection in EU and US Criminal Cooperation, a substantive law approach to the EU internal and transatlantic cooperation in criminal matters between judicial and law enforcement authorities*, Maklu, Antwerpen, 2009, p. 23.

¹¹⁴ *Ibid.*, p. 23-24.

instruments in the treaties, in order to develop systems which combine police and judicial co-operation in criminal matters (which was covered by Title VI of the Treaty of the EU, the so-called third pillar) and the policy regarding visas, immigration and free movement of people (which was covered by Title IV of the EC Treaty, part of the so-called first pillar).¹¹⁵ At the time of the first LEA's access proposal Germany was not sure if new legal provisions had to be created for granting LEA's access to Eurodac.¹¹⁶ The legal service of the Council rightly informed the German presidency in 2007 that this was essential to comply with the principle of legality. A first pillar regulation amending the original Eurodac Regulation containing a 'bridging clause' to a new third pillar council decision was subsequently prepared, so providing a legal basis. With the Lisbon Treaty having entered into force, a different legal instrument will be needed. The preamble¹¹⁷ of the proposed Eurodac Regulation, which is the first pillar instrument that contains provisions for LEA's access, still only refers to article 63(1)a of the EC Treaty¹¹⁸ as its legal basis, which does not in any way refer to law enforcement goals. Security goals cannot be deemed to be covered by provisions which refer to the 1951 Geneva Refugee Convention and its 1967 Protocol.¹¹⁹ It is true that the proposed Council Decision for LEA's access (the third pillar instrument) does refer to article 30(1)(b) and 34(2)c of the Treaty on European Union¹²⁰ on law enforcement co-operation. However, Eurodac itself remains a database for managing asylum within the EU, as the treaty provisions to which it refers to legitimise its purpose are not enlarged. Therefore, the legal basis for allowing access to Eurodac for other purposes than those mentioned in article 63(1)(a) of the EC Treaty is insufficient.¹²¹ It is only in the proposed third pillar Council Decision that referral is made to treaty provisions concerning law enforcement, stating that the data will be used for EU law enforcement obligations. This does not change the fact that the collection of data for Eurodac has a different purpose. Consequently, a sufficient legal basis for using the data for criminal investigations afterwards is lacking. It is not sufficient for the European Commission to refer to parallel trends concerning LEA's access to SIS II and VIS for security purposes as good precedents for the extension of the purpose of Eurodac, exactly because SIS II and VIS have a different legal basis and

¹¹⁵ Commission of the European Communities, COM(2001) 720 final, Communication from the Commission to the Council and the European Parliament - Development of the Schengen Information System II, Brussels, 18 December 2001, p. 13-14.

¹¹⁶ Council of the European Union, Policy document concerning access to Eurodac by Member State's police and law enforcement authorities, 16982/06, Brussels, 20 December 2006, p. 3.

¹¹⁷ Commission of the European Communities, COM(2009) 342, 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] (Recast version), 10 September 2009, p. 14.

¹¹⁸ Because of the Lisbon Treaty, the different treaties were restructured. The provisions mentioned can now be found back in article 78 of the TFEU.

¹¹⁹ Standing Committee of experts on international immigration, refugee and criminal law, Proposal to give law enforcement authorities access to Eurodac, CM0714, Utrecht, 6 November 2007, p. 1.

¹²⁰ Same remark as above on the Lisbon Treaty implications. The provisions can now be found back in article 87 and 88 of the TFEU.

¹²¹ House of Lords - European Union Committee, Behind closed doors: the meeting of the G6 interior ministers at Heiligendamm - Report with evidence - 40th report of session 2005-06, The Stationery Office, London, 19 July 2006, p. 10, House of Lords - European Union Committee, Prüm: an effective weapon against terrorism and crime? - Report with evidence - 18th report of session 2006-07, The Stationery Office, London, 9 May 2007, p. 16 and European Parliament, Resolution on the fight against terrorism, P6_TA(2007)0612, 12 December 2007, Strasbourg, WWW.

<<http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P6-TA-2007-0612&language=EN>>.

accordingly another purpose.¹²² It is likely that, now the Lisbon Treaty has been agreed on, the European Court of Justice upholds a similar decision as it did concerning the Council Decision on the conclusion of the Passenger Name Record (PNR) Agreement of 17 May 2004. Then, the ECJ annulled the Council Decision on the sole basis that it could not be adopted on the legal basis of article 95 EC.¹²³

Moreover, disregarding the insufficient legal basis provided for in the proposals, actions on the EU level are limited to the purpose described in the relevant legislation. In the case of Eurodac, article 1(1) of the Eurodac Regulation strictly limits the purpose to the determination of the member state responsible for an asylum claim. To remedy this restriction, a new, broader, **purpose limitation** has been incorporated in the LEA's access proposals. The European Commission was well aware that this LEA's access had to be limited as not to constitute a breach of data protection rules and the right to privacy.¹²⁴ Therefore, access to Eurodac is limited to specific cases, when necessary and proportionate in a democratic society. The necessity and proportionality will be discussed in the subsequent paragraph, while the limitation to specific cases will be reviewed here. According to the Commission, access to Eurodac's data by LEA's "*should only be requested when there are reasonable grounds to believe that comparison will provide information that will substantially assist them in preventing, detecting or investigating a terrorist or other serious criminal offence*".¹²⁵ This is broader than the original LEA's access purpose given back in 2006 by the German Presidency, where LEA's access was said to be "*based on factual indications for believing that the data subject has committed or will commit a [serious] criminal offence*".¹²⁶ The number of persons whose data would be checked is much smaller in the earlier discussions on LEA's access to Eurodac. The purpose limitation for access by Europol has been widened even more, allowing comparison with Eurodac data for purposes of specific analysis or for "*analysis of a general nature and of a strategic type*". The original aim has thus been deviated from, leaving behind the idea that access to Eurodac for law enforcement purposes had to be limited to specific cases as not to infringe the right to privacy and data protection. The new purpose cannot be deemed compatible to the purpose the data were gathered for originally, namely the effective application of the Dublin Regulation. This widening of the original intent for which the data has been collected, has been labelled as **function creep**.¹²⁷ The Commission merely states that this widening of the purpose limitation is fully in line with the CFREU and more specifically its data protection standards, not further substantiating their claim or elaborating on this function creep.¹²⁸ Both the opinion of the European Data

¹²² The SIS II regulation has its legal basis in articles 62, 63 and 66 of the (now changed) EC Treaty and the VIS is based on article 62 and 66 of the (now changed) EC Treaty. See also: Standing Committee of experts on international immigration, refugee and criminal law, *o.c.*, p. 4.

¹²³ European Court of Justice, Joined Cases C-317/04 and C-318/04 (European Parliament v. Council and Commission), Judgment of the Grand Chamber, 30 May 2006, ECR I-4721.

¹²⁴ Both are recognised in article 7 (respect for private life) and article 8 (protection of personal data) of the Charter of Fundamental Rights of the European Union, which now has binding character thanks to the Lisbon Treaty. Article 8 of the European Convention on Human Rights refers to the right to respect for private life.

¹²⁵ Preamble (11) of the 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, 21 p. These conditions are repeated in article 7 and 8 of the proposal.

¹²⁶ Council of the European Union, Policy document concerning access to Eurodac by Member State's police and law enforcement authorities, 16982/06, Brussels, 20 December 2006, p. 2.

¹²⁷ Besters, M. and Brom, F.W.A., 'Greedy' information technology: the digitalization of the European Migration Policy, *European Journal of Migration and Law* (12) 2010, p. 465.

¹²⁸ Commission of the European Communities, COM(2009) 344 final, 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, p. 4 and Commission of the European Communities,

Protection Supervisor and recent judicial rulings illustrate however, that the rules concerning purpose limitations should be interpreted in a stricter way. Firstly, the EDPS reports in its opinion on the overview of information management in the AFSJ, that the purpose limitation principle requires that “*the purposes for which personal data are collected should be clearly specified not later than at the time of collection, and that data should not be processed for purposes incompatible with those initial purposes*”.¹²⁹ The Commission self-consciously admits this has not been the case for SIS, SIS II and VIS¹³⁰, and Eurodac is seemingly heading the same way, no longer putting the purpose limitation at the core of EU-level information management. Article 13 of the Data Protection Directive 95/46/EC allows exceptions to the purpose limitation rule, but the EDPS has similarly highlighted that the necessity and proportionality of the breach have not been proven.¹³¹ More information on both aspects will be given in the next paragraphs. Furthermore, the current proposal for LEA’s access to Eurodac might risk annulment by the European Court of Justice, similar to the cases ‘Rechnungshof v. Österreichischer Rundfunk’ and ‘Huber v. Germany’ on the basis of non compliance with the rules set forth in the Data Protection Directive. In ‘Rechnungshof v. Österreichischer Rundfunk’¹³², it has been confirmed that the rules for legitimate data processing (including the purpose limitation rule) have direct effect, thereby giving the possibility to individuals to seek access to courts to prevent the application of rules contrary to the data protection rules (para. 100). The purpose limitation implies that data processing should be foreseeable for the data subject and should not go beyond the reasonable expectations of the person concerned.¹³³ In this way, individuals who have their data already stored in Eurodac can easily contest the provisions on LEA’s access to their data. Furthermore, the importance of a strict reading of the purpose limitation rule has been

SEC(2009) 936, Commission staff working document - Accompanying document to the amended proposal for a regulation of the European Parliament and 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) and to the proposal for a Council Decision on requesting comparisons with EURODAC data by Member States’ law enforcement authorities and Europol for law enforcement purposes - Impact assessment, Brussels, 10 September 2009, p. 15-16.

¹²⁹ European Data Protection Supervisor, Opinion of the European Data Protection Supervisor on the communication from the Commission to the European Parliament and the Council - ‘Overview of information management in the area of freedom, security and justice’, 29 December 2010, OJ C 355/18.

¹³⁰ Commission of the European Communities, COM(2010) 385 final, Communication from the Commission to the European Parliament and the Council - overview of the information management in the area of freedom, security and justice, 20 July 2010, p. 22

¹³¹ 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 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], and on the Proposal for a Council Decision on requesting comparisons with EURODAC data by Member States’ law enforcement authorities and Europol for law enforcement purposes, 10 April 2010, OJ C 92/6-7

¹³² European Court of Justice, Joined Cases C-465/00, C-138/01 and C-139/01 (Rechnungshof and Österreichischer Rundfunk, Wirtschaftskammer Steiermark, Marktgemeinde Kaltenleutgeben, Land Niederösterreich, Österreichische Nationalbank, Stadt Wiener Neustadt, Austrian Airlines, Österreichische Luftverkehrs-AG and between Christa Neukomm, Joseph Lauer mann and Österreichischer Rundfunk), Preliminary ruling, 20 May 2003, WWW <<http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=en>>.

¹³³ Standing Committee of experts on international immigration, refugee and criminal law, The amended proposal for the Eurodac Regulation (COM (2009) 342) and the Decision on requesting comparisons with Eurodac data by Member States’ law enforcement authorities and Europol for law enforcement purposes (COM (2009) 344), CM0910, Utrecht, 30 December 2009, p. 6.

acknowledged in the case ‘Huber v. Germany’¹³⁴, which deals with the storage of information on Mr. Huber, an Austrian citizen, in the centralised register of the German national aliens administration. This database contained information on his name, date and place of birth, sex, nationality, date of entry, involvement in serious crimes, etc.. The storage of such information was deemed lawful to determine residence status in the light of the Data Protection Directive, especially when the requirement of necessity was at hand. However, with regard to the use of information held by the aliens’ administration for statistical purposes, the ECJ judged that the requirements of necessity were not met. Also, the use of these data on aliens for the purpose of fighting crime was considered unlawful as it violated the prohibition of discrimination as set out in (the old) article 12 EC. The latter was not, however, checked against the Data Protection Directive as it is not applicable to third pillar issues. Nevertheless, there is no reason to conclude that less strict criteria would apply with regard to LEA’s access to asylum seekers: their rights are also protected under EU law.¹³⁵ Although the Data Protection Directive applies to the former first pillar matters, the expected new EU data protection rules will have major attention for the purpose limitation principle. The European Commission even stated in its 2010 communication that the current data protection rules regarding police and judicial cooperation ‘*contain too wide an exception to the purpose limitation principle*’.¹³⁶ As such, the Commission should even be more careful when assessing the possible access of LEA’s to Eurodac. With regard to the control on whether or not the purpose limitation will be respected, things seem to be taken care of. The proposal provides a ‘verifying authority’ installed in each member state, which will only forward requests for comparison with the Eurodac data when all conditions are fulfilled.¹³⁷ Control on that authority can be done by the National Supervisory Authorities and the European Data Protection Supervisor mentioned in the Eurodac Regulation.

The different evolutions illustrated above show that the purpose limitation rule is being increasingly put under pressure. Austria, for example, has asked that “*Eurodac should be used as extensively as possible*”.¹³⁸ Nonetheless, it is important to remember that the use and purpose of Eurodac has been strictly limited by its founders. The database was carefully, and after substantial deliberation, placed beyond the reach of police and law enforcement agencies on the basis of the fundamental rights of asylum seekers.¹³⁹ As such, it could be used to implement only the relevant regulations relating to the Dublin Convention and not for other purposes. The legal service of the Council stated in its advice that the database could not be used for other purposes, e.g. “*for starting criminal investigations against asylum seekers*”, while the European Parliament, however powerless back then, stated that ‘the use of the

¹³⁴ European Court of Justice, Case C-524/06 (Heinz Huber v. Bundesrepublik Deutschland), preliminary ruling, 16 December 2008, WWW

<<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62006J0524:EN:NOT>>.

¹³⁵ Standing Committee of experts on international immigration, refugee and criminal law, *o.c.*, p. 7.

¹³⁶ Commission of the European Communities, COM(2010) 609 final, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of Regions - A comprehensive approach on personal data protection in the European Union, 4 November 2010, p. 13.

¹³⁷ Article 4 of the Proposal for a Council Decision on requesting comparisons with EURODAC data by Member States’ law enforcement authorities and Europol for law enforcement purposes, COM(2009) 344, 10 September 2009, 21 p.

¹³⁸ Standing Subcommittee on European Union Affairs, Statement to the European Commission, 17 April 2009, 6 p., WWW

<http://www.ipex.eu/ipex/webdav/site/myjahiasite/users/atnatcorresp/public/Statement_Asylum.en.pdf>.

¹³⁹ House of Lords - European Union Committee, Prüm: an effective weapon against terrorism and crime? - Report with evidence - 18th report of session 2006-07, The Stationery Office, London, 9 May 2007, p. 16.

Eurodac system must on no account be extended to cover wider areas or purposes'.¹⁴⁰ Nevertheless, policy goals have shifted a decade later, and the existence of a large database remains a temptation to enlarge its use for other purposes. The Commissioner for Human Rights reiterated that the purpose limitation rule requires that data collected for one specific purpose (*in casu* the determination of the member state responsible for an asylum claim) can only be used for another specific purpose (*in casu* the detection, prevention and investigation of serious crimes), if the data could have been independently collected for that second purpose.¹⁴¹ This is not the case for the proposal for LEA's access to Eurodac.

Concrete: Data protection issues take a prominent place in an ever-developing information society. The above paragraphs point out that those principles are still not taken seriously. Firstly, the legal basis for extending Eurodac's purpose is not satisfactory. A bridging clause which refers to a third pillar council decision is not sufficient as the Eurodac Regulation's legal basis (art. 63(1)a) still only allows it to be a migration policy tool. Secondly, Eurodac's original purpose limitation is deviated from. Although this is allowed in certain circumstances, judgments before the European Court of Justice concerning similar facts have indicated that the purpose limitation rule has to be interpreted strictly. *In casu*, this is not the case, especially when one takes into account that the new EU data protection will show renewed attention to the purpose limitation principle as even current data protection rules are too loose.

3.4.2 The principles of proportionality, subsidiarity and necessity

The Commission is duly aware that its legislative proposal has to be compatible with the CFREU. For this reason it reiterated that the right to the protection of personal data enshrined in article 8 requires that a limitation of this right can only be justified when the measure has a legitimate aim, subject to the principle of proportionality (implying a subsidiarity check) and when it is necessary in a democratic society. The Commission therefore certifies that its proposal to grant the LEA's access to Eurodac is a proportional way to investigate whether an asylum seeker is involved in serious crime, and that it is necessary to ensure public safety.¹⁴² No reasonable efficient alternative to Eurodac exists to establish or verify the exact identity of an asylum seeker which is later linked to serious crime. Thus, LEA's access is seen as the only timely, accurate, secure and cost-efficient way to prevent and combat serious crime involving third country nationals. It can therefore not be considered

¹⁴⁰ Council Legal Service, Advice, 5546/93, JUR 25, 18 March 1993 and Van der Ploeg, I., The illegal body: 'Eurodac' and the politics of biometric identification, *Ethics and Information Technology* (1) 1999, p. 299.

¹⁴¹ Commissioner for Human Rights, CommDH/IssuePaper(2008)3, Protecting the Right to privacy in the fight against terrorism, Strasbourg, 4 December 2008, p. 7.

¹⁴² Commission of the European Communities, SEC(2009) 936, Commission staff working document - Accompanying document to the amended proposal for a regulation of the European Parliament and 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) and to the proposal for a Council Decision on requesting comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes - Impact assessment, Brussels, 10 September 2009, p. 15-16.

disproportionate to the aims of the prevention, detection and investigation of terrorist and other serious offences.¹⁴³

The balancing of human rights and limitations to them is a delicate matter, and opinions amongst the Commission and different human rights organisations differ widely. It is certainly true that the proposal contains a threshold of several crimes for which LEA's may access Eurodac. The proposal refers to the 32 crimes also mentioned in other documents on international police and judicial co-operation, such as the European Arrest Warrant and the European Evidence Warrant.¹⁴⁴ Because of the seriousness of the facts, not having LEA's access to Eurodac is identified as a shortcoming.¹⁴⁵ However, from the police and judicial instances' point of view, every denial of access to a potential source of information can be seen as a shortcoming to effective and efficient crime fighting. This viewpoint thus has to be weighed against the severity of the breach of human rights, to assess whether or not the **principle of proportionality** is respected. In this light it is remarkable to hear that the Dutch Minister of Justice declared the proposal to record the fingerprints of all Dutch nationals in order to facilitate criminal investigations to be 'disproportional'.¹⁴⁶ The Dutch Minister of Justice is however in favour of the proposal for LEA's access to Eurodac and is not of the opinion that this measure is disproportional.¹⁴⁷ This gives the impression that a 'dual standard' is being used to determine the proportionality of access to Eurodac for law enforcement purposes, depending on people's nationality. This is in line with the comments of the EDPS and the Meijers Committee, who say that the proportionality (and necessity) of the proposal is not sufficiently proven.¹⁴⁸ The Commission in its impact assessment seems to

¹⁴³ Commission of the European Communities, *o.c.*, p. 33-34 and Commission of the European Communities, COM(2009) 344 final, 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, p. 6.

¹⁴⁴ Article 2.1(e) of the Proposal for a Council Decision on requesting comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes, COM(2009) 344, 10 September 2009, 21 p.

¹⁴⁵ Commission of the European Communities, COM(2005) 597 final, Communication from the Commission to the Council and the European Parliament - on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs, 24 November 2005, p. 6 and Commission of the European Communities, SEC(2009) 936, Commission staff working document - Accompanying document to the amended proposal for a regulation of the European Parliament and 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) and to the proposal for a Council Decision on requesting comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes - Impact assessment, Brussels, 10 September 2009, p. 5.

¹⁴⁶ Brouwer, E., Data surveillance and border control in the EU - balancing efficiency and legal protection, in: Balzacq, T. and Carrera, S. (eds.), *Security versus freedom?: a challenge for Europe's future*, Ashgate, Aldershot, 2006, p. 243.

¹⁴⁷ "In its opinion of 7 October 2009, the EDPS expresses serious doubts on the legitimacy, necessity and proportionality of the European Commission proposal. I do not yet share these concerns." See the letter of the Minister of Justice Hirsch Ballin: Eerste Kamer der Staten-Generaal, Verslag van een schriftelijk overleg vastgesteld 5 februari 2010, 23 490 FQ, 2010, p. 3.

¹⁴⁸ 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 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], and on the Proposal for a Council Decision on requesting

reiterate several times that the proposal is proportionate, however seemingly unable to substantiate the claim. It is true that the crimes are particularly serious, but the Commission does not explain further why LEA's access is proportionate, considering the equally extensive breach of individuals' rights. Compliance with the proportionality principle does not only imply that the proposed measure is effective, which includes the argument of a timely, accurate, secure and cost-effective tool for law enforcement purposes.¹⁴⁹

It is equally remarkable that the Commission proposal refers to art. 8 CFREU (protection of personal data), but not to art. 8 ECHR and art. 6 CFREU (right to private life). As demonstrated in the case *S. Marper v. UK* before the European Court of Human Rights, large-scale databases, including fingerprints of individuals, are within the scope of this fundamental right.¹⁵⁰ The case dealt with the storage of fingerprints and DNA samples of individuals who were suspected of having committed criminal offences, but who were not convicted. The storage of these data is "capable of affecting his or her private life and retention of this information without the consent of the individual cannot be regarded as neutral or insignificant" (para. 84). The asylum seeker, however mandatorily, has to give his fingerprints when claiming asylum, and is not able to refuse its use in criminal proceedings. The Court concluded that the UK violated art. 8 ECHR, because storing the data concerning non-convicted persons was disproportional. The Eurodac proposal concerns a wider, European, database, with the fingerprints of asylum seekers, irrespective of the fact that these persons were ever suspected or involved in criminal procedures.¹⁵¹ Accordingly, the proposal is likely to be considered outside the states' margin of appreciation on the limitation of the right to private life, which in the *S.* and *Marper* case implies that the United Kingdom did not strike the right balance. Also of interest, although it has no influence on EU law, is the 1983 case *Kolender v. Lawson* in which the United States Supreme Court decided that the government cannot require citizens to provide credible and reliable identification if they committed no crime other than looking suspicious.¹⁵² It shows that information collected from unsuspecting individuals for an administrative purpose (asylum claim) should be unavailable for law enforcement. The case illustrates how much the concept of proportionality has changed throughout the years.

Proportionality also implies that the purpose of prevention, detection and investigation of serious crimes cannot be reached using the existing tools.¹⁵³ The **subsidiarity** of using Eurodac will be reviewed hereunder. The criteria developed by the European Court of Human Rights in the *Hatton* case to establish whether due respect was given to the principle of

comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes, 10 April 2010, OJ C 92 and Standing Committee of experts on international immigration, refugee and criminal law, The amended proposal for the Eurodac Regulation (COM (2009) 342) and the Decision on requesting comparisons with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (COM (2009) 344), CM0910, Utrecht, 30 December 2009, p. 4.

¹⁴⁹ European Data Protection Supervisor, *o.c.*, p. 7.

¹⁵⁰ European Court of Human Rights, *S. and Marper v. The United Kingdom*, judgment, 4 December 2008, WWW <<http://www.echr.coe.int/echr/en/hudoc>>.

¹⁵¹ Standing Committee of experts on international immigration, refugee and criminal law, The amended proposal for the Eurodac Regulation (COM (2009) 342) and the Decision on requesting comparisons with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (COM (2009) 344), CM0910, Utrecht, 30 December 2009, p. 3.

¹⁵² United States Supreme Court, *Kolender, Chief of Police of San Diego, et al. v. Edward Lawson*, 461 U.S. 352, 2 May 1983, WWW <<http://supreme.justia.com/us/461/352/case.html>>.

¹⁵³ European Data Protection Supervisor, *o.c.*, p. 7.

proportionality could be of relevance here.¹⁵⁴ In assessing the impact on the right to a private life and the interests of the community the ECtHR asserted that “*States are required to minimise, as far as possible, the interference with these rights, by trying to find alternative solutions and by generally seeking to achieve their aims in the least onerous way as regards human rights. In order to do that, a proper and complete investigation and study with the aim of finding the best possible solution which will, in reality, strike the right balance should precede the relevant project*”.¹⁵⁵ Hence, two features can be studied more closely: whether or not alternative solutions are being used and other solutions have been examined.

Firstly, the Commission did include a condition on subsidiarity in the proposal: Eurodac data can only be consulted if the fingerprints have already been searched in the member state’s own national fingerprint database and if, subsequently, a search under the Prüm Decision¹⁵⁶ did not provide any positive results.¹⁵⁷ Since different countries do not store the asylum seekers’ fingerprint information in their criminal databases or restrict access to them for law enforcement purposes, the Commission rightly notices that law enforcement authorities will remain ignorant about information available on the asylum seeker in various EU countries.¹⁵⁸ On the other hand, the Prüm Decision was very much criticised, by the British House of Lords, the European Parliament and the EDPS. Not all countries wanted to co-operate with Prüm initially, and only a core group of seven EU member states further elaborated the system. It was deemed that, because of the technical limitations in this decentralised system, with each country having multiple databases to be connected, available information was likely to be overlooked.¹⁵⁹ The Commission also notices this: ‘the existing instruments on exchange of law enforcement information do not allow to timely determine with sufficient certainty whether a member state actually holds fingerprint data of an asylum seeker’.¹⁶⁰ By concluding that the existing measures would not work, the Commission seems to question the efficiency of EU instruments for the protection of security and for law enforcement purposes in general which it advocated in the past.¹⁶¹ It may feel uncomfortable when a system that was developed outside the EU, is later used - even though there was not enough agreement on it - as an argument to go further within the EU. This may be perceived as if the EU is used to compensate for an inadequate measure that it did not want in the first place. The EDPS notes that the Commission presents the fact that ‘*while [the Prüm Decision] might be successful for*

¹⁵⁴ Brouwer, E., *o.c.*, p. 244-245.

¹⁵⁵ European Court of Human Rights, *Hatton and others v. The United Kingdom*, judgment, 2 October 2001, WWW <<http://www.echr.coe.int/echr/en/hudoc>>.

¹⁵⁶ Council of the European Union, 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, 6 August 2008, OJ L 210. The Prüm Decision provides for the automated exchange of DNA, fingerprints and vehicle registration data, as well other forms of police cooperation, between the national databases of the 27 Member States. Access to DNA profiles and fingerprints held in national databases is granted on a ‘hit/no-hit’ basis.

¹⁵⁷ Article 7.1 of the Proposal for a Council Decision on requesting comparisons with EURODAC data by Member States’ law enforcement authorities and Europol for law enforcement purposes, COM(2009) 344, 10 September 2009, 21 p.

¹⁵⁸ Explanatory memorandum of the Proposal for a Council Decision on requesting comparisons with EURODAC data by Member States’ law enforcement authorities and Europol for law enforcement purposes, COM(2009) 344, 10 September 2009, 21 p.

¹⁵⁹ Eechautd, V., *De impact van het kaderbesluit 2006/960/JHA op de informatie-uitwisseling tussen rechtshandhavingsautoriteiten binnen de EU en de implicaties voor Europol*, Ghent, 2009. (Bachelor dissertation).

¹⁶⁰ Explanatory memorandum of the Proposal for a Council Decision on requesting comparisons with EURODAC data by Member States’ law enforcement authorities and Europol for law enforcement purposes, COM(2009) 344, 10 September 2009, 21 p.

¹⁶¹ Standing Committee of experts on international immigration, refugee and criminal law, *o.c.*, p. 5.

those Member States that store fingerprints of asylum seekers together with other fingerprints collected for law enforcement authorities in a national [database], it will be unsuccessful for those Member States that do not store fingerprints of asylum seekers in their national [fingerprint database] unless they are related to crime' as a justification of the proposal. Additionally, the EDPS argues that there is a good reason for this: non-criminal asylum seekers' fingerprints should not be stored in the same database as those holding information of persons related to crime (see also the previous paragraph 3.3). Instead, the Commission should be considering whether the storage of asylum seekers' fingerprints in law enforcement databases is in compliance with EU law on data protection.¹⁶² If Eurodac would not be opened to law enforcement authorities in the future, it could be that some member states will link their asylum database to the Prüm system. As data protection rules in Prüm defer from the ones in the LEA's access proposal, this could endanger refugees, which has been a big concern of refugee and asylum organisations when assessing the LEA's access proposal (see *infra*: effective control on data).

Secondly, we can notice the following when evaluating the existing instruments. The LEA's access proposals or the impact assessment often refer to the Prüm Decision, the Framework Decision on simplifying the exchange of information¹⁶³, the SIS (II) and the VIS as similar evolutions regarding the exchange of information or to identify shortcomings. Additionally (and more importantly), article 6 of the Council Decision refers to the use of the Prüm Decision as a prerequisite for accessing Eurodac for law enforcement purposes. The Prüm Decision should be implemented by August 2011 and a first evaluation on its implementation should be handed in by July 2012.¹⁶⁴ The VIS would go live in October 2011 and SIS II would be operational during the first quarter of 2013.¹⁶⁵ New EU instruments should first be implemented and evaluated, and their conclusions should be taken into account before considering analogous measures such as the extended use of Eurodac. Such comprehensive assessments have not yet taken place.¹⁶⁶ Referring back to the Hatton Case discussed earlier, the Commission's impact assessment can't be regarded as a 'proper and complete investigation': 'the best possible solution which strikes the right balance' is difficult to find when a report on the Prüm Decision has not yet been written.

Falling under the umbrella of national security and public safety, countering terrorism and other forms of serious crime are legitimate grounds to accept limits on the right to data protection and the right to privacy, as prescribed by article 8(2) ECHR. This way, the state can equally ensure the right to liberty and security of a person. As touched upon previously and attested in the explanatory memorandum of the proposal, a legitimate aim is not the only criterion, it also needs to be in accordance with the law and necessary in a democratic society. The principle of proportionality thus takes into account the **principle of necessity**. The EDPS reasons that this necessity should be demonstrated all the more in the case of a substantial intrusion in the rights of individuals from a vulnerable group.¹⁶⁷ Due attention is given to the situation asylum seekers find themselves in, taking into account the rulings of the European

¹⁶² European Data Protection Supervisor, *o.c.*, p. 7-8.

¹⁶³ Council of the 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, 19 December 2006, OJ L 386, 12 p.

¹⁶⁴ *Ibid.*

¹⁶⁵ Frank Paul, Head of the unit 'large-scale IT systems and biometrics', part of the Directorate-General for Home Affairs, presentation at the ERA conference on information exchange, 19 May 2011.

¹⁶⁶ European Data Protection Supervisor, *o.c.*, p. 6-7 and Standing Committee of experts on international immigration, refugee and criminal law, *o.c.*, p. 5.

¹⁶⁷ European Data Protection Supervisor, *o.c.*, p. 5.

Court of Human Rights. For example, the Court emphasises in the Buckley, Chapman and Connors cases - the latter being of further importance later in this chapter - that “the vulnerable position of Gypsies as a minority means that some special attention has to be given to their needs”. Asylum seekers are to be regarded equally as a vulnerable group. National jurisprudence also gives considerable attention to the vulnerable position of particular groups. More specifically, the French Constitutional Court prohibited access to the French asylum seekers’ fingerprint database for law enforcement purposes, stating that ‘*The confidential treatment of information held by the Office for the protection of refugees and stateless persons on applicants for refugee status in France is a vital guarantee of the right of asylum, a principle of constitutional status which implies inter alia that applicants for refugee status must enjoy special protection; it follows that only such officers as are empowered to apply asylum law, notably in decisions granting refugee status, may have access to such information, and in particular to applicants’ fingerprints*’.¹⁶⁸ The EDPS concludes that, to be valid, the necessity of using Eurodac data must be supported by clear and undeniable elements. The Commission states in its defence that the ECtHR’s jurisprudence has decided various times that actions aimed at combating terrorism and other serious crimes have been accepted as exceptions to the necessity principle, as prescribed by article 8(2).¹⁶⁹ Even though this is true, it is unfortunate that no reference is made to specific cases to substantiate their claim to check on which grounds the cases were settled. The ECtHR has set out in different cases how the principle of necessity should be interpreted when dealing with the right to private life. In the case of *Gillow v. The United Kingdom*, the interference was permitted, as far as it answered a ‘pressing social need’, and if the reasons given were ‘relevant and sufficient’.¹⁷⁰ Law enforcement stakeholders are of the opinion that access to Eurodac is necessary to achieve an adequate level of efficiency in the prevention, detection and investigation of serious crime.¹⁷¹ Notwithstanding, the ECtHR recalls in *Leander v. Sweden* and *Connors v. The United Kingdom* that the margin of appreciation enjoyed by the states depends also on the interference involved and will be narrower where the right at stake is crucial to the individual’s effective enjoyment of intimate or key rights.¹⁷² The argument of the law enforcement authorities thus certainly has its merits. However, to respond to the demands of the ECtHR, mere efficiency is not enough to infringe on the right to private life. A clear link between terrorism and serious crime on the one hand and asylum seekers on the other hand has to be proven. This substantive link is far from proven and the necessity is thus far from being demonstrated (for more details see paragraph 3.5). As such, the EDPS has a considerable argument when it points out that a possible scenario does not make it a general

¹⁶⁸ French Constitutional Council, Decision 97-389, Act making various provisions in respect of immigration, 22 April 1997, WWW <<http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/97389DCa97389dcpdf>>.

¹⁶⁹ Commission of the European Communities, SEC(2009) 936, Commission staff working document - Accompanying document to the amended proposal for a regulation of the European Parliament and 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) and to the proposal for a Council Decision on requesting comparisons with EURODAC data by Member States’ law enforcement authorities and Europol for law enforcement purposes - Impact assessment, Brussels, 10 September 2009, p. 16.

¹⁷⁰ European Court of Human Rights, *Gillow v. The United Kingdom*, judgment, 24 November 1986, WWW <<http://www.echr.coe.int/echr/en/hudoc>>.

¹⁷¹ Commission of the European Communities, *o.c.*, p. 23.

¹⁷² European Court of Human Rights, *Leander v. Sweden*, judgment, 26 March 1987, WWW <<http://www.echr.coe.int/echr/en/hudoc>> and European Court of Human rights, *Connors v. The United Kingdom*, judgment, 27 May 2004, WWW <<http://www.echr.coe.int/echr/en/hudoc>>.

pattern which would justify the adoption of the LEA's access proposals.¹⁷³ The violation of the right to privacy cannot be considered in proportion to the effect that the access to Eurodac for law enforcement purposes will have on the tasks of the LEA's activities because no direct and causal link can be given for the nexus between the entry of asylum seekers on the one hand and the fight against terrorism and other serious crime on the other hand.¹⁷⁴

Concrete: The proposal mentions the principles of proportionality, subsidiarity and necessity various times. Although the Commission assures that those are complied with, it does not substantiate this claim. In the first place, European jurisprudence has shown that similar practices were deemed disproportional, because of the fact that the data concerned unconvicted persons. Secondly, both the use of alternative solutions and their evaluation has not been taken into account sufficiently to comply with the principle of subsidiarity. The fact that Prüm will not always return positive results, is used as an argument by the Commission. However, this is exactly because certain member states did not want to open their asylum database for law enforcement purposes. Moreover, an evaluation of similar law enforcement instruments (Prüm, SIS II, ...) still has not taken place, because these are not yet operational. Thirdly, the principle of necessity got some attention. It is true that access to Eurodac might prove to be useful for law enforcement purposes, just as it could be useful to have access to a database of every citizen's biometrics. In line with ECtHR jurisprudence however, in case of an extensive interference, there is only a narrow margin of appreciation for the state to act. As no direct link can be established between asylum seekers and terrorism and serious crime, focussing solely on asylum seekers cannot be considered to fall within the state's margin of appreciation.

3.4.3. *Effective control on the data*

Effective control on the data in Eurodac relates to controlling who has access to the data, where the data is going and for what purposes it is used. To prevent misuse or loss of the data, different restrictions have been integrated in the proposal for LEA's access to Eurodac. Access to Eurodac is currently limited to 'competent authorities' for the purpose of the Eurodac Regulation. This means that it was drafted to allow access to the database only of authorised persons for the purpose of determining the outcome of an asylum claim.¹⁷⁵ In practice, different countries let Eurodac be operated entirely or partly by police as they are the national institutions dealing with an asylum claim.¹⁷⁶ Consequently, the fact that Eurodac has not been (officially) used for law enforcement purposes would rather be a matter of trust than possibilities.¹⁷⁷ However, that an amendment to the Eurodac Regulation is proposed, means that law enforcement agencies are not getting the information they want, or, as has been

¹⁷³ European Data Protection Supervisor, *o.c.*, p. 10.

¹⁷⁴ De Busser, E., *Data Protection in EU and US Criminal Cooperation, a substantive law approach to the EU internal and transatlantic cooperation in criminal matters between judicial and law enforcement authorities*, Maklu, Antwerpen, 2009, p. 181.

¹⁷⁵ House of Lords - European Union Committee, *The Treaty of Lisbon: an impact assessment - volume II: evidence - 10th report of session 2007-08*, The Stationery Office, London, 13 March 2008, p. E47.

¹⁷⁶ Eurodac Supervision Coordination Group, *Report of the First coordinated inspection*, Brussels, 17 July 2007, p. 12.

¹⁷⁷ Geyer, F., *Taking stock: databases and systems of information exchange in the area of freedom, security and justice*, Centre for European Policy Studies, May 2008, p. 6, WWW <www.ceps.eu>.

surmised, law enforcement agencies are concerned about the legality of access to that data.¹⁷⁸ Of the essence is that ‘competent authorities’ are interpreted in different ways in different countries. Several member states’ data protection agencies even have troubles identifying which authorities have access to or control the actual data.¹⁷⁹ To ensure that information on asylum seekers is not misused or lost, the access to Eurodac is further regulated by the Commission proposals for a recast of the Eurodac Regulation.¹⁸⁰ Several processes and limitations have been added to prevent the unauthorised use or dissemination of information on asylum seekers, including the publication of a list in the EU Official Journal of all authorities having access to Eurodac for the purpose of determining an asylum claim.¹⁸¹ The new provisions mentioned above should ensure a higher level of data protection and should enable asylum seekers to control their data more easily. Previous controls actually revealed that persons whose data were in Eurodac, were unaware of their rights to access their data and to seek legal remedy if their data was misused or incorrect.¹⁸²

This framework of enhanced protection concerning **data access** is partially applied to the provisions concerning access to Eurodac by law enforcement agencies. The proposal foresees the obligation to member states to keep a list of the ‘designated authorities’ who will access Eurodac for law enforcement purposes.¹⁸³ This has been welcomed as a means to improve transparency and accountability, as such facilitating the task of national and supra-national data protection agencies. The fact that the list does not have to be forwarded to the Commission nor published - as is the case for designated authorities who access Eurodac for determining an asylum claim - should not cause a major problem if it can be accessed easily by the competent authorities. However, in the light of harmonisation of procedures it would not be a bad idea per se. The Meijers Committee is more pessimistic about this point and argues that it would be impossible for the asylum seeker to find out which authorities under certain circumstances may get access to his or her personal information.¹⁸⁴ Furthermore, every member state is free to designate its law enforcement authorities that are granted access to

¹⁷⁸ House of Lords - European Union Committee, *o.c.*, p. E47.

¹⁷⁹ Eurodac Supervision Coordination Group, *o.c.*, p. 13.

¹⁸⁰ Commission of the European Communities, COM(2010) 555, Amended proposal for a regulation of the European Parliament and 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), 11 October 2010, 70 p., Commission of the European Communities, COM(2009) 342, 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] (Recast version), 10 September 2009, 74 p., Commission of the European Communities, COM(2008) 820, 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, 67 p.

¹⁸¹ See the article on “data security” in the different proposals for a recast of the Eurodac Regulation.

¹⁸² Eurodac Supervision Coordination Group, Second Inspection Report, Brussels, 24 June 2009, p. 8-15.

¹⁸³ Preamble (9) and Article 3 of the proposal for a Council Decision on requesting comparisons with EURODAC data by Member States’ law enforcement authorities and Europol for law enforcement purposes, COM(2009) 344, 10 September 2009, 21 p.

¹⁸⁴ Standing Committee of experts on international immigration, refugee and criminal law, The amended proposal for the Eurodac Regulation (COM (2009) 342) and the Decision on requesting comparisons with Eurodac data by Member States’ law enforcement authorities and Europol for law enforcement purposes (COM (2009) 344), CM0910, Utrecht, 30 December 2009, p. 5.

Eurodac, as long as they abide by the rules set out in the proposal. In this respect it is valuable to point out the continual widening of agencies which will have access to different databases.¹⁸⁵ As has been stated in a House of Lords Report: “*The wording of who has access to these different databases has a tendency to be wider, not only limited to police agencies but also including intelligence agencies, or, at least, to use wording which certainly leaves open the possibility that the Member States can interpret access as being made available to intelligence agencies as well*”.¹⁸⁶ For example, the wording of which LEA’s will have access to the Visa Information System or the Schengen Information System II, is not limited to the classic law enforcement authorities.¹⁸⁷ While normal coercive agencies, e.g. the police, are regulated by fairly substantial rules, about how and why they have access and what they can use information for, the intelligence services tend to be less carefully regulated.¹⁸⁸ In this regard it is positive to see that the Commission’s proposal for a Council Decision on LEA’s access stipulates that “designated authorities shall not include agencies or units dealing especially with national security issues”.¹⁸⁹ As previous controls have indicated that different authorities had illegitimate access to Eurodac as they were not in charge of the asylum application (such as the tax authority or the judiciary for the purpose of identifying corpses), this provision on limited access should be effectively controlled.¹⁹⁰

The German Constitutional Court reiterated in 2008 that it is important for an individual to be able to oversee with sufficient reliability what personal information is known to which authorities.¹⁹¹ Even though access to Eurodac for law enforcement purposes is limited in some way, it is important to ensure that the **processing of data** retrieved from Eurodac is regulated, and that the data is not stored in national databases without any control on where the information is going, especially since the data concerns persons not previously linked to crime. The proposal therefore specifies that data obtained from Eurodac shall be erased from national and Europol files after a period of one month if the data are not required for ongoing criminal investigations.¹⁹² This should be sufficient enough to offer adequate protection, but based on past incidences with Eurodac, the following factors should also be taken into consideration. Firstly, although the proposal prescribes otherwise, data might not be deleted. For example, the Dutch Minister of Justice admitted that in 2007, four years after Eurodac became operational, there was no mechanism available to assure that asylum seekers who were recognised as a refugee would be automatically deleted, although this was prescribed by the Eurodac Regulation. The refugees instead had to ask for the deletion or hiding of the data

¹⁸⁵ House of Lords - European Union Committee, *o.c.*, p. E46.

¹⁸⁶ *Ibid.*, p. E46.

¹⁸⁷ Article 5 of the 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 offences, 13 August 2008, OJ L 218.

¹⁸⁸ House of Lords - European Union Committee, *o.c.*, p. E46.

¹⁸⁹ Article 3.1 of the Proposal for a Council Decision on requesting comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes, COM(2009) 344, 10 September 2009, 21 p.

¹⁹⁰ Eurodac Supervision Coordination Group, Report of the First coordinated inspection, Brussels, 17 July 2007, p. 12-13.

¹⁹¹ Bundesverfassungsgericht, 1 BvR 518/02, judgment, 4 April 2006, WWW <<http://www.bverfg.de/entscheidungen>>.

¹⁹² Article 10.4 of the Proposal for a Council Decision on requesting comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes, COM(2009) 344, 10 September 2009, 21 p.

themselves.¹⁹³ The Commission Report on the evaluation of the Dublin System disclosed similar findings, commenting that the deletion of data is not done routinely and therefore stays in the database of other member states.¹⁹⁴ If data is not deleted by national authorities, this might lead to the further process of data on innocent individuals, without any possibility to know where the information is, consequently offering no data protection. The fact that personal data is not deleted in time from Eurodac means that their data can still be accessed by LEA's, even if this is contrary to the proposals. Secondly, attention should also be paid to the transferring of data to third parties and member states. The proposal prohibits the transfer of data retrieved from Eurodac to any non-EU country (except for those who participate in Eurodac like Switzerland), international organisation or private entity.¹⁹⁵ The SIS II Council Decision for example, equally prohibits the transferring of data to non-EU countries and international organisations. However, if the member state consents, Europol and Eurojust may disseminate the data to non-EU countries and third bodies.¹⁹⁶ This is not the case for Eurodac, of which no information can be transferred further, even though different member states and Europol have agreements on the exchange of information. Looking at the asylum seekers' interests, different organisations warned that LEA's access to Eurodac may **endanger refugees** and expose them to the risk of torture and inhuman treatment¹⁹⁷ This is the case if information on an asylum application would reach the country of origin, as such making the asylum seeker prone to persecution if sent back to their country of origin. This would be contrary to the principle of non-refoulement, which is underwritten in i.a. the 1951 UN Refugee Convention and the ECHR. However, the proposal however the transmission of Eurodac data, which should, if complied with, protect the asylum seeker.

Concrete: The Commission has included several provisions on data protection, which have been welcomed by all stakeholders. Especially the fact that data on asylum seekers cannot be transferred to third states, was considered important in light of the non-refoulement principle and the prohibition of torture and inhuman treatment. Similarly, intelligence agencies have been denied access to Eurodac (in theory) as they are less carefully regulated and more difficulty held accountable for their actions.

¹⁹³ Tweede Kamer der Staten-Generaal, Aanhangsel van de Handelingen - Vragen gesteld door de leden der kamer, met daarop door de regering gegeven antwoorden - 317, vergaderjaar 2006-2007, WWW <http://www.eerstekamer.nl/eu/behandeling/20061115/kamervragen_klaas_de_vries_pvda/f=/vhn5inhraj2w.pdf>.

¹⁹⁴ Commission of the European Communities, COM(2007) 2999, Report from the Commission to the European Parliament and the Council on the evaluation of the Dublin system, Brussels, 6 June 2007, p. 10.

¹⁹⁵ Article 12 of the Proposal for a Council Decision on requesting comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes, COM(2009) 344, 10 September 2009, 21 p.

¹⁹⁶ Article 41.3, 42.2 and 54 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), 7 August 2007, L 205.

¹⁹⁷ Standing Committee of experts on international immigration, refugee and criminal law, The amended proposal for the Eurodac Regulation (COM (2009) 342) and the Decision on requesting comparisons with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (COM (2009) 344), CM0910, Utrecht, 30 December 2009, p. 7 and European Council on Refugees and Exiles, LTT - The European Commission will present on the 8th of July a proposal to provide law enforcement authorities with access to Eurodac, 30 June 2009, 2 p..

3.5 Stigmatising asylum seekers?

Different organisations have pointed out that access to Eurodac might further stigmatise asylum seekers as criminals.¹⁹⁸ This critique finds its foundation in the fact that immigrants, including asylum seekers, are already exposed to discrimination to a greater degree than non-immigrants¹⁹⁹, and are increasingly considered suspects, as public perceptions of refugees and asylum seekers have become mixed up with public discourse on the increase in terrorism.²⁰⁰ This influences the way these persons are treated in society: access to housing, education, work, etc. proves to be more difficult, and they are more often prone to discrimination and humiliation.²⁰¹

The link between asylum seekers and terrorism and serious crime has led to the proposal on LEA's access to Eurodac. Jurisprudence of the European Court of Human Rights has however condemned such practices in the past, as this link is not sufficiently established and fingerprints are regarded as a special category of sensitive data (as is DNA) that may stigmatise persons. In *Marper v. UK*, the Court stated that *“even if the retention of private data on a person cannot be equated with the voicing of suspicions, nonetheless their perception that they are not being treated as innocent could be heightened by the fact that their data are dealt with in the same way as convicted persons”* (para 122).²⁰² Nevertheless, the Commission brings forward data from Austria, Germany, the Netherlands and the UK, to prove that access to Eurodac could be very useful.²⁰³ This is highly likely, but does not

¹⁹⁸ European Council on Refugees and Exiles, LTT - The European Commission will present on the 8th of July a proposal to provide law enforcement authorities with access to Eurodac, 30 June 2009, p. 1, Standing Committee of experts on international immigration, refugee and criminal law, Note on the proposal of the JHA Council to give law enforcement authorities access to Eurodac, CM0712-IV, Utrecht, 18 September 2007, p. 3 and 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 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], and on the Proposal for a Council Decision on requesting comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes, 10 April 2010, OJ C 92/3.

¹⁹⁹ Commission of the European Communities, COM (2003) 336 final, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - On immigration, integration and employment, Brussels, 3 June 2003, p. 32.

²⁰⁰ Greenslade, R., *Seeking scapegoats. The coverage of asylum in the UK press*, Institute for Public Policy Research, London, 2005 and Lewis, M., *Asylum: understanding public attitudes*, Institute for Public Policy Research, London, 2005.

²⁰¹ “Ethnicity or immigrant origin consistently emerges as the most significant ground for experiencing discrimination [...]” See European Union Agency for Fundamental Rights, Data in focus report - multiple discrimination, Vienna, 2010, p. 4 and Standing Committee of experts on international immigration, refugee and criminal law, Note on the proposal of the JHA Council to give law enforcement authorities access to Eurodac, CM0712-IV, Utrecht, 18 September 2007, p. 3.

²⁰² European Court of Human Rights, *S. and Marper v. The United Kingdom*, judgment, 4 December 2008, WWW <<http://www.echr.coe.int/echr/en/hudoc>>.

²⁰³ Commission of the European Communities, SEC(2009) 936, Commission staff working document - Accompanying document to the amended proposal for a regulation of the European Parliament and 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) and to the proposal for a Council Decision on requesting comparisons with EURODAC data by Member States' law enforcement

provide a link serious enough to want access to a database keeping data only on asylum applicants and border crossers. Although the impact assessment is written carefully enough as not to state this explicitly, the numbers suggest a substantial link between refugees and terrorism and serious crime.²⁰⁴ The data brought forward insinuates a causal relationship, even though no analysis of a causal relationship between criminals and the relevant crimes is given. Austria for example, which claims to have the highest proportion of criminals that are asylum seekers, mentions numbers on crime suspects, but not on convicted criminals.²⁰⁵ Similarly, the evidence provided by the UK mention a hit rate of 7% when accessing the asylum and immigration database for counter-terrorism purposes. Yet, no differentiation is made between asylum seekers and non-asylum seekers and no number is mentioned of asylum seekers who were actually prosecuted or convicted, the point where it all comes down to.²⁰⁶ In the above-mentioned Marper case, the ECtHR equally underscored that such statistics are insufficient to justify the extended registration of fingerprints and DNA for law enforcement purposes. The German Federal Constitutional Court equally recognised the risk of stigmatisation in the ‘Rasterfahndung’ case in 2006, thus rendering police access to personal information collected for another purpose unconstitutional.²⁰⁷ According to the Federal Constitutional Court, the existence of a general threat after the terrorist attacks on the World Trade Centre in September 2001 was not serious enough to screen people that never even aroused any suspicion, and thus they were not to be subjected to the police’s distrust.²⁰⁸

The access of law enforcement authorities to Eurodac should logically lead to more criminal cases being resolved, which is praiseworthy. Nonetheless, the selective application of police resources (as there is no comparable database on non-asylum seekers) combined with the dark number of crime, will lead to an increase of the proportion of criminal asylum seekers in general crime statistics. This, in turn, leads to a higher stigmatisation of this group, which will self-evidently be associated even more with crime and extremism in public opinion. This fuels misperceptions about links between asylum and crime and exacerbates xenophobia and intolerance.²⁰⁹

Concrete: Asylum seekers are often linked with terrorism and serious crime. Although the Commission brings forward numbers that also insinuate this link, no substantial causal relation between asylum seekers and terrorism and serious crime is given. The ECtHR also prohibited similar law enforcement measures in the past, as the link between both was insufficiently demonstrated.

authorities and Europol for law enforcement purposes - Impact assessment, Brussels, 10 September 2009, p. 7-8.

²⁰⁴ *Ibid.*, p. 8. The numbers given by the Netherlands and the United Kingdom comprise crimes committed by all aliens, including but not limited to asylum seekers

²⁰⁵ Standing Committee of experts on international immigration, refugee and criminal law, Note on the proposal of the JHA Council to give law enforcement authorities access to Eurodac, CM0712-IV, Utrecht, 18 September 2007, p. 4.

²⁰⁶ *Ibid.*, p. 5.

²⁰⁷ Bundesverfassungsgericht, 1 BvR 518/02, judgment, 4 April 2006, WWW <<http://www.bverfg.de/entscheidungen>>.

²⁰⁸ Müller, F. and Richter, T., Report on the Bundesverfassungsgericht’s (Federal Constitutional Court) Jurisprudence in 2005/2006, *German Law Journal* (9) 2008, p. 178-184.

²⁰⁹ UNHCR, UNHCR’s recommendations to the Slovenian presidency of the European Union, 10 December 2007, 9 p.

3.6 The need for a complete, qualitative database and correct identifications

The Commission's proposal mentions that fingerprint data is especially useful information for law enforcement purposes, as it constitutes an important element in establishing the exact identity of a person.²¹⁰ This is true insofar that (1) the quality of the data accessed is up to standards and (2) that correct identifications are possible. Both aspects will be looked into hereunder.

(1) **Access to a database should only be granted if the database is complete, correct and working properly.** Eurodac is recognised as a qualitatively high database, although the Commission's evaluation reports have identified certain concerns. It has been noted that although the Eurodac Regulation prescribes the deletion of individual data after 2 or 10 years, reality demonstrates that data is not always deleted automatically.²¹¹ Equally, the Dutch Minister of Justice admitted in 2007 that there was no mechanism to assure that asylum seekers who obtained refugee status or were naturalised would be automatically deleted from Eurodac.²¹² Be that as it may, the quality of the data in Eurodac appears to be high: in 2009, 7% of all data uploaded to the Eurodac Central Unit was refused because fingerprints were not clear enough (e.g. due to the age of the asylum seeker or because fingerprint scanners are inadequate) to be stored in Eurodac.²¹³ This means that there are some concerns regarding the completeness and correctness of Eurodac data, but these have been identified. As a result, these problems could be solved, not longer standing in the way of opening Eurodac for law enforcement purposes.

(2) When checking a database on whether or not a matching fingerprint can be found, the assumption is that when a hit occurs, there is a **correct identification of the person whose fingerprints have been recognised.** However, biometric verification is a form of advanced probability calculation and the uncertainty of the outcome is inherent to the technique used. False identifications remain possible, leading to false positives (wrongly identifying someone) as well as false negatives (wrongly reporting that no matches have been found). The so-called 'false rejection rate' of biometric identifiers is estimated between 0,5 and 1%, and chances of having a failed verification of fingerprints taken from people older than 60 years are deemed high.²¹⁴ This has led to a.o. fingerprints rejected as proof before court and the Netherlands postponing the creation of a central fingerprint database, because false recognition rates were deemed too high.²¹⁵ Similarly, Peter Hustinx, supervisor of the European Data Protection

²¹⁰ Explanatory memorandum of the Proposal for a Council Decision on requesting comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes, COM(2009) 344, 10 September 2009, 21 p.

²¹¹ Commission of the European Communities, COM(2007) 2999, Report from the Commission to the European Parliament and the Council on the evaluation of the Dublin system, Brussels, 6 June 2007, p. 10.

²¹² Standing Committee of experts on international immigration, refugee and criminal law, Proposal to give law enforcement authorities access to Eurodac, CM0714, Utrecht, 6 November 2007, p. 5.

²¹³ Commission of the European Communities, COM(2010) 415 final, Report from the Commission to the European Parliament and the Council - Annual report to the European Parliament and the Council on the activities of the EURODAC Central Unit in 2009, 2 August 2010, p. 9.

²¹⁴ Brouwer, E., Data surveillance and border control in the EU - balancing efficiency and legal protection, in: Balzacq, T. and Carrera, S. (eds.), *Security versus freedom?: a challenge for Europe's future*, Ashgate, Aldershot, 2006, pp. 137-154 and Ministerie van binnenlandse zaken en koninkrijksrelaties, 2b or not 2b - evaluatierapport biometrieproef, 2005, p. 22.

²¹⁵ The UK's Asylum and Immigration Tribunal has upheld a previous key ruling on the reliability of Eurodac fingerprints. By providing only a fingerprint match on the EURODAC database the Secretary of State for the Home Department had not discharged his burden of proof. The applicant from Eritrea claimed to have been undertaking his military service from which he deserted in June 2005 at the time

Supervisor, stated when discussing third pillar EU databases, that the accuracy of biometrics is overestimated.²¹⁶ The question is if this is also true for Eurodac data. Information specifically on Eurodac's false identification rate is limited, with only the European Commission mentioning one false hit since the beginning of the activities of Eurodac.²¹⁷ What is more, member states are in no way obliged to inform the Commission of any incorrect hit. Nonetheless, the numbers of false negatives appear to be low and they do not seem to cause a direct problem to investigations. The issue then turns out to be: what legal remedies are provided for persons that are mistakenly identified? The proposal mentions none. Provisions as for example a recheck by a forensic expert could be considered. Those provisions should be possible if the false identification rate is indeed low. A higher rate could prejudice investigations as the remedies provided could potentially require valuable resources. In any case, the proportion of false identifications should be investigated more closely, as false hits might demand extra resources to investigate wrong presumptions, or for legal remedies for the accused.

Concrete: Both the need for a correct database and the need for correct identifications seem to be largely fulfilled. Regarding the completeness and correctness of Eurodac data, some problems arise such as the non-deletion of data. As those concerns have been identified, those could be remedied easily with enough political willpower. Regarding the number of correct identifications, at first sight Eurodac seems to have only one false hit since it was operational. Nonetheless, this number should be further investigated as no information obligation exists to inform the Commission in case of false recognitions. Additionally, certain legal safeguards should be incorporated in to the proposals which define the rights of the identified person in case he is wrongly identified. As the latter are said to be almost non-existent, those legal safeguards should not be resource-intensive.

* *

*

when the Home Office alleged he had sought asylum in Italy. The Home Office's case was based on a EURODAC fingerprint match. Other elements, such as a photograph, would have sufficed to conclude that the applicant was the same person as the one who claimed asylum in Italy. However, in the absence of such corroborating evidence, the applicant' account could not be said not to be credible. See Asylum and Immigration Tribunal, YI (previous claims - fingerprint match - Eurodac) Eritrea [2007] UKAIT 00054, 24 May 2007, WWW <<http://www.unhcr.org/refworld/pdfid/467bf1142.pdf>> and Ministerie van binnenlandse zaken en koninkrijksrelaties, Brief van minister J.P.H. Donner betreffende reisdocumenten, 2011/U51459, 26 April 2011, p. 4-5.

²¹⁶ European Data Protection Supervisor, Press release - Interoperability of databases: EDPS raises concerns on principal issues and calls for better analysis, 13 March 2006, p. 1.

²¹⁷ Commission of the European Communities, COM(2009) 13 final, Communication from the Commission to the European Parliament and the Council - Annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit in 2007, 26 January 2009, p. 3.

4. CONCLUSIONS

In 2009, the European Commission presented a proposal to open Eurodac for law enforcement purposes. This was met with considerable criticism by civil society, which pointed out several points of concern regarding data protection, the stigmatisation of asylum seekers, etc. The provisions on law enforcement access to Eurodac are however still advocated by the European Council and the European Commission, who point out their usefulness to reduce terrorism and serious crime. As such, this paper examined the arguments of the different stakeholders, who find themselves opposite to each other within the spectrum of migration and law enforcement.

The LEA's access proposal is an application of the 'Principle of availability', which was propagated in the Hague Programme. While this remains the leading principle for EU law enforcement policy, this proposal extends its meaning to non-law enforcement areas, *in casu* asylum policy. As such, it's an example of the increasing interweaving of terrorism and serious crime with asylum issues within the Area of Freedom, Security and Justice. Also in the West, migration issues are of increasing importance because of the increasing number of migrants, and EU member states have a legitimate interest in wanting to coordinate the arrival of those third country nationals. For these reasons the EU established the Dublin system, including the use of Eurodac, as part of a common European asylum system which aimed to take into account the vulnerable position of refugees, and share responsibilities between member states. Eurodac was then established to determine, with the use of fingerprints, which member state was responsible for processing an asylum claim. This evolution ran parallel to developments in the law enforcement area, with the establishment of the SIS database and the soon to be operational Prüm decision, SIS II, which are used to identify criminals. As such, information exchange between EU member states was digitalised, automated and improved. The fact that Eurodac stores similar information on persons as law enforcement databases, the idea emerged to also grant law enforcement authorities access to Eurodac to prevent, detect and investigate terrorism and serious crime, instead of limiting it to individuals competent for processing the asylum procedure. The finality of Eurodac is, however, completely different to law enforcement, with the result that the proposal not only has to deal with known sensitive issues that are encountered when a database is established, but equally with additional problems such as the fact that the data subjects are people often in need of protection and without a criminal record.

The proposal to give LEA's access to Eurodac consisted of a regulation as well as a council decision as it combined migration policy with law enforcement policy (respectively a first and a third pillar policy area). However, the Lisbon Treaty has been ratified in the meantime, thus the possible future proposal for LEA's access to Eurodac will have to be submitted in a different legal form. This does not mean that the problems mentioned in this paper do not have merits anymore: the balance between efficient and effective law enforcement on the one hand and legal safeguards and human rights on the other remains at the core of the discussion.

In the first place, the proposal fails to substantiate why it is necessary to focus on asylum seekers in the fight against terrorism and serious crime. There are no compelling reasons to focus only on this particular group of people, and the proposal to open up Eurodac for law enforcement purposes therefore risks being annulled by the European Court of Justice, similar to the case of *Hüber v. Germany*. Additionally, Eurodac might be very useful in the beginning, but 'established' terrorists are likely to circumvent Eurodac once it is being used

for law enforcement purposes. Lastly, the EU justifies its action by stating that certain member states already have access to their migration database for law enforcement purposes. Be that as it may, the conditions under which this is possible have not been mentioned, and these might be stricter than those proposed by the EU (certainly considering the broad access for Europol), and some countries have even declared access to asylum seekers' data for law enforcement purposes unconstitutional.

Secondly, the principles of data protection have not been complied with. With regard to the principle of legality and the purpose limitation principle, law enforcement access cannot be granted, as long as the Eurodac regulation is defined only as a migration policy tool. In 2010, the European Commission stated that current data protection rules contain too wide an exception to the purpose limitation principle. This is ignored, however, when advocating LEA's access to Eurodac. When considering the principles of proportionality and necessity, the proposal does not take into account the limitations set out by the ECtHR in its *Marper v. UK* case: the retention of biometric data from unconvicted persons for law enforcement purposes was deemed disproportional. Additionally, the European Commission did not wait for Prüm or SIS II to be operational, as to evaluate whether or not those might be effective enough to prevent, detect and investigate terrorism and serious crime. When it comes to the effective control on data, the Commission has included several provisions that limit the circulation of data, for example to third countries (which was important in the light of the non-refoulement principle).

Thirdly, the proposal might stigmatise asylum seekers even more than now. Although the link between asylum seekers and terrorism or serious crime has not been demonstrated, focussing on this particular group will logically lead to more criminal cases involving asylum seekers being solved, making them appear higher in criminal statistics. Equally, the ECtHR has prohibited similar measures before as the link between crime and the targeted group was not considered to be significant enough.

Fourthly, Eurodac has been identified as a qualitatively high database, which implies a low number of false hits. However, the number of wrongly identified persons should be researched further, as no relevant statistics are available and a higher number of false hits might render the proposal for LEA's access inefficient. Additionally, certain legal safeguards should be implemented in case a person would be wrongly identified.

Most points of concern that were highlighted by civil society are well-founded. What is more, the Commission did take into account some of those remarks and accordingly included them in the proposal, e.g. the prohibition of transferring asylum seekers' data to third countries or organisations. Taking into account the bigger picture however, the proposal must be seen as insufficiently taking into account different human rights and migration related matters. Certainly, some points of concern can be incorporated in a new updated proposal on LEA's access, such as legal safeguards for wrongly identified persons and the correct deletion of data of persons who have been granted residence status. Nonetheless, certain basic requirements such as those regarding data protection, the insufficient legal basis and the non-proven link between asylum seekers and terrorism and serious crime account for the fact that this proposal should not become permanent legislation. The European Union should reflect on which direction it wants to take: Europe has a well developed human rights system and tradition. This also seems the case for the Area of Freedom, Security and Justice, when looking at the attention that is given to victims' rights and minimum rights for the accused. The intertwining

of asylum policy and law enforcement however, shows that balancing law enforcement and human rights is not always easy, and sometimes fails to meet established standards.

* *

*

BIBLIOGRAPHY

Literature: books and articles

- Aas, K.F., *Globalization & crime*, Sage publications, Thousand Oaks, 2007, 220 p.
- Aus, J.P., Eurodac: a solution looking for a problem?, *European Integration online papers* (10) 2006, WWW <<http://www.eiop.or.at/eiop/index.php/eiop>>.
- Bauman, Z., *Globalization: the human consequences*, Polity Press, Cambridge, 1998, 136 p.
- Besters, M. and Brom, F.W.A., ‘Greedy’ information technology: the digitalization of the European Migration Policy, *European Journal of Migration and Law* (12) 2010, pp. 455-470.
- Boeles, P., Den Heijer, M., Lodder, G. and Wouters, K., *European Migration Law*, Intersentia, Mortsel, 2009, 638 p.
- Broeders, D., The new digital borders of Europe: EU databases and the surveillance of irregular migrants, *International sociology* (22) 2007, pp. 71-92.
- Brouwer, E., Data surveillance and border control in the EU - balancing efficiency and legal protection, in: Balzacq, T. and Carrera, S. (eds.), *Security versus freedom?: a challenge for Europe’s future*, Ashgate, Aldershot, 2006, pp. 137-154.
- Brouwer, E., Eurodac: its limitations and temptations, *European Journal of Migration and Law* (4) 2002, pp. 231-247.
- Carrera, S. and Merlino, M., *Assessing EU policy on irregular immigration under the Stockholm Programme*, Centre for European Policy Studies, 14 October 2010, 40 p., WWW <www.ceps.eu>.
- Castles, S. and Miller, M.J., *The age of migration: international population movements in the modern World*, Fourth edition, Palgrave Macmillan, Basingstoke, 2009, 369 p.
- Chalmers, D., Hadjiemmanuil, C., Monti, G. and Tomkins, A., *European Union Law*, Cambridge University Press, Cambridge, 2006, 1235 p.
- De Busser, E., *Data Protection in EU and US Criminal Cooperation, a substantive law approach to the EU internal and transatlantic cooperation in criminal matters between judicial and law enforcement authorities*, Maklu, Antwerpen, 2009, 474 p.
- Decorte, T., *Methoden van Criminologisch Onderzoek: Ontwerp en dataverzameling*, Gent, 2009, 495 p. (Syllabus).
- European Union Agency for Fundamental Rights, *Data Protection in the European Union: the role of national data protection authorities - strengthening the fundamental rights in the EU II*, Publications Office of the European Union, Luxembourg, 2010, 50 p.

Geyer, F., *Taking stock: databases and systems of information exchange in the area of freedom, security and justice*, Centre for European Policy Studies, May 2008, 43 p., WWW <www.ceps.eu>.

Greenslade, R., *Seeking scapegoats. The coverage of asylum in the UK press*, Institute for Public Policy Research, London, 2005, 39 p., WWW <http://www.ippr.org/ecomms/files/wp5_scapegoats.pdf>.

Guild, E., International terrorism and EU immigration, asylum and borders policy: the unexpected victims of 11 September 2001, in: Carr, F. and Massey, A. (eds.), *Public policy and the new European Agendas*, Edward Elgar Publishing, Cheltenham, 2006, pp. 233-248.

Guild, E., *Security and migration in the 21st century*, Polity Press, Cambridge, 2009, 218 p.

Guild, E., The Europeanisation of Europe's asylum policy, *International journal of refugee law* (3-4) 2006, pp. 630-651.

Harvey, D., *The condition of postmodernity: an enquiry into the origins of cultural change*, Blackwell, Oxford, 1990, 392 p.

Lodge, J., *Quantum surveillance and 'shared secrets' - a biometric step too far?*, Centre for European Policy Studies, 13 July 2010, 39 p., WWW <www.ceps.eu>.

Lodge, J., Transparency, justice and territoriality: the EU border challenge, in: Balzacq, T. and Carrera, S. (eds.), *Security versus freedom?: a challenge for Europe's future*, Ashgate, Aldershot, 2006, pp. 257-277.

Müller, F. and Richter, T., Report on the Bundesverfassungsgericht's (Federal Constitutional Court) Jurisprudence in 2005/2006, *German Law Journal* (9) 2008, p. 161-194.

Neale, P., Thapa, S. and Boyce, C., *Preparing a case study: a guide for designing and conducting a case study for evaluation input*, Pathfinder International, 2006, 16 p., WWW <http://www.pathfind.org/site/DocServer/m_e_tool_series_case_study.pdf?docID=6302>.

Papastergiadis, N., *The turbulence of migration: globalization, deterritorialization, and hybridity*, Polity Press, Cambridge, 2000, 256 p.

Thieleman, E., Why asylum policy harmonisation undermines refugee burden-sharing, *European journal of migration and law* (1) 2004, pp. 47-65.

Van der Ploeg, I., The illegal body: 'Eurodac' and the politics of biometric identification, *Ethics and Information Technology* (1) 1999, pp. 295-302.

Vermeulen, G., *Europese en internationale instellingen en organisaties relevant voor criminologie en strafrechtsbedeling*, Maklu, Antwerpen, 2006, 222 p.

Vermeulen, G., Het Europees aanhoudingsmandaat, *Tijdschrift voor mensenrechten*, 2002, pp. 3-7.

Vogel, D., McDonald, W., Düvell, F., Jordan, B., Kovacheva, V. and Vollmer, B., Police Cooperation in Internal Enforcement of Immigration Control: Learning from International Comparison. In: McDonald, W. (ed.), *Immigration, Crime and Justice. Sociology of Crime, Law and Deviance* (13) 2009, Emerald, pp. 207-244.

Yin, R., *Case Study Research: Design and Methods*, Fourth Edition, Sage Publications, Thousand Oaks, 2009, 240 p.

Policy documents: treaties, laws, reports, advisory opinions, working documents, etc.

APAP, J. and INCERTI, M., *Trust and co-operation in judicial, extradition, immigration and asylum matters - proceedings of a CEPS-SITRA network meeting*, Brussels, 23 March 2002, 26 p.

Assemblée Nationale - Commission des affaires européennes, Rapport d'information sur la deuxième phase de mise en œuvre du régime d'asile européen commun, 15 December 2009, 34 p.

Association of Chief Police Officers of England, Wales and Northern Ireland, Asylum Seekers Policing Guide, 2001.

Aus, J.P., *EU governance in an area of freedom, security and justice: logics of decision-making in the justice and home affairs council - working paper No. 15*, October 2007, 50 p., WWW <www.arena.uio.no/publications>.

Bigo, D., Carrera, S. And Guild, E., *What future for the area of freedom, security and justice? Recommendations on EU migration and borders policies in a globalising world*, March 2008, 4 p., WWW <www.ceps.eu>.

Commission of the European Communities, COM(2001) 720 final, Communication from the Commission to the Council and the European Parliament - Development of the Schengen Information System II, Brussels, 18 December 2001, 28 p.

Commission of the European Communities, COM (2003) 336 final, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - On immigration, integration and employment, Brussels, 3 June 2003, 58 p.

Commission of the European Communities, COM(2005) 597 final, Communication from the Commission to the Council and the European Parliament - on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs, Brussels, 24 November 2005, 11 p.

Commission of the European Communities, SEC(2005) 839, Commission staff working paper - Second Annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit, Brussels, 20 June 2005, 17 p.

Commission of the European Communities, COM(2007) 2999, Report from the Commission to the European Parliament and the Council on the evaluation of the Dublin system, Brussels, 6 June 2007, 13 p.

Commission of the European Communities, COM(2008) 0242, Proposal for a regulation of the European Parliament and 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), Brussels, 3 December 2008, 60 p.

Commission of the European Communities, COM(2008) 820, 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), Brussels, 3 December 2008, 67 p.

Commission of the European Communities, COM(2009) 13 final, Communication from the Commission to the European Parliament and the Council - Annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit in 2007, Brussels, 26 January 2009, 20 p.

Commission of the European Communities, COM(2009) 292 final, Communication from the Commission - Legislative package establishing an agency for the operational management of large-scale IT systems in the area of freedom, security and justice, Brussels, 24 June 2009, 5p.

Commission of the European Communities, COM(2009) 342, 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] (Recast version), Brussels, 10 September 2009, 74 p.

Commission of the European Communities, COM(2009) 344 final, Proposal for a Council Decision on requesting comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes, Brussels, 10 September 2009, 21 p.

Commission of the European Communities, COM(2009) 494 final, Report from the Commission to the European Parliament and the Council - Annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit in 2009, Brussels, 25 September 2009, 20 p.

Commission of the European Communities, COM(2010) 385 final, Communication from the Commission to the European Parliament and the Council - overview of the information management in the area of freedom, security and justice, Brussels, 20 July 2010, 53 p.

Commission of the European Communities, COM(2010) 415 final, Report from the Commission to the European Parliament and the Council - Annual report to the European Parliament and the Council on the activities of the EURODAC Central Unit in 2009, Brussels, 2 August 2010, 26 p.

Commission of the European Communities, COM(2010) 555, Amended proposal for a regulation of the European Parliament and 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), Brussels, 11 October 2010, 70 p.

Commission of the European Communities, COM(2010) 609 final, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of Regions - A comprehensive approach on personal data protection in the European Union, Brussels, 4 November 2010, 19 p.

Commission of the European Communities, SEC(2005) 839, Commission staff working paper - Second Annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit, Brussels, 20 June 2005, 17 p.

Commission of the European Communities, SEC(2006) 1170, Commission staff working document - Third Annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit, Brussels, 15 September 2006, 13 p.

Commission of the European Communities, SEC(2007) 1184, Commission staff working document - Annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit, Brussels, 11 September 2007, 49 p.

Commission of the European Communities, SEC(2009) 936, Commission staff working document - Accompanying document to the amended proposal for a regulation of the European Parliament and 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) and to the proposal for a Council Decision on requesting comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes - Impact assessment, Brussels, 10 September 2009, 59 p.

Commissioner for Human Rights, CommDH/IssuePaper(2010)1, Criminalisation of Migration in Europe: human rights implications, Strasbourg, February 2010, 51 p.

Commissioner for Human Rights, CommDH/IssuePaper(2008)3, Protecting the Right to privacy in the fight against terrorism, Strasbourg, 4 December 2008, 16 p.

Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data, ETS No. 108, Strasbourg, 28 January 1981.

Council Legal Service, Advice, 5546/93, JUR 25, 18 March 1993.

Council of the European Union, Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), 7 August 2007, L 205.

Council of the European Union, 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, 6 August 2008, OJ L 210.

Council of the European Union, 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 offences, 13 August 2008, OJ L 218.

Council of the European Union, 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, 25 February 2003, OJ C 50.

Council of the European Union, 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, 5 March 2002, OJ L 62.

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, 15 December 2000, OJ L 316.

Council of the European Union, Draft council conclusions on access to Eurodac by Member State police and law enforcement authorities, 8688/07, Brussels, 20 April 2007, 3 p.

Council of the European Union, Draft council conclusions on access to Eurodac by Member State police and law enforcement authorities as well as Europol, 10002/07, Brussels, 25 May 2007, 3 p.

Council of the European Union, EU-US informal JHA senior level meeting (22-23 January 2007, Berlin), 5655/07, Brussels, 26 January 2007, 13 p.

Council of the 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, 19 December 2006, OJ L 386, 12 p.

Council of the European Union, Outcome of proceedings of CATS on 25 and 26 October 2010, 16006/10, Brussels, 9 November 2010, 7 p.

Council of the European Union, Policy document concerning access to Eurodac by Member State's police and law enforcement authorities, 16982/06, Brussels, 20 December 2006, 3 p.

Council of the European Union, Press release - 3043rd Council meeting - Justice and Home Affairs, 15848/10, Brussels, November 2010, 24 p.

Council of the European Union, Press release - 3081st Council meeting - Justice and Home Affairs, 8692/11 provisional version, Luxembourg, April 2011, 22 p.

Council of the European Union, The Hague Programme: strengthening freedom, security and justice in the European Union, 3 March 2005, OJ C 53.

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, 23 November 1995, OJ L 281.

Eerste Kamer der Staten-Generaal, Verslag van een schriftelijk overleg vastgesteld 5 februari 2010, 23 490 FQ, 2010, 6 p.

Eurodac Supervision Coordination Group, Report of the First coordinated inspection, Brussels, 17 July 2007, 16 p.

Eurodac Supervision Coordination Group, Second Inspection Report, Brussels, 24 June 2009, 25 p.

European Council on Refugees and Exiles, Comments from the European Council on Refugees and Exiles on the European Commission proposal to recast the Dublin Regulation, Brussels, April 2009, 13 p.

European Council on Refugees and Exiles, LTT - The European Commission will present on the 8th of July a proposal to provide law enforcement authorities with access to Eurodac, 30 June 2009, 2 p.

European Council on Refugees and Exiles, *Report on the application of the Dublin II Regulation in Europe*, Brussels, March 2006, 11 p.

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 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], and on the Proposal for a Council Decision on requesting comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes, 10 April 2010, OJ C 92.

European Data Protection Supervisor, Opinion of the European Data Protection Supervisor on the communication from the Commission to the European Parliament and the Council - 'Overview of information management in the area of freedom, security and justice', 29 December 2010, OJ C 355.

European Data Protection Supervisor, Press release - Interoperability of databases: EDPS raises concerns on principal issues and calls for better analysis, 13 March 2006, 1 p.

European Parliament - Committee on Civil Liberties, Justice and Home Affairs, 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 (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)), 23 December 2010, 19 p.

European Parliament, Resolution on the alleged use of European countries by the CIA for the transportation and illegal detention of prisoners (provisional), P6_TA-PROV(2007)0032, 2007, 32 p.

European Parliament, Resolution on the fight against terrorism, P6_TA(2007)0612, 12 December 2007, Strasbourg, WWW.
<<http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P6-TA-2007-0612&language=EN>>.

European Parliament - Directorate-general for external policies of the Union, *Current challenges regarding respect of human rights in the fight against terrorism*, Brussels, April 2010, 40 p.

European Union Agency for Fundamental Rights, Data in focus report - multiple discrimination, Vienna, 2010, 20 p.

Europol, TE-SAT 2010 - EU terrorism situation and trend report, 2010, 56 p., WWW
<http://www.europol.europa.eu/publications/EU_Terrorism_Situation_and_Trend_Report_TE-SAT/Tesat2010.pdf>.

Fortescue, A., Combating illegal migration: from Tampere via Seville, *Policy briefs & recommendations: the Greek presidency conference on managing migration for the benefit of Europe*, May 2003, pp. 26-28.

General Secretariat of the Council of the EU, The Lisbon Treaty's impact on the Justice and Home Affairs (JHA) Council: More co-decision and new working structures, Brussels, December 2009, 4 p., WWW
<http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/111615.pdf>.

Guild, E., Carrera, S. and Eggenschwiler, A., *Informing the immigration debate*, May 2009, 4 p., WWW <www.ceps.eu>.

House of Commons - European Scrutiny Committee - Seventh Report of Session 2010-11, HC 428-vii, The Stationery Office, London, 23 November 2010, 81 p.

House of Lords - European Union Committee, Behind closed doors: the meeting of the G6 interior ministers at Heiligendamm - Report with evidence - 40th report of session 2005-06, The Stationery Office, London, 19 July 2006, 66 p.

House of Lords - European Union Committee, Prüm: an effective weapon against terrorism and crime? - Report with evidence - 18th report of session 2006-07, The Stationery Office, London, 9 May 2007, 98 p.

House of Lords - European Union Committee, The Treaty of Lisbon: an impact assessment - volume II: evidence - 10th report of session 2007-08, The Stationery Office, London, 13 March 2008, 479 p.

Koslowski, R., *Real challenges for virtual borders: the implementation of US-VISIT*, Migration Policy Institute, June 2005, 64 p.

Ministerie van binnenlandse zaken en koninkrijksrelaties, 2b or not 2b - evaluatierapport biometrieproef, 2005, 83 p.

Ministerie van binnenlandse zaken en koninkrijksrelaties, Brief van minister J.P.H. Donner betreffende reisdocumenten, 2011/U51459, 26 April 2011, 5 p.

Select Committee on Home Affairs, Letter to the Chairman of the Committee from Rt Hon Charles Clarke MP, Secretary of State for the Home Department, 21 February 2005, WWW <<http://www.publications.parliament.uk/pa/cm200405/cmselect/cmhaff/321/321we02.htm>>

Standing Committee of experts on international immigration, refugee and criminal law, Note on the proposal of the JHA Council to give law enforcement authorities access to Eurodac, CM0712-IV, Utrecht, 18 September 2007, 3 p.

Standing Committee of experts on international immigration, refugee and criminal law, Proposal to give law enforcement authorities access to Eurodac, CM0714, Utrecht, 6 November 2007, 5 p.

Standing Committee of experts on international immigration, refugee and criminal law, The amended proposal for the Eurodac Regulation (COM (2009) 342) and the Decision on requesting comparisons with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (COM (2009) 344), CM0910, Utrecht, 30 December 2009, 8 p.

Standing Subcommittee on European Union Affairs, Statement to the European Commission, 17 April 2009, 6 p., WWW <http://www.ipex.eu/ipex/webdav/site/myjahiasite/users/atnatcorresp/public/Statement_Asylum.en.pdf>.

Statewatch, *Statewatch bulletin vol. 3 no 1*, January-February 1993, 13 p., WWW <www.statewatch.org>.

Treaty of Amsterdam, 10 November 1997, OJ C 340.

Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, 17 December 2007, OJ C 306.

Treaty on European Union, 29 July 1992, OJ C 191.

Tweede Kamer der Staten-Generaal, Aangangsels van de Handelingen - Vragen gesteld door de leden der kamer, met daarop door de regering gegeven antwoorden - 317, vergaderjaar 2006-2007, WWW

<http://www.eerstekamer.nl/eu/behandeling/20061115/kamervragen_klaas_de_vries_pvda/f=/vhn5inhraj2w.pdf>.

UNHCR, *Asylum levels and trends in industrialized countries 2009 - statistical overview of asylum applications lodged in Europe and selected non-European countries*, Geneva, 2010, 36 p., WWW <<http://www.unhcr.org/4ba7341a9.html>>.

UNHCR, *The application of the "safe third country" notion and its impact on the management of flows and on the protection of refugees - background paper no. 2*, Geneva, May 2001, 3 p.

UNHCR, 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, 25 p.

UNHCR, UNHCR's recommendations to the Slovenian presidency of the European Union, 10 December 2007, 9 p.

United States' National Research Council, *Protecting individual privacy in the struggle against terrorists: a framework for program assessment*, 2008, 352 p., WWW <<http://www.nap.edu/catalog/12452.html>>.

Case-law:

Asylum and Immigration Tribunal, YI (previous claims - fingerprint match - Eurodac) Eritrea [2007] UKAIT 00054, 24 May 2007, WWW <<http://www.unhcr.org/refworld/pdfid/467bf1142.pdf>>.

Bundesverfassungsgericht, 1 BvR 518/02, judgment, 4 April 2006, WWW <<http://www.bverfg.de/entscheidungen/>>.

European Court of Human rights, *Connors v. The United Kingdom*, judgment, 27 May 2004, WWW <<http://www.echr.coe.int/echr/en/hudoc/>>.

European Court of Human Rights, *Gillow v. The United Kingdom*, judgment, 24 November 1986, WWW <<http://www.echr.coe.int/echr/en/hudoc/>>.

European Court of Human Rights, *Hatton and others v. The United Kingdom*, judgment, 2 October 2001, WWW <<http://www.echr.coe.int/echr/en/hudoc/>>.

European Court of Human Rights, *Leander v. Sweden*, judgment, 26 March 1987, WWW <<http://www.echr.coe.int/echr/en/hudoc>>.

European Court of Human Rights, *M.S.S. v. Belgium and Greece*, judgment, 21 January 2011, WWW <<http://www.echr.coe.int/echr/en/hudoc>>.

European Court of Human Rights, *S. and Marper v. The United Kingdom*, judgment, 4 December 2008, WWW <<http://www.echr.coe.int/echr/en/hudoc>>.

European Court of Human Rights, *T.I. v. UK*, admissibility decision, 7 March 2000, WWW <<http://www.echr.coe.int/echr/en/hudoc>>.

European Court of Justice, *Joined Cases C-317/04 and C-318/04 (European Parliament v. Council and Commission)*, Judgment of the Grand Chamber, 30 May 2006, ECR I-4721.

European Court of Justice, *Joined Cases C-465/00, C-138/01 and C-139/01 (Rechnungshof and Österreichischer Rundfunk, Wirtschaftskammer Steiermark, Marktgemeinde Kaltenleutgeben, Land Niederösterreich, Österreichische Nationalbank, Stadt Wiener Neustadt, Austrian Airlines, Österreichische Luftverkehrs-AG and between Christa Neukomm, Joseph Laueremann and Österreichischer Rundfunk)*, Preliminary ruling, 20 May 2003, WWW <<http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=en>>.

European Court of Justice, *Case C-524/06 (Heinz Huber v. Bundesrepublik Deutschland)*, preliminary ruling, 16 December 2008, WWW <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62006J0524:EN:NOT>>.

French Constitutional Council, *Decision 97-389*, Act making various provisions in respect of immigration, 22 April 1997, WWW <<http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/97389DCa97389dcpdf>>.

United States Supreme Court, *Kolender, Chief of Police of San Diego, et al. v. Edward Lawson*, 461 U.S. 352, 2 May 1983, WWW <<http://supreme.justia.com/us/461/352/case.html>>.

Gray Literature: newspaper articles, dissertations, etc.

Eechaudt, V., *De impact van het kaderbesluit 2006/960/JHA op de informatie-uitwisseling tussen rechtshandavingsautoriteiten binnen de EU en de implicaties voor Europol*, Ghent, 2009. (Bachelor dissertation).

Eechaudt, V., *De voorbereidingen van het Stockholm Programma geanalyseerd*, Ghent, 2010, WWW <http://lib.ugent.be/fulltxt/RUG01/001/458/143/RUG01-001458143_2011_0001_AC.pdf>. (Master dissertation).

Harmit Athwal, 'Analysis: Who are the terrorists?', Institute of Race Relations, 12 August 2004, WWW <<http://www.irr.org.uk/2004/august/ak000007.html>>.

Vincent, E., *Les nouvelles routes de la Méditerranée*, *Le Monde*, 24 June 2010.

Crosbie, J., Commission wants to open up Eurodac database to police, *European Voice*, 2 July 2009.

* *

*

ANNEXES

1. Proposal for a Council Decision on access to Eurodac, COM(2009) 344
2. Proposal for a Regulation establishing Eurodac, COM(2009) 342

EN

EN

EN



COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels,
COM(2009) 344/3

2009/xxxx (CNS)

Proposal for a

COUNCIL DECISION

**on requesting comparisons with EURODAC data by Member States' law enforcement
authorities and Europol for law enforcement purposes**

{COM(2009) 342}
{SEC(2009) 936}
{SEC(2009) 937}

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

- **Grounds for and objectives of the proposal**

Information about citizens of EU Member States and about third country nationals is available in many forms and systems in the Member States and at EU level. National and European instruments lay down the rules and conditions under which law enforcement authorities can have access to this information in order to carry out their lawful tasks.

Fingerprint data is especially useful information for law enforcement purposes, as it constitutes an important element in establishing the exact identity of a person. The usefulness of fingerprint databases in fighting crime is a fact that has been repeatedly acknowledged.

Fingerprint data of asylum seekers are collected and stored in the Member State in which the asylum application was filed, as well as in EURODAC. In all Member States that replied to the questionnaire of the Commission services, the law enforcement authorities had direct or indirect access to their national databases that contain the fingerprints of asylum seekers for the purpose of fighting crime. During the consultation of experts it became clear that those national law enforcement authorities that consult national databases containing fingerprints of asylum seekers for criminal investigations consider the hit rate significant.

However, while Member States successfully access asylum seekers fingerprints on a national level, it seems that access to asylum seekers fingerprint databases of other Member States is more problematic. The reason is that there is a structural information and verification gap since there is currently no single system that is accessible to law enforcement authorities which enables to determine the Member State that has information on an asylum seeker. If a query of a national Automated Fingerprint Identification Systems (AFIS) using the Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (Prüm Decision) which will be implemented by Member States by June 2011 does not result in a "hit", it is not certain that no information is available in a Member State. Therefore, law enforcement authorities will not only remain ignorant about whether or not information is available at all and in which Member State, but often also whether this information relates to the same person. Law enforcement officials will only know whether information is available in a database of another Member State if their judicial authorities issue a request for mutual legal assistance requesting the other Member State to query their databases and send the relevant information.

- **General context**

The Hague Programme stated that the exchange of information to strengthen security should be improved. One of the ideas contained in the Programme is to make full use of new technology, inter alia - where appropriate - by direct (on-line) access for law enforcement authorities, including for Europol, to existing central EU databases.

The conclusions of the Mixed Committee of the JHA Council of 12-13 June 2007 considered that, in order to fully achieve the aim of improving security and to enhance the fight against terrorism, access under certain conditions to EURODAC should be granted to Member States' police and law enforcement authorities, as well as Europol, in the course of their duties in relation to the prevention, detection and investigation of terrorist offences and other serious criminal offences. It therefore invited the Commission to present as soon as possible the necessary proposals to achieve this aim.

The absence of the possibility for law enforcement authorities to access EURODAC to combat terrorism and other serious crime was also reported as a shortcoming in the Commission Communication to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs of 24 November 2005.

The existing instruments on exchange of law enforcement information do not allow to timely determine with sufficient certainty whether a Member State actually holds fingerprint data of an asylum seeker. This means that without any action at EU level, law enforcement authorities will continue to remain ignorant about whether or not information on a fingerprint is available at all, in which Member State information is available, and whether information relates to the same person. Without efficient and reliable means to determine whether or not information is available in another Member State the action of public authorities either becomes prohibitively expensive or seriously jeopardises the application of the law because no further efficient and reasonable action to determine a person's identity can be taken.

- **Existing provisions in the area of the proposal**

Council Regulation (EC) No 2725/2000 of 11 December 2000 established 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention (the 'Eurodac' Regulation). On 3 December 2008 the Commission adopted a proposal to amend the EURODAC regulation aimed at making the EURODAC system more efficient.

There are currently some EU instruments that permit consultation of fingerprints and other law enforcement data held by one Member State by another Member State.

The first instrument that is likely to be used for consultations regarding fingerprints is the Prüm Decision.. On the basis of this Council Decision the Member States' grant each other automated access inter alia to national AFIS on the basis of a hit/no hit request. If a query on the basis of the Prüm Decision produces a hit, supplementary information, including personal data, can be obtained in the Member State that recorded the fingerprint in its national AFIS using national law, including mutual legal assistance.

While this procedure might be successful for those Member States that store fingerprints of asylum seekers together with other fingerprints collected by law enforcement authorities in a national AFIS, it will be unsuccessful for those Member States that do not store fingerprints of asylum seekers in their national AFIS unless they are related to crime.

Another instrument that could be used for consultations regarding fingerprints is

Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities (FWD 2006/960). This instrument facilitates the exchange of information (the fingerprint as well as the supplementary information) that is held or is available to law enforcement authorities in Member States. This instrument is operational as from 18 December 2008.

The last instrument that Member States could use is mutual legal assistance under which the judicial authorities of the Member States can seek access to criminal and non-criminal fingerprint collections, including on asylum seekers on the basis of the Convention on Mutual Assistance in Criminal Matters.

The last two instruments cannot be used when the Member State that holds data on a fingerprint is not known. Currently no system exists which could be used to identify such Member State.

- **Consistency with the other policies and objectives of the Union**

The proposal is fully in line with the overall objective of creating a European area of freedom, security and justice. In particular, this proposal was subject to in-depth scrutiny to ensure that its provisions are fully compatible with fundamental rights and notably the right to asylum and the protection of personal data as enshrined respectively in Article 8 (protection of personal data) and 18 (right to asylum) of the Charter of Fundamental Rights of the EU as reflected in the Impact Assessment accompanying this proposal.

With regard to the special situation of persons seeking international protection, the concern was raised that data extracted from EURODAC for law enforcement purposes could end up in the hands of the countries from which the applicants fled and fear persecution. This could have adverse effects on the applicant, his relatives and friends, thus potentially discouraging refugees from formally applying for international protection in the first place. As a result of this scrutiny, the proposal contains a specific prohibition of sharing personal data obtained pursuant to this proposal with third countries, organisations or entities. In addition, an extensive monitoring and evaluation mechanism of the proposal is foreseen. This evaluation will include whether the operation of the Decision will have led to the stigmatisation of persons seeking international protection. Furthermore, to keep the interference with the right to protection of personal data legitimate and proportional, strict access conditions are provided which also exclude that EURODAC fingerprint are searched on a routine basis. The proposal is also fully compatible with data protection principles since the Council Framework Decision on the Protection of Personal Data processed in the Framework of Police and Judicial Co-operation in Criminal Matters 2008/977/JHA applies to it. This Framework Decision lays down the principles that Member States must abide by when processing data retrieved from an EU database, such as EURODAC, while at the same time requires Member States to impose effective sanctions for violations of the data protection principles.

2. CONSULTATION OF INTERESTED PARTIES AND IMPACT ASSESSMENT

- **Consultation of interested parties**

Consultation methods, main sectors targeted and general profile of respondents

The Commission consulted the States applying the Dublin acquis, i.e. the Member States, Iceland, Norway and Switzerland, as well as to Europol by way of two questionnaires and an expert meeting which took place in Brussels on 25-26 September 2007, during which the experts had the opportunity to clarify the replies to the questionnaire and express further views.

Secondly, the Commission consulted the following intergovernmental organisations, non-governmental organisations and other scientific experts working in the area of asylum law/policy, fundamental rights and protection of personal data during a meeting in Brussels on 8 October 2007. MEPs Cavada, Klamt and Ludford also participated at the same meeting.

Finally, the Commission consulted representatives of the national data protection authorities of the States that implement the Dublin acquis, as well as the Joint Supervisory Body of Europol and the European Data Protection Supervisor during a meeting held in Brussels on 11 October 2007.

Summary of responses and how they have been taken into account

The consultation process had a major impact on shaping the legislative proposal. More specifically, such impact affected the choice of the legislative option and the various parameters of the option. The consultations showed that the Member States were very favourable to having the possibility to compare fingerprints with EURODAC for law enforcement purposes, while civil liberties and asylum NGOs were not very favourable. The proposal presents a balance on the positions of the various interested groups, by containing several guarantees and limits.

- **Collection and use of expertise**

There was no need for external expertise.

- **Impact assessment**

The Impact Assessment considered three options, and a number of sub-options. The options was a no action option, a legislative option for making it possible to request the comparison with EURODAC data for law enforcement purposes and a legislative option for making it possible to request the comparison with EURODAC data for law enforcement purposes while at the same time regulating the exchange of supplementary information following a successful 'hit' from EURODAC. A fourth option was originally considered but rejected as it would entail disproportionate costs.

Between the "no action" option and the legislative proposal options, the legislative proposal options present clear advantages. Access of law enforcement authorities to EURODAC is the only timely, accurate, secure and cost-efficient way to identify

whether and if so where data about asylum seekers are available in the Member States. No reasonable efficient alternative exists to EURODAC to establish or verify the exact identity of an asylum seeker that allows law enforcement authorities to obtain the same result. This unique identification is essential for law enforcement authorities in order to prevent and combat terrorism and serious crime involving third country nationals, as well as to protect victims of terrorism or serious crime. Access to 'Eurodac' cannot be considered disproportionate to the aims to be achieved.

Between the two options involving legislative measures, both options present the same impacts on fundamental rights. The third option would make supplementary information on the asylum seeker available between Member States through a special procedure where such is requested, while the second option would use the existing instruments to facilitate access to such supplementary information. Even though the achievement of the objectives would be more effective under the third option, it is considered that the costs of implementing the third option would be higher compared to the second option.

In addition, currently there are no indications that current instruments on exchange of law enforcement information would not be a sufficient instrument for the exchange of supplementary information.

The Commission carried out an impact assessment listed in the Work Programme, whose report is accessible on

3. LEGAL ELEMENTS OF THE PROPOSAL

- **Summary of the proposed action**

The proposed action establishes the basis for the right of Member States as well as Europol to request a comparison of fingerprint data or a latent with EURODAC data. A successful comparison will result in a 'hit' reply from EURODAC, which will be accompanied by all data that is held in EURODAC regarding the fingerprint. Requests for supplementary information following a hit would not be regulated in the proposed Council Decision but rather be covered by existing instruments on the exchange of law enforcement information.

The scope of the proposal will be the fight against terrorist offences and serious criminal offences, such as trafficking in human beings and drugs.

Even though currently EURODAC does not provide the possibility to search the database on the basis of a latent, this search facility can be added to the EURODAC system under the Biometric Matching System (BMS) project. This search facility is very important from a law enforcement point of view, since in most cases it is only possible to find latents at a crime scene under investigation.

- **Legal basis**

The Treaty on European Union, and in particular Articles 30(1)(b) and 34(2)(c).

- **Subsidiarity principle**

The subsidiarity principle applies insofar as the proposal does not fall under the exclusive competence of the Community.

The objectives of the proposal cannot be sufficiently achieved by the Member States for the following reason(s).

The proposed actions require an amendment of the EURODAC Regulation in order to add a secondary purpose to it, that of using EURODAC data in the fight against terrorism and crime. This amendment can only be proposed by the Commission. Without this amendment, the Member States have no right to act.

Any action undertaken by Member States alone is likely to be prohibitively expensive and disproportional.

Community action will better achieve the objectives of the proposal for the following reason(s).

The right to consult EURODAC is the simplest, most proportionate and least expensive way to close the identified information gap.

The proposed measures merely permit the request for comparison with EURODAC data. The further cooperation and exchange of information is left to current instruments and to the Member States.

The proposal therefore complies with the subsidiarity principle.

- **Proportionality principle**

The proposal complies with the proportionality principle for the following reason(s).

Access of law enforcement authorities to EURODAC is the only timely, accurate, secure and cost-efficient way to identify whether and if so where data about asylum seekers are available in the Member States. No reasonable efficient alternative exists to EURODAC to establish or verify the exact identity of an asylum seeker that allows law enforcement authorities to obtain the same result. The proposed measures focus on the essentials of the right to consultation, and do not go beyond what is proportionate.

The proposed measure involves the least costs on the Community and the Member States, as it uses existing databases and existing information sharing structures and does not seek to create new such systems.

- **Choice of instruments**

Proposed instruments: other.

Other means would not be adequate for the following reason(s).

Since fundamental rights are at stake, other regulatory means than a Decision under Title VI TEU would not be appropriate.

4. BUDGETARY IMPLICATION

The proposal would entail a technical amendment to EURODAC in order to provide the possibility to carry out a comparison on the basis of a latent.

5. ADDITIONAL INFORMATION

- **Review/revision/sunset clause**

The proposal includes a review clause.

Proposal for a

COUNCIL DECISION

on requesting comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on European Union, and in particular Article 30(1)(b) and 34(2)(c) thereof,

Having regard to the proposal from the Commission,

Having regard to the opinion of the European Parliament¹,

Whereas:

- (1) The Hague Program on strengthening freedom, security and justice in the European Union, as adopted by the European Council on 4 November 2004, asked for improvement of the cross-border exchange of data, also by extending the access to existing data filing systems of the European Union.
- (2) 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 established by the Council Regulation (EC) No .../... [*new Eurodac*]² 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 Decision, for comparison by the designated authorities of Member States and Europol.
- (3) 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 Affairs³ 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

¹ OJ C , , p. .

² OJ L , , p. .

³ COM(2005) 597, 24.11.2005.

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.

- (4) 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)⁴.
- (5) This Decision complements Regulation (EC) No [.../...] [*new EURODAC*], insofar as it provides for a legal basis under Title VI of the Treaty establishing the European Union to authorise requests for comparison with EURODAC data by Member States authorities and Europol.
- (6) Since EURODAC has been established to facilitate the application of the Dublin Regulation, 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.
- (7) 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.
- (8) This Decision 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.
- (9) 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

⁴ OJ L 121, 15.5.2009, p. 37

terrorism⁵ 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 States⁶.

- (10) 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 verifying authorities should be responsible for ensuring strict compliance with the conditions for access as established in this Decision. 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 the verifying authority should process the request immediately and only do the verification afterwards.
- (11) For the purposes of protection of personal data, and in particular to exclude mass 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 crime⁷ (Prüm Decision) have returned negative results. Such 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.
- (12) The 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 matters⁸ applies to the personal data which are processed pursuant to this Decision.
- (13) 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 the Dublin Regulation applies, in order to ensure that Member States have the possibility of cooperating with such third countries for the purposes of this Decision.

⁵ OJ L 164, 22.6.2002, p. 3.

⁶ OJ L 190, 18.7.2002, p. 1.

⁷ OJ L 210, 6.8.2008, p. 1.

⁸ OJ L 350, 30.12.2008, p. 60.

- (14) 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 Joint Supervisory Body set up by the Europol Decision should monitor the lawfulness of data processing activities performed by EUROPOL.
- (15) 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 data⁹ and in particular Articles 21 and 22 thereof concerning confidentiality and security of processing apply to the processing of personal data by the Community institutions and bodies when carrying out their responsibilities in the operational management of EURODAC in the exercise of activities all or part of which fall within the scope of Community law.
- (16) The effective application of this Decision should be evaluated at regular intervals.
- (17) Since the objectives of this decision, namely the creation of conditions for requests for comparison with data stored in the EURODAC central database by Member States' designated authorities and by Europol cannot be sufficiently achieved by the Member States and can, therefore, by reason of the scale and effects of the action, be only achieved at the level of the European Union, the Council may adopt measures in accordance with the principle of subsidiarity, referred to in Article 2 of the Treaty on European Union and defined in Article 5 of the Treaty establishing the European Community. In accordance with the principle of proportionality as set out in those Articles, this Decision does not go beyond what is necessary in order to achieve those objectives.
- (18) In accordance with Article 47 of the Treaty on the European Union, this Decision does not affect the competences of the European Community, in particular as exercised in Regulation (EC) No [.../...] [*new EURODAC*]¹⁰ and in 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 movement of such data¹¹.
- (19) This Decision respects the fundamental rights and observes the principles reflected in particular in the Charter of Fundamental Rights of the European Union and notably the right to protection of personal data and the right to asylum. This Decision should be applied in accordance with these rights and principles,

⁹ OJ L 8, 12.1.2001, p. 1.

¹⁰

¹¹ OJ L 281, 23.11.1995, p. 31.

HAS ADOPTED THIS DECISION:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter and scope

This Decision 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.

Article 2

Definitions

1. For the purposes of this Decision, the following definitions shall apply:
 - (a) 'EURODAC' means the database as established by Regulation (EC) No [.../...] *[new EURODAC]*;
 - (b) 'Europol' means the European Police Office as established by Council Decision [.../.../ JHA];
 - (c) 'EURODAC data' means all fingerprint data stored in the central database in accordance with Article 9 and Article 14(2) of *[new EURODAC]*;
 - (d) 'terrorist offences' means the offences under national law which correspond or are equivalent to the offences referred to in Articles 1 to 4 of Council Framework Decision 2002/475/JHA;
 - (e) '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;
 - (f) '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;
 - (g) 'National Access Point' is the designated national system which communicates with the Central System as referred to in Article 4(2) of the *[new EURODAC]*;
 - (h) Management Authority means the entity responsible for the operational management of EURODAC referred to in Article 5 of the *[new EURODAC]*.

2. The definitions in Regulation (EC) No [...] [new *EURODAC*] shall also apply.

Article 3

Designated authorities

1. Member States shall designate the authorities which are authorised to access EURODAC data pursuant to this Decision. 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 dealing especially with national security issues.
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 4

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. Verifying authorities shall not include agencies or units dealing especially with national security issues.
2. The verifying authority shall ensure that the conditions for requesting comparisons of fingerprints with EURODAC data are fulfilled.
3. 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 5

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.

CHAPTER II

PROCEDURE FOR COMPARISON AND DATA TRANSMISSION

Article 6

Procedure for comparison of fingerprint data with EURODAC data

1. The designated authorities referred to in Article 3(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 7 or Article 8, 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 7 or Article 8 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 which have accessed it and they shall inform the verifying authority of such destruction.

Article 7

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 the Council Decision 2008/615/JHA¹² 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;

¹² OJ L 210, 6.8.2008, p. 1.

- (b) the comparison is necessary in a specific case;
 - (c) 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.
2. Requests for comparison with EURODAC data shall be limited to searching with fingerprint data.

Article 8

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.

Article 9

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 to the Regulation (EC) No [.../...] [*new EURODAC*], in order to ensure that the comparison can be carried out by means of the computerised fingerprint recognition system.

CHAPTER III

PERSONAL DATA PROTECTION

Article 10

Protection of personal data

1. The Framework Decision 2008/977/JHA is applicable to the processing of personal data under this Decision.

2. The processing of personal data by Europol pursuant to this Decision shall be in accordance with the [Europol] Decision [.../.../JHA] and the rules adopted in implementation thereof and shall be supervised by the independent joint supervisory body established by Article 34 of that Decision.
3. Personal data obtained pursuant to this Decision 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 Decision 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 Decision 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.

Article 11
Data security

1. The Member State responsible shall ensure the security of the data during all transmissions of data under this Decision to the designated authorities and when received by them.
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;
 - (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 deletion of stored personal data (storage control);
 - (e) prevent the unauthorised processing of data in EURODAC and any unauthorised modification or deletion of data processed in EURODAC (control of data processing);
 - (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 to request comparisons with data held in EURODAC create profiles describing the functions and responsibilities of persons who are authorised to access, enter, update, delete and search the data and make these profiles available to the National Supervisory Authorities designated under Article 25 of the 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 deletion 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 appropriate 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 Decision (self-auditing).

Article 12

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 Decision 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 conditions of Article 13 of the Framework Decision 2008/977/JHA are fulfilled.

Article 13

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 Decision 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;
 - (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 6(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 17. 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.

TITLE IV

FINAL PROVISIONS

Article 14 **Costs**

Each Member State and Europol shall set up and maintain at their expense, the technical infrastructure necessary to implement this Decision, and be responsible for bearing its costs resulting from requests for comparison with EURODAC data for the purposes of this Decision.

Article 15 **Penalties**

Member States and Europol shall take the necessary measures to ensure that any use of EURODAC data contrary to the provisions of this Decision is punishable by penalties, including administrative and/or criminal penalties, which are effective, proportionate and dissuasive.

Article 16

Notification of designated authorities and verifying authorities

1. By [three months after the date of entry into force of this Decision] at the latest each Member State shall notify the Commission and the General Secretariat of the Council 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 Decision] at the latest each Member State shall notify the Commission and the General Secretariat of the Council 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 Decision] at the latest Europol shall notify the Commission and the General Secretariat of the Council 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.

Article 17

Monitoring and evaluation

1. Each Member State and Europol shall prepare annual reports on the effectiveness of the comparison of fingerprint data with EURODAC data, 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.
2. Three years after the entry into force of this Decision and every four years thereafter, the Commission shall produce an overall evaluation of this Decision. This evaluation should include an examination of the results achieved against objectives and an assessment of the continuing validity of the underlying rationale, and shall make any necessary recommendations. The Commission shall submit the evaluation report to the European Parliament and the Council.
3. The Management Authority, Member States and Europol shall provide the Commission the information necessary to draft the evaluation reports referred to in paragraph 2. This information shall not jeopardise working methods nor include information that reveals sources, staff members or investigations of the designated authorities.

Article 18

Entry into force and date of application

1. This Decision shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.
2. This Decision shall apply from the date referred to in Article 33(2) of Regulation [...] [*new EURODAC*].

Done at Brussels,

For the Council

The President

EN

EN

EN



COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels,
COM(2009) 342

2008/0242 (COD)

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]

(Recast version)

{COM(2009) 344}

{SEC(2009) 936}

{SEC(2009) 937}

EXPLANATORY MEMORANDUM

1. INTRODUCTION

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. A recast proposal which aimed at amending this Regulation was adopted by the Commission in December 2008² (hereafter the December 2008 proposal).

This proposal was designed to ensure a more efficient use of the EURODAC database for the purpose of determining the Member State responsible for examining an asylum claim (i.e. provide a more efficient support to the application of the Dublin Regulation) and to properly address data protection concerns.

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 justice³ (hereinafter: IT Agency).

The December 2008 proposal also proposed to repeal the Implementing Regulation and to include its content in the EURODAC Regulation.

Finally, changes were introduced to take into account developments in the asylum *acquis* and technical progress which took place since the adoption of the Regulation in 2000.

The proposal was sent to European Parliament and the Council on 3 December 2008. The European Parliament referred the proposal to its Committee on Civil Liberties, Justice and Home Affairs (LIBE).

At its sitting on 7 May 2009, the European Parliament adopted a legislative resolution⁴ endorsing the Commission proposal subject to a number of amendments.

2. AMENDED PROPOSAL

The current proposal amends the December 2008 proposal 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

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.

⁴ Establishment of 'Eurodac' for the comparison of fingerprints (recast), P6_TA(2009)0378.

prevention, detection and investigation of terrorist offences and other serious criminal offences.

In case a person suspected to have committed an act of terrorism or a serious crime has been previously registered as an asylum seeker but is not in any other database or is only registered with alphanumerical data (which might be incorrect, for example if that person has given a wrong identity or used forged documents), the only information available to identify him/her might be the biometric information contained in EURODAC.

The intention is now to allow consultation of EURODAC by law enforcement authorities for the purpose of prevention, detection and investigation of terrorist offences and other serious criminal offences. In order to do this it is necessary to amend the EURODAC Regulation to include explicitly this additional purpose.

Therefore, the current proposal introduces a bridging clause to permit this access for law enforcement purpose as well as the necessary accompanying provisions and amends the December 2008 proposal.

Comparison of fingerprints in possession of Member States' designated law enforcement authorities and Europol with those stored in the EURODAC database will only be possible in case of necessity of such comparison in a specific case under well-defined circumstances. Provisions on access to data and data security take into account access for law enforcement purposes.

Since the European Parliament issued its report on the recast proposal in first reading on 7 May 2009, it is understood that it should have the possibility of issuing a new report in first reading on the current proposal which includes the content of the December 2008 proposal alongside the abovementioned modifications.

This proposal is presented at the same time as the Proposal for a Council Decision on requesting comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes (hereafter: Council Decision No [.../...]JHA [*EURODAC law enforcement Decision*], spelling out the exact modalities of access for law enforcement purposes .

General context

The Hague Programme called for the improvement of the cross-border exchange of data by law enforcement authorities, also by extending the access to existing data filing systems of the European Union.

The conclusions of the Mixed Committee of the JHA Council of 12-13 June 2007 invited the Commission to present as soon as possible the necessary proposals to achieve the aim of granting access under certain conditions to EURODAC to Member States' law enforcement authorities and Europol, to assist them in the course of their duties in relation to the prevention, detection and investigation of terrorist offences and other serious criminal offences.

The impacts of the access for law enforcement purposes introduced in the present amended proposal are assessed by an Impact Assessment attached to this proposal.

3. CONSISTENCY WITH OTHER POLICIES

This proposal is fully in line with the Hague programme of 2004, the European Pact on Immigration and Asylum endorsed by the European Council of 15-16 October 2008 and the Charter of Fundamental Rights of the European Union, in particular as regards the right to asylum and protection of personal data.

Furthermore, this proposal is in line with the Commission's Communication to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs⁵, which noted that the Council and the law enforcement community identifies the absence of access by internal security authorities to VIS, SIS II immigration and EURODAC data as a shortcoming, which results in a serious gap in the identification of suspected perpetrators of terrorist or serious crimes. Since the adoption of the Communication in 2005, the VIS Decision was adopted in order to grant law enforcement authorities and Europol access to that database.

4. COMPLIANCE WITH THE CHARTER OF FUNDAMENTAL RIGHTS

During the drafting exercise, due attention was given to fundamental rights. The right to asylum and protection of personal data were considered in the Impact Assessment attached to the proposal.

As regards the right to asylum, amendments to the provisions of the Regulation on the *information to be given to asylum seekers on the application of the Dublin system* enables them to effectively exercise their right to asylum. The new provision that requires Member States to *indicate in EURODAC the fact that they apply the discretionary clauses* of the Dublin Regulation, facilitates communication amongst Member States and therefore prevents uncertainty for the asylum seeker, by making clarity about which Member States handles his case. As regards the protection of personal data, by allowing for *efficient management of deletions of data*, the proposal ensures that no data should be kept in a form which allows the identification of data subjects for longer than is necessary for the purposes for which data were collected. The same principle is underpinning the amendment aligning the *storage period for data on third country nationals or stateless persons fingerprinted in connection with the irregular crossing of an external border* with the period until which the Dublin Regulation allocates responsibility on the basis of that information.

With regard to the special situation of persons seeking international protection, for instance, the concern was raised that data extracted from EURODAC for law enforcement purposes could end up in the hands of the countries from which the applicants fled and fear persecution. This could have adverse effects on the applicant, his relatives and friends, thus potentially discouraging refugees from formally applying for international protection in the first place. As a result of this scrutiny, the proposal contains a specific prohibition of sharing personal data obtained pursuant to this proposal with third countries, organisations or entities. In addition, an extensive monitoring and evaluation mechanism of the proposal is foreseen. This evaluation will include whether the operation of the search functionality for law enforcement purposes will have led to the stigmatisation of persons seeking international protection. Furthermore, in order to ensure that the processing of personal data for law enforcement

⁵ COM(2005) 597.

purposes does not contravene the fundamental right to the protection of personal data, in particular the necessity and the proportionality, the proposal sets out strict conditions with regard to the access to EURODAC data by law enforcement authorities, which excludes that the EURODAC database be searched on a routine basis. The proposal also prohibits the further processing for law enforcement purposes by clearly defining the kind of crimes which will allow access to EURODAC. It also lays down strict security measures to ensure the security of personal data processed and establishes supervision of the processing activities by independent public data protection authorities. The proposal also states that Directive 95/46/EC and Regulation 45/2001/EC apply to the processing of personal data carried out under the Regulation and that the processing of personal data carried out by law enforcement authorities on EURODAC data once have been extracted is subject to Council Framework Decision 2008/977/JHA.

Therefore, this proposal is fully in line with the Charter of Fundamental Rights of the European Union, in particular as regards the right to asylum (Article 18) and protection of personal data (Article 8) and has to be applied accordingly.

5. CONSULTATION OF INTERESTED PARTIES

The Commission published the Green Paper on the future Common European Asylum System⁶ in June 2007, which proposed options concerning the future features of the Dublin and EURODAC Regulations. In the framework of the wide public consultation on the Green Paper, 89 contributions were received from a wide range of stakeholders.

The Commission services discussed the outcome of the Evaluation Report and the outline of the planned amendments to the Regulation with the Member States in the Committee on Immigration and Asylum (CIA) in March 2008 as well as in two informal expert meetings with Member States' practitioners dedicated to the conclusions of the Evaluation Report in October 2007 and April 2008.

UNHCR, the European Council on Refugees and Exiles (ECRE) as well as the EDPS were also informally consulted in the preparation of the amendment of the Regulation.

During the drafting of the present amended proposal, the Commission consulted the States applying the Dublin *acquis*, i.e. the Member States, Iceland, Norway and Switzerland, as well as to Europol by way of two questionnaires and an expert meeting which took place in Brussels on 25-26 September 2007, during which the experts had the opportunity to clarify the replies to the questionnaire and express further views. Several intergovernmental organisations, non-governmental organisations and other experts working in the area of asylum, fundamental rights were consulted during a meeting in Brussels on 8 October 2007. Representatives of the national data protection authorities of the States that implement the Dublin *acquis*, as well as the Joint Supervisory Body of Europol and the European Data Protection Supervisor were consulted in the framework of a meeting held in Brussels on 11 October 2007.

A detailed list of consulted parties is included in the Impact Assessment attached to this proposal.

⁶ COM(2007) 301.

6. LEGAL BASIS

This proposal amends the 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] - COM(2008) 825.

The present amended proposal uses the same legal base as the original proposal, namely Article 63(1)(a) of the Treaty establishing the European Community.

Title IV of the Treaty is not applicable to the United Kingdom and Ireland, unless those two countries decide otherwise, in accordance with the provisions set out in the Protocol on the position of the United Kingdom and Ireland attached to the Treaties.

The United Kingdom and Ireland are bound by Council Regulation (EC) No 343/2003 following their notice of their wish to take part in the adoption and application of that Regulation based on the above-mentioned Protocol. The position of these Member States with regard to the current Regulation does not affect their possible participation with regard to the amended Regulation.

In accordance with Articles 1 and 2 of the Protocol on the position of Denmark attached to the Treaties, Denmark does not take part in the adoption of this Regulation and is not bound by it nor subject to its application. However, given that Denmark applies the current Dublin Regulation, following an international agreement⁷ that it concluded with the EC in 2006, it shall, in accordance with Article 3 of that agreement, notify the Commission of its decision whether or not to implement the content of the amended Regulation.

7. IMPACT OF THE PROPOSAL ON NON EU MEMBER STATES ASSOCIATED TO THE DUBLIN SYSTEM

In parallel to the association of several non-EU Member States to the Schengen acquis, the Community concluded, or is in the process of doing so, several agreements associating these countries also to the Dublin/EURODAC acquis:

- the agreement associating Iceland and Norway, concluded in 2001⁸;
- the agreement associating Switzerland, concluded on 28 February 2008⁹;
- the protocol associating Liechtenstein, signed on 28 February 2008¹⁰.

⁷ 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 (OJ L 66, 8.3.2006).

⁸ 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 (OJ L 93, 3.4.2001, p. 40).

⁹ 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 (OJ L 53, 27.2.2008, p. 5).

In order to create rights and obligations between Denmark –which as explained above has been associated to the Dublin/EURODAC acquis via an international agreement – and the associated countries mentioned above, two other instruments have been concluded between the Community and the associated countries¹¹.

In accordance with the three above-cited agreements, the associated countries shall accept the Dublin/EURODAC acquis and its development without exception. They do not take part in the adoption of any acts amending or building upon the Dublin acquis (including therefore this proposal) but have to notify to the Commission within a given time-frame of their decision whether or not to accept the content of that act, once approved by the Council and the European Parliament. In case Norway, Iceland, Switzerland or Liechtenstein do not accept an act amending or building upon the Dublin/EURODAC acquis, the "guillotine" clause is applied and the respective agreements will be terminated, unless the Joint/Mixed Committee established by the agreements decides otherwise by unanimity.

Since the amendment of the EURODAC Regulation to include a bridging clause to allow law enforcement access constitutes a development of the Dublin/EURODAC *acquis* within the terms of the abovementioned agreements, the described procedure applies also as concerns this proposal.

8. SUBSIDIARITY PRINCIPLE

Due to the transnational nature of the problems related to asylum and refugee protection, the EU is well placed to propose solutions in the framework of the Common European Asylum System (CEAS) to the issues described above as problems regarding the EURODAC Regulation. Although an important level of harmonization was reached in the Regulation adopted in 2000, there is still room for developing the support that EURODAC provides to the implementation of the Dublin Regulation. The need for EU action regarding the management of an EU database which was created for assisting in the implementation of a Regulation dealing with transnational movements of asylum seekers seems clear.

An amendment of the EURODAC Regulation is also required in order to add a secondary purpose thereto, namely allow access for the purpose to fight against terrorism and crime to data stored in the EURODAC central database. This objective cannot be sufficiently achieved by the Member States, since such amendment can only be proposed by the Commission.

¹⁰ Protocol between the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of Liechtenstein to the Agreement between the European Community and Switzerland concerning the criteria and mechanisms for establishing the State responsible for examining a request for asylum lodged in a the Member State or in Switzerland - COM(2006) 754, conclusion pending.

¹¹ Protocol between the European Community, the Swiss Confederation and 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 (2006/0257 CNS, concluded on 24.10.2008, publication in OJ pending) and Protocol to the Agreement between the Community, 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, Iceland and Norway (OJ L 93, 3.4.2001).

9. PROPORTIONALITY PRINCIPLE

The impact assessment published along with the December 2008 proposal¹² assessed each sub-option regarding the problems identified so as to represent an ideal proportion between practical value and efforts needed. It concluded that opting for EU action does not go beyond what is necessary to achieve the objective of solving those problems.

The relevant Impact Assessment concluded that access of law enforcement authorities to EURODAC is the only timely, accurate, secure and cost-efficient way to identify whether and if so, where data about asylum seekers are available in the Member States. No reasonable efficient alternative to EURODAC exists to establish or verify the exact identity of an asylum seeker that allows law enforcement authorities to obtain the same result.

10. DETAILED EXPLANATION OF THE PROPOSAL

10.1. Modifications introduced following the European Parliament resolution

In its legislative resolution, the European Parliament broadly supported the Commission proposal and proposed mostly editorial amendments along with some substantial ones. The amendments are for the most part acceptable or partly acceptable, with some exceptions. The position of the Commission on each the amendments is detailed hereafter.

10.1.1. Amendments accepted

Amendments 3, 5, 6, 10, 13, 15, 19, 20, 21, 22, 26, 27, 30, 39

These amendments are accepted since they aim to correct inaccuracies and ensure consistency of the proposal.

Amendments 12 and 29

These amendments are inserted in a new Article 8 (information on the status of the data subject) which merges Article 6(2) and 17(6) of the December 2008 proposal.

Amendment 16, 17 and 18

Although with slightly different wording, the substance of these amendments is accepted in article 12.

Amendment 35

This amendment, aiming to ensure that information is provided to the persons concerned 'in a language he or she understands or may reasonably be presumed to understand', is accepted in Article 25(1).

Amendments 37 and 38

These amendments are accepted since they contain clarifications of text concerning rights of the data subject (Article 25 of the present proposal).

¹² SEC(2008) 2981.

10.1.2. Amendments partly accepted

Amendment 1

As it appears from recital 2 of the present proposal, this amendment is accepted as far as a reference to "*international* protection" is concerned, but not as far as the deletion of the expression "forced by circumstances" is concerned, for reasons of consistency with Council Directive 2005/85/EC of 1 December 2005 on minimum standards on procedures in Member States for granting and withdrawing refugee status.¹³

Amendment 11

The first part of the amendment, which splits the deadline for taking and sending fingerprints in two parts, is not acceptable, since such an approach could create practical difficulties for Member States. However, it is accepted to extend the deadline for transmission to 72 hours (in conformity with the EP proposal of 48 hours plus 24 hours) and Article 7 is modified accordingly. The second part of the amendments which proposes exceptions to the general rule is generally acceptable, but a different wording is proposed in order to take into account the results of the discussion in the Council.

Amendment 25

The first part of the amendment adding a new reference to the reference number used when searching a transaction on a third country national or stateless person found illegally present in a Member State is accepted (in Article 18(3) of the present proposal).

Amendment 42

The wording of this amendment is reflected in Article 5(4).

10.1.3. Amendments which cannot be accepted

Amendment 4 and 14

The amendments on Article 9 and the related recital 11 of the December 2008 proposal (recital 17 and Article 11 in the present proposal) suggest that persons who obtained long term residence status in accordance with Council Directive 2003/109/EC of 25 November 2003 concerning the status of third-country nationals who are long-term residents¹⁴ (Long-term Residence Directive) be erased from EURODAC. The Long-term Residence Directive explicitly excludes from its scope of application the applicants and beneficiaries of international protection: for this reason it is not possible to accept those amendments. In addition, these amendments cannot be considered admissible since they are introduced in the text untouched by the recast.

Amendment 8

The amendment is not accepted since the purpose of Article 5 paragraph 7 is not to determine the scope of the IT Agency, but to clarify that the Management Authority referred to in the present Regulation is the same as the one referred to in the SIS II and VIS Regulations.

¹³ OJ L 326, 13.12.2005, p. 13-34.

¹⁴ OJ L 16, 23.1.2004, p. 44-53.

Amendment 9

This amendment (related to Article 5 of the present proposal) is not accepted since its subject is relevant for the proposal on the establishment of the IT Agency and not for this one.

Amendment 23

The amendment, which proposes to add a reference to some additional articles of 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 granted¹⁵ in Article 16 (2) of the present proposal, is not considered necessary, as those situations are already covered in the current drafting.

Amendment 28

The amendment aims at introducing the obligation to inform the EDPS of each 'false hit'. Since it is the task of the national data protection authorities and not of the EDPS to directly monitor the everyday operation of the system, this amendment (not requested by the EDPS in his opinion on the proposal) is not accepted.

Amendment 31

This amendment aims at introducing a provision prohibiting the transfer of data to authorities of third countries. By stipulating that only MSs' designated authorities can have access to EURODAC and by explicitly forbidding, in its Article 22, the transfer of such data to third countries, the Regulation in force is already clear that such data cannot be accessed by third countries. Therefore this amendment is not accepted because it is not needed and actually it might give the impression that previously it was possible to transfer data to third countries.

Amendment 32

This amendment aims at introducing a requirement that the Management Authority lay down "a common set of requirements to be fulfilled by persons in order to be granted authorisation to access EURODAC". The suggested provision is unclear and could create unnecessary administrative burden for the Management Authority, since the screening of personnel accessing EURODAC is more efficiently performed at national level.

Amendment 33

This amendment aims at introducing an obligation for Member States to notify changes in their list of authorities within a maximum of 30 days after the change took effect. This is regarded as an unnecessary burden and the deadline proposed as unrealistic. In addition, it is not in line with similar provision in the Dublin Regulation.

Amendment 40

This amendment aims to ensure the supervision of the Management Authority by the EDPS. This is not the subject matter of the EURODAC Regulation .

¹⁵ OJ L 304, 30.09.2004, p. 12-23.

10.2. Modifications introduced following the outcome of negotiations in the Council

Article 8

This new Article was introduced in order to provide information to Member States on the status of the data subject. First of all, it includes provisions which already figured in the December 2008 proposal, namely Article 6(2) and Article 17(6) thereof, which refer to information on persons transferred following a *take back* procedure and the application of the sovereignty clause of the Dublin Regulation. In addition, the article foresees that Member States are also informed if a given person, whose data is stored in the database, was transferred following a *take charge* procedure, or if he or she left the territory of the Member States, either voluntarily or as the result of a return decision or removal order.

This new Article will therefore facilitate Member States' task to determine the Member State responsible under the Dublin Regulation.

Article 12

The modifications introduced in this article aim to clearly spell out which third country nationals or stateless persons have to be fingerprinted and at what point in time. The introduced change will help harmonising practices between Member States and ensure that as soon as a person is allowed entry on the territory of the Member States, his/her fingerprints need to be taken and sent to the EURODAC database.

Article 30

Until the start of operation of the IT Agency, the Commission will continue to produce the two types of reporting foreseen in the Regulation in force, ie. the annual reports (containing the analysis of annual statistics) and the evaluation reports (along with the respective evaluation of the Dublin Regulation).

Other changes

Modifications were also introduced to recitals 3, 19 and 32 and Articles 5 (1) and (4), and 19 (1) in order to take into account drafting suggestions put forward during the negotiations in Council which the Commission considered could be accepted.

10.3. Modifications to allow access for law enforcement purposes

Article 1

Paragraph 2 is amended in order to reflect the addition of a new purpose of the system.

Article 2

Paragraph 1(c)(iv) is added in order to ensure that the authorities designated for accessing EURODAC for a law enforcement purpose will also comply with the provisions on responsibility for data use and data security. In points (f) and (g), the National Access Point and verifying authority is defined.

Article 3

This new article introduces a bridging clause in order to allow access for law enforcement purposes by providing a link between a third pillar instrument (Council Decision No [.../...]JHA [*EURODAC law enforcement Decision*]) and the present first pillar Regulation.

Article 6

Points (i) and (j), introduce the obligation to collect statistics on the number of law enforcement searches and the number of hits these produced.

In order to better facilitate the purposes of law enforcement access, the present proposal entails a technical amendment to the EURODAC central system, ie. a new functionality to search on the basis of a so-called latent¹⁶.

Article 13

In the second indent of paragraph 1, a reference is made to Article 3 in order to take note of the possibility of access for law enforcement purposes.

Article 19

The scope of paragraph 4 was extended in order to take note of the possibility of access for law enforcement purposes.

Article 22

The new paragraph 2 ensures the new type of search in the system: during access for law enforcement purposes, the data entered is searched against all fingerprints stored in the central database.

¹⁶ A latent print is the chance reproduction of the friction ridges deposited on the surface of an item. Latent prints are often fragmentary and may require chemical methods, powder, or alternative light sources in order to be visualised.

Article 25

The amendment of paragraph 1(b) ensures that upon taking his or her fingerprints, the data subject is also informed about the possibility of his or her data be accessed for law enforcement purposes.

Article 30

Paragraph 5 was amended in order to extend the overall evaluation of the EURODAC Regulation so as to include the mechanism of access for law enforcement purposes. This extended evaluation can examine in particular whether the mechanism introduced in Article 3 has been used in a proportionate manner, whether the rights of individuals have been duly safeguarded, and whether its application has led to stigmatisation of asylum seekers. The evaluation can also take account of the reports prepared by the European Data Protection Supervisor and the national data protection authorities, as well as the Joint Supervisory Body of Europol with regard to their supervisory tasks. In light of this evaluation the Commission may present appropriate proposals.

11. BUDGETARY IMPLICATIONS

The present proposal entails a technical amendment to the EURODAC central system in order to provide for the possibility to carry out comparisons for law enforcement purposes. A new functionality to search on the basis of a latent is also proposed.

The financial statement attached to this proposal is also valid for the proposal concerning the request for comparison with EURODAC data by Member States' law enforcement authorities and by Europol for the purposes of prevention, detection and investigation of terrorist offences and other serious criminal offences [COM (2009) XXX].

The cost estimate of 2,415 million euros includes costs of 3 years of technical maintenance, and consists of IT-related services, software and hardware and would cover the upgrade and customisation to allow searches for law enforcement purposes and also the changes for the original asylum purpose unrelated to law enforcement access. The amounts of the EURODAC recast proposal adopted on 3 December 2008 are kept in the present financial statement for the sake of clarity.

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 the Dublin Convention ☒ **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] ☒

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 63 point (1)(a) thereof,

Having regard to the proposal from the Commission¹⁷,

Acting in accordance with the procedure laid down in Article 251 of the Treaty¹⁸,

Whereas

↓ 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 Convention¹⁹ 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 Convention²⁰. In the interest of clarity, those Regulations should be recast.

¹⁷ COM(2008) XXX.

¹⁸ OJ C [...], [...], p. [...].

¹⁹ OJ L 316, 15.12.2000, p. 1.

²⁰ OJ L 62, 5.3.2002, p. 1.

↓ 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").~~

↓ 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 Community.
- (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.
- (4) The Hague Programme called for the improvement of access to existing data filing systems of the European Union.
- (5) 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 Affairs²¹ of 24 November 2005 the Commission indicated that authorities responsible for internal security could have access to EURODAC in well defined cases, where there is a substantiated suspicion that the perpetrator of a terrorist offence or other serious criminal offence has applied for asylum.
- (6) In order to prevent, detect and investigate terrorist offences and other serious criminal offences, it should be possible to access fingerprint data stored in the EURODAC central database for law enforcement purposes.

²¹ COM(2005) 597 final of 24 November 2005

- (7) Such access should only be granted to law enforcement authorities designated by Member States and to Europol in specific, well-defined cases where no other, less intrusive measures are available and only after the Member States have consulted their national databases and have followed the procedure laid down in Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime²².
- (8) No mass comparison of fingerprints for the purposes of prevention, detection or investigation of terrorist offences and of other serious criminal offences should be conducted in EURODAC.

↓ 2725/2000/EC recital 3
(adapted)
⇒ new

- (9) For the purposes of applying ~~the Dublin Convention~~ ☒ Council 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]²³ ☒, 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 (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] ☒, and in particular points ~~(e) and (c)~~ (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 on its territory has applied for ~~asylum~~ ⇒ international protection ⇐ in another Member State.

↓ 2725/2000/EC recital 4

- (10) 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.

↓ 2725/2000/EC recital 5
⇒ new

- (11) 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

²² OJ L 210, 6.8.2008, p. 1.

²³ COM(2008)XXX.

of the electronic means of transmission between the Member States and the ~~central database~~ ⇒ Central System ⇐.

↓ new

- (12) In view of ensuring equal treatment for all applicants and beneficiaries of international protection, as well as in order to ensure consistency with current EU 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 (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], it is appropriate to extend the scope of this Regulation to order to include applicants for subsidiary protection and persons enjoying subsidiary protection.
-

↓ 2725/2000/EC recital 6
(adapted)
⇒ new

- (13) 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

- (14) 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 national or stateless persons ⊗.
-

↓ new

- (15) Hits obtained from EURODAC should be verified by a fingerprint expert in order to ensure both the accurate determination of responsibility under 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] and the exact identification of the criminal suspect whose data might be stored in EURODAC.

↓ 2725/2000/EC recital 8
(adapted)
⇒ new

- (16) ~~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 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)

- (17) 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

- (18) 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.

- (19) In the long term, and following an impact assessment, containing a substantive analysis of alternatives from financial, operational and organisational perspective, the establishment of a Management Authority responsible for the operational management of EURODAC should be foreseen. Until then, the Commission should remain responsible for the management of the Central System and for the Communication Infrastructure.

↓ 2725/2000/EC recital 10
(adapted)
⇒ new

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

↓ new

- (21) It is necessary to draw up statistics on the number of comparisons requested for law enforcement purposes, as well as the number of hits such requests produced in EURODAC.
- (22) The data subject should be informed of the possibility that his data will be searched by law enforcement authorities for the purposes of prevention, detection and investigation of terrorist offences and other serious criminal offences.

↓ 2725/2000/EC recital 11

- (23) 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

- (24) 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 objective.

↓ 2725/2000/EC recital 15
(adapted)

- (25) 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 data²⁴ 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.~~

↓ 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

(26) 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

(27) 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 data²⁵ should apply to the processing of personal data by the Community institutions and bodies 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.

(28) 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, appointed pursuant to Decision 2004/55/EC of the European Parliament and of the Council of 22 December 2003 appointing the independent supervisory body provided for in Article 286 of the EC Treaty²⁶, should monitor the activities of the Community institutions and bodies in relation to the processing of personal data in view of the limited tasks of the Community institutions and bodies with regard to the data themselves.

²⁴ OJ L 281, 23.11.1995, p. 31.

²⁵ OJ L 8, 12.1.2001, p. 1.

²⁶ OJ L 12, 17.1.2004, p. 47.

↓ 2725/2000/EC recital 18
⇒ new

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

↓ 2725/2000/EC recital 19
(adapted)
⇒ new

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

↓ new

- (31) 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 (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].

- (32) 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 protection of personal data and the right to asylum.
-

↓ 2725/2000/EC recital 22
(adapted)

- (33) 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 (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] .

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 (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] 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

~~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.~~
3.2. Without prejudice to the 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 Article ~~15(1)~~32(1) of the Dublin ~~Convention~~ Regulation and for the purpose of the prevention, detection and investigation of terrorist offences and other serious criminal offences, under the conditions set out in Article 3 of this Regulation and in Council Decision No [...]JHA [*EURODAC law enforcement Decision*] .

Article 2

Definitions

1. For the purposes of this Regulation:

- (a) "the Dublin ~~Convention~~ Regulation 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 (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] asylum international protection alien third-country national or a stateless person 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
 - (i) in relation to an ~~applicant for asylum~~ person covered by Article 7

new

(iv) in relation to the tasks covered by Article 17 and Article 21

- the Member State which transmits the personal data to the Central System and receives the results of the comparison,
- the Member States' and Europol's authorities designated in accordance with Article 4(1) and (4) of Council Decision No [.../...]JHA [EURODAC law enforcement Decision];

↓ 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 Article 2(a) of Council Directive 2004/83/EC ⇐;
- (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 ~~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)~~ 19(4).

↓ new

- (f) 'National Access Point' means the designated national system which communicates with the Central System.
- (g) 'Verifying authority' means the single national body designated by a Member State or by Europol in accordance with Article 4 of Decision No [.../...]JHA [EURODAC law enforcement Decision].

↓ 2725/2000/EC (adapted)

2. The terms defined in Article 2 of Directive 95/46/EC shall have the same meaning in this Regulation.
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

Article 3

Availability of data for the prevention, detection and investigation of terrorist offences and other serious criminal offences

1. Where comparison with data stored in its national fingerprint database and access to 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 crime²⁷ (Prüm Decision) return negative results, Member States' and Europol authorities designated in accordance with Article 3(1) and 5(2) of Decision No [.../...]JHA [*EURODAC law enforcement Decision*], may within the scope of their powers in case it is necessary in a specific case and following a reasoned written or a reasoned logged electronic request, ask for comparison of fingerprint data with data stored in the EURODAC central database referred to in Articles 9 and 12(2) if there are reasonable grounds to consider that consultation of data stored in the EURODAC central database will substantially contribute to the prevention, detection or investigation of terrorist offences and of other serious criminal offences.

2. The comparison referred to in paragraph 1 shall be carried out through the verifying authority referred to in Article 4 of Decision No [.../...]JHA [*EURODAC law enforcement Decision*], which screens and forwards requests by the designated authorities to the National Access Point. The verifying authority shall be responsible for ensuring that the conditions for requesting comparisons of fingerprints with EURODAC data established in Decision No [.../...]JHA [*EURODAC law enforcement Decision*] are fulfilled. In an exceptional case of urgency, the verifying authority may receive reasoned written or reasoned logged electronic requests and only verify *ex-post* whether all the conditions for access are fulfilled, including whether an exceptional case of urgency existed. The *ex-post* verification shall take place without undue delay after the processing of the request.
3. Neither the hit, nor data obtained from EURODAC pursuant to Decision No [.../...]JHA [*EURODAC law enforcement Decision*] shall be transferred or made available to a third country, international organisation or a private entity established in or outside the European Union.
4. Without prejudice to Article 23(2), the Central System shall not store the fingerprint data which is transmitted to it under this Article, and shall delete the data immediately upon completion of the transmission of the results of the comparison.

↓ 2725/2000/EC (adapted)

Article 4

~~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.~~

²⁷ OJ L 210, 6.8.2008, p. 1.

↓ 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~~ 7, 12 and 15 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.

Article 5

Operational management by the Management Authority

1. A Management Authority, funded from the general budget of the European Union, shall be responsible for the operational management of EURODAC. The Management Authority 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 Management Authority 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 Management Authority takes up its responsibilities, the Commission shall be responsible for all tasks attributed to the Management Authority 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 the Staff Regulations of Officials of the European Communities, the Management Authority 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.
7. The Management Authority referred to in this Regulation shall be the Management Authority competent for SIS II under 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) and for VIS under Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas.

↓ 2725/2000/EC (adapted)
⇒ new

Article 6~~3~~

⊗ Statistics ⊗

3. The ~~Central Unit~~ ⊗ Management Authority ⊗ 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 7(1), ~~8(1)~~ and ~~11(1)~~ 12(1) and 15(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)~~ 10(1) who have subsequently lodged an application for ~~asylum~~ ⇒ international protection ⇐;
- (d) the number of hits for persons referred to in Article ~~11(1)~~ 13(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;3

↓ new

- (f) the number of data sets marked in accordance with Article 16(1);
- (g) the number of hits for persons referred to in Article 16(1);
- (h) for whom hits have been recorded under (b),(c),(d) and (g);
- (i) the number of comparisons requested in accordance with Article 3;
- (j) the number of hits obtained in application of Article 3.

↓ 2725/2000/EC
⇒ new

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 (b), (c), ~~and~~ (d) ⇒ (g) and (i) ⇐ .

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.~~

↓ 2725/2000/EC (adapted)
⇒ new

CHAPTER II

APPLICANTS FOR ~~ASYLUM~~ INTERNATIONAL PROTECTION

Article ~~7~~ 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 ~~(g)~~ (g) of Article ~~5(1)~~ 9 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 19 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

3. Fingerprint data within the meaning of point ~~(b)~~ (a) of Article ~~5(1) 9~~, transmitted by any Member State, ~~☒~~ with exception to those transmitted in accordance with Article 8 point (b) ~~☒~~ shall be compared ⇒ 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 Article ~~5(1) 9(a) 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 16(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

Article 8

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 10 for the purpose of transmission under Article 7(5):

- (a) When an applicant for international protection or another person as referred to in Article 18(1)(d) 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 9 relating to the person concerned by adding his/her 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 9 relating to the person concerned and include his/her 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 9 has left the territory of the Member States, it shall update its dataset recorded in conformity with Article 9 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 9 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 9 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 9 relating to that applicant by adding the date when the decision to examine the application was taken.

↓ 2725/2000/EC
⇒ new

Article 95

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 Article 8 point (b), 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 8 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 8 point (c), the date when the person
concerned left the territory of the Member States;

(j) where applicable in accordance with Article 8 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 8 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 ~~10~~ 6

Data storage

Each set of data, as referred to in Article ~~5(1)~~ 9, shall be stored in the ~~Central~~ ~~Unit~~ ~~⇒ 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 ~~11~~ 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~~ 10 shall be erased from the ~~Central~~ ~~Unit~~ ~~⇒ System~~ ~~⇐~~, in accordance with Article ~~15(3)~~ 22(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 7(1) or Article 12(1).

CHAPTER III

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

Article 12 §

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 ⇒ 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 ⇐;

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 19 of this Regulation, 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

Article 13 ~~9~~

Recording of data

1. The data referred to ~~in Article 5(1)(g) and in Article 8(2) 12(2)~~ shall be recorded in the ~~central database~~ ⇒ Central System ⇐.

Without prejudice to Article ~~3(3)6~~ ⇒ and Article 3 ⇐, data transmitted to the Central ~~Unit~~ ⇒ System ⇐ pursuant to Article ~~8(2) 12(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) 12(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) 12(2)~~.
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) 7(3) and (5) and in Article 19(4)~~ shall apply.

Article ~~14~~ 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)~~ 12(1) shall be stored in the ~~central database~~ Central System for one year ~~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)~~ 12(1) shall be erased from the ~~central database~~ Central System in accordance with Article ~~15(3)~~ 22(3) as soon as the Member State of origin becomes aware of one of the following circumstances before the ~~two~~ one -year period mentioned in paragraph 1 has expired:
 - (a) the ~~alien~~ third country national or stateless person has been issued with a residence permit;
 - (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 paragraph 2(a) or (b) by another Member State of origin having produced a hit with data which they transmitted relating to persons referred to in Article 12(1).
4. The Central System shall inform all Member States of origin about the erasure of data for the reason specified in paragraph 2(c) by another Member State of origin having produced a hit with data which they transmitted relating to persons referred to in Article 7(1) or Article 12(1).

CHAPTER IV

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

Article 15 ~~H~~

Comparison of fingerprint data

1. With a view to checking whether an ~~alien~~ ☒ third country national or a stateless person ☒ found illegally present 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)~~ 12(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)~~ 7(3) and (5) 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.~~

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).~~

↓ new

Article 16

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 9 in the Central System shall mark the relevant data in conformity with the requirements for electronic communication with the Central System established by the Management Authority. This mark shall be stored in the Central System in accordance with Article 10 for the purpose of transmission under Article 7(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.

CHAPTER VI

DATA USE, DATA PROTECTION AND LIABILITY

Article 17 ~~13~~

Responsibility for data use

1. The Member State of origin shall be responsible for ensuring that:
 - (a) fingerprints are taken lawfully;
 - (b) fingerprint data and the other data referred to in Article ~~5(1)~~ 9, Article ~~8(2)~~ 12(2) and Article ~~11(2)~~ 15(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~~ ⇒ Management Authority ⇐, 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 used.
2. In accordance with Article ~~14~~12, 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)~~ 19(4).
4. The ~~Commission~~ ⇒ Management Authority ⇐ 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~~ ⇒ Management Authority ⇐ shall:
 - (a) adopt measures ensuring that persons working ⇒ with ⇐ in the Central ~~Unit~~ ⇒ System ⇐ use the data recorded ⊗ therein ⊗ ~~in the central database~~ only in accordance with the purpose of ~~Eurodac~~ EURODAC as laid down in Article 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~~ 12;

(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~~ ⇒ Management Authority ⇐ shall inform the European Parliament and the Council of the measures it takes pursuant to the first subparagraph.

↓ 407/2002/EC Article 2
(adapted)
⇒ new

Article ~~182~~

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~~ ☒ Management Authority ☒ 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~~ ☒ Management Authority ☒ 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)~~ 9(1), ~~Article 12(2) and Article 15(2) of the Eurodac Regulation~~ electronically. ⇒ The data referred to in Article 9(1) and Article 12(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~~ ☒ Management Authority ☒ 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. The reference number referred to in Article ~~5(1)(d)~~ 9(d) and ~~Article 12(2)(d) and 15(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~~⁷, Article 12 or Article 15.

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 7(1) , "2" to persons referred to in Article ~~8~~ ^{12(1) of the Eurodac Regulation} and "3" to persons referred to in Article ~~11~~ ^{15 of the Eurodac Regulation}.
5. The ~~Central Unit~~ Management Authority shall establish the technical procedures necessary for Member States to ensure receipt of unambiguous data by the Central ~~Unit~~ System .
- ~~64~~ The Central ~~Unit~~ System shall confirm receipt of the transmitted data as soon as possible. To this end the ~~Central Unit~~ Management Authority shall establish the necessary technical requirements to ensure that Member States receive the confirmation receipt if requested.

Article ~~19~~³

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~~ Management Authority 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~~ Management Authority'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~~ Management Authority 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~~ Management Authority 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. Final identification shall be made by the Member State of origin in cooperation with the Member States concerned, pursuant to Article ~~1532~~ of the Dublin ~~Convention~~ Regulation and Decision No [.../...]JHA [EURODAC law enforcement Decision] .

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 Management Authority.

↓ 407/2002/EC (adapted)
⇒ new

Article ~~204~~

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~~ Management Authority shall establish the technical procedures necessary for the use of ~~IDA generic services~~ the Communication Infrastructure .

~~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.~~

Article 21

Data security

1. The Member State of origin shall ensure the security of the data before and during transmission to the Central System. Each Member State shall ensure the security of the data which it receives from the Central System.

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;
 - (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 deletion of stored personal data (storage control);
 - (e) prevent the unauthorised processing of data in EURODAC and any unauthorised modification or deletion 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, delete and search the data and make these profiles available to the National Supervisory Authorities referred to in Article 26 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 deletion 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 appropriate 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 Management Authority 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.

↓ 2725/2000/EC
⇒ new

Article 22 ~~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)~~ 7(5).

↓ new

- 2 By way of derogation from paragraph 1, Member States' designated authorities and Europol's specialised unit designated in accordance with Article 4(1) and (4) of Decision No [.../...]JHA [*EURODAC law enforcement Decision*] may conduct searches in all data stored in the central database regardless of their Member State of origin and may receive such data in accordance with Article 3 of this Regulation and Decision No [.../...]JHA [*EURODAC law enforcement Decision*].

↓ 2725/2000/EC (adapted)
⇒ new

3. 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 Management Authority ⇐ a list of those authorities ⇒ and any amendments thereto. The Management Authority shall publish the consolidated list in the Official Journal of the European Union. Where there are amendments thereto, the Management Authority shall publish once a year an updated consolidated list. ⇐
4. 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)~~ 10 or Article 14(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.~~

5. If a Member State or the ~~Central Unit~~ ⇒ Management Authority ⇐ 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 Management Authority, 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.

6. The ~~Central Unit~~ ⇒ Management Authority ⇐ 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 ⇐.

Article 21

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).~~

Article 23 ~~16~~

Keeping of records by the ~~Central Unit~~

1. The ~~Central Unit~~ ⇒ Management Authority ⇐ 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~~ 12. The records must be protected by appropriate measures against unauthorised access and erased after a period of one year \Rightarrow after the retention period referred to in Article 10 and in Article 14(1) has expired \Leftarrow , if they are not required for monitoring procedures which have already begun.
-

\Downarrow 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.
-

\Downarrow 2725/2000/EC (adapted)
 \Rightarrow new

Article 22

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 24 ~~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~~ \Rightarrow Central System \Leftarrow , that Member State shall be held liable for such damage, unless and insofar as the ~~Commission~~

⇒ Management Authority 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.

Article ~~25~~ 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) ⊗ regarding ⊗ the purpose for which ~~the~~ ⊗ his or her ⊗ 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 and of the aims of Article 3 of this Regulation and of Decision No [.../...]JHA [EURODAC law enforcement Decision] ⇐.

(c) the recipients of the data;

(d) in relation to a person covered by Article ~~4~~ 7 or Article ~~8~~ 12, 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 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 26(1) ⇐.

In relation to a person covered by Article ~~4~~ 7 or Article ~~8~~ 12, 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~~ 15, 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

Where a person covered by this Regulation is a minor, Member States shall provide the information in an age-appropriate manner.

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.

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)~~ 22(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 referred to in Article 26(1) without delay, upon their request.

↓ 2725/2000/EC (adapted)
⇒ new

~~9.~~ 10. In each Member State, the national supervisory authority shall ~~assist the data subject~~ ⇒ 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 ~~26~~ 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 27

Supervision by the European Data Protection Supervisor

1. The European Data Protection Supervisor shall check that the personal data processing activities of the Management Authority are carried out in accordance with this Regulation. The duties and powers referred to in Articles 46 and 47 of Regulation (EC) No 45/2001 shall apply accordingly.
2. The European Data Protection Supervisor shall ensure that an audit of the Management Authority'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 Management Authority, the Commission and the National Supervisory Authorities. The Management Authority shall be given an opportunity to make comments before the report is adopted.

Article 28

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 Management Authority every two years.

CHAPTER VII

FINAL PROVISIONS

Article ~~29~~ 24

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 ⇒ verifying authorities and ⇐ national ⇒ access points ⇐ units and the costs for connection to the ~~central database~~ ⇒ Central System ⇐ shall be borne by each Member State.
- ~~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 ~~30~~ 24

Annual report: ~~m~~ Monitoring and evaluation

1. The ~~Commission~~ ⇒ Management Authority ⇐ 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~~ ⇒ Management Authority ⇐ 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 Management Authority shall have access to the necessary information relating to the processing operations performed in the Central System.
 4. Every two years, the Management Authority shall submit to the European Parliament, the Council and the Commission 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 35(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, ⇒ including in respect of the mechanism introduced by Article 3, the application of this Regulation in respect of the Central System, the security of the Central System, ⇐ 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 Management Authority and the Commission with the information necessary to draft the reports referred to in paragraph 4 and 5.
7. The Management Authority shall provide the Commission with the information necessary to produce the overall evaluations referred to in paragraph 5.
8. Until the Management Authority provided for in Article 5 is established, the Commission will only produce reports in accordance with paragraph 1 and 5.

↓ 2725/2000/EC (adapted)
⇒ new

Article 31 ~~25~~

Penalties

Member States shall ☒ take the necessary measures to ☒ ensure that ☒ any ☒ 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) ~~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 32 ~~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 33

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 14(1) of this Regulation on the date provided for in Article 35(2).

↓

Article 34

Repeal

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 are repealed with effect from the date provided for in Article 35(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 ~~35~~ 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, ~~and Eurodac shall start operations,~~ from the date which the Commission shall publish in the Official Journal of the European ~~Communities~~ Union, when the following conditions are met:
 - (a) each Member State has notified the Commission that it has made the necessary technical arrangements to transmit data to the Central ~~Unit~~ System in accordance with this Regulation ~~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~~ System to begin operations in accordance with this Regulation ~~the implementing rules adopted under Article 4(7) and Article 12(5).~~

↓ new

3. Member States shall notify the Commission as soon as the arrangements referred to in paragraph 2(a) have been made, and in any event no later than 12 months from the date of the entry into force of this Regulation.

↓ 2725/2000/EC

4. This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaty establishing the European Community.

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-ITL 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 alien was apprehended	
3.	Date of the application for asylum or date on which the alien was apprehended	
4.	Sex	
5.	Date on which the fingerprints were taken	
6.	Date on which the data were transmitted to the Central Unit	

105 mm from top of form
155 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
50 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	55 mm		



ANNEX II
Repealed Regulations
(referred to in Article 32)

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 4(1)
Article 1(2), second subparagraph	Article 4(4)
Article 1(3)	Article 1(2)
Article 3(1)	deleted
Article 2	Article 2
Article 3(2)	Article 4(3)
Article 3(3)	Article 6
Article 3(4)	deleted
Article 4(1)	Article 7(1)
Article 4(2)	Deleted
Article 4(3)	Article 7(3)
Article 4(4)	Article 7(4)
Article 4(5)	Article 7(5)
Article 4(6)	Article 19(4)
Article 5	Article 9
Article 6	Article 10
Article 7	Article 11
Article 8	Article 12
Article 9	Article 13
Article 10	Article 14
Article 11(1)-(4)	Article 15(1)-(4)

Article 11(5)	deleted
Article 12	- Article 16
Article 13	Article 17
Article 14	- Article 21
Article 15	Article 22
Article 16	Article 23
Article 17	Article 24
Article 18	Article 25
Article 19	Article 26
Article 20	Article 27
Article 21	Article 29
Article 22	deleted
Article 23	deleted
Article 24	Article 30
Article 25	Article 31
Article 26	Article 32
Article 27	Article 35
-	Annex II

Regulation 407/2002/EC	This Regulation
Article 2	Article 16
Article 3	Article 17
Article 4	Article 18
Article 5(1)	Article 3(2)
Annex I	Annex I
Annex II	-

ANNEX IV
LEGISLATIVE FINANCIAL STATEMENT

1. NAME OF THE PROPOSAL:

Proposal for a Regulation of the European Parliament and the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No [.../...] ²⁸

2. ABM / ABB FRAMEWORK

Policy Area: Area of Freedom, Security and Justice (title 18)

Activities:

Migration flows — Common immigration and asylum policies (chapter 18.03)

3. BUDGET LINES

3.1. Budget lines (operational lines and related technical and administrative assistance lines (ex- B.A lines)) including headings:

Financial framework 2007-2013: Heading 3A

Budget line: 18.03.11 - Eurodac

3.2. Duration of the action and of the financial impact:

The entry into force of the EURODAC Regulation is linked to the entry into force of the Dublin Regulation. This can also be foreseen in 2011 the earliest.

3.3. Budgetary characteristics:

Budget line	Type of expenditure		New	EFTA contribution	Contributions from applicant countries	Heading in financial perspective
18.03.11.	Non-comp	Diff ²⁹	NO	NO	NO	3A

²⁸ The present legislative financial statement only deals with the costs foreseen to occur with respect to the changes introduced by the present amendment, hence it does not deal with the costs of regular management of EURODAC.

²⁹ Differentiated appropriations

4. SUMMARY OF RESOURCES

4.1. Financial Resources

4.1.1. Summary of commitment appropriations (CA) and payment appropriations (PA)

EUR million (to 3 decimal places)

Expenditure type	Section no.		Year 2010	2011	2012	2013	n+4	n + 5 and later	Total
------------------	-------------	--	-----------	------	------	------	-----	-----------------	-------

Operational expenditure³⁰

Commitment Appropriations (CA)	8.1.	a	0.000	2.415	0.000	0.000			2.415
Payment Appropriations (PA)		b	0.000	2.415	0.000	0.000			2.415

Administrative expenditure within reference amount³¹

Technical & administrative assistance (NDA)	8.2.4.	c	0.000	0.000	0.000	0.000			0.000
---	--------	---	-------	-------	-------	-------	--	--	-------

TOTAL REFERENCE AMOUNT

Commitment Appropriations		a+c	0.000	2.415	0.000	0.000			2.415
Payment Appropriations		b+c	0.000	2.415	0.000	0.000			2.415

Administrative expenditure not included in reference amount³²

Human resources and associated expenditure (NDA)	8.2.5.	d	0.000	0.244	0.122	0.122			0.488
Administrative costs, other than human resources and associated costs, not included in reference amount (NDA)	8.2.6.	e	0.000	0.084	0.020	0.000			0.104

Total indicative financial cost of intervention

TOTAL CA including cost of Human Resources		a+c +d+ e	0.000	2.743	0.142	0.122			3.007
TOTAL PA including cost of Human Resources		b+c +d+ e	0.000	2.743	0.142	0.122			3.007

³⁰ Expenditure that does not fall under Chapter xx 01 of the Title xx concerned.

³¹ Expenditure within article xx 01 04 of Title xx.

³² Expenditure within chapter xx 01 other than articles xx 01 04 or xx 01 05.

Co-financing details

No co-financing is anticipated.

EUR million (to 3 decimal places)

Co-financing body		Year n	n + 1	n + 2	n + 3	n + 4	n + 5 and later	Total
.....	f							
TOTAL CA including co-financing	a+c +d+ e+f							

4.1.2. Compatibility with Financial Programming

- Proposal is compatible with existing financial programming.
- Proposal will entail reprogramming of the relevant heading in the financial perspective.
- Proposal may require application of the provisions of the Interinstitutional Agreement³³ (i.e. flexibility instrument or revision of the financial perspective).

4.1.3. Financial impact on Revenue

- Proposal has no financial implications on revenue
- Proposal has financial impact – the effect on revenue is as follows:

EUR million (to one decimal place)

Budget line		Revenue	Prior to action [Year n-1]	Situation following action						
				[Year n]	[n+1]	[n+2]	[n+3]	[n+4]	[n+5] 34	
		a) Revenue in absolute terms								
		b) Change in revenue	Δ							

³³

See points 19 and 24 of the Interinstitutional agreement.

³⁴

Additional columns should be added if necessary i.e. if the duration of the action exceeds 6 years

4.2. Human Resources FTE (including officials, temporary and external staff) – see detail under point 8.2.1.

Annual requirements	Year 2010	2011	2012	2013	n + 5
Total number of human resources	0	2.0	1.0	1.0	

5. CHARACTERISTICS AND OBJECTIVES

5.1. Need to be met in the short or long term

In order to facilitate prevention, detection and investigation of terrorist offences and other serious criminal offences, access for consultation for law enforcement purposes to EURODAC will be allowed.

5.2. Value-added of Community involvement and coherence of the proposal with other financial instruments and possible synergy

This proposal will provide a solution to the concerns of the Council and the law enforcement community about the absence of access by internal security authorities to EURODAC data, seen as a shortcoming, which results in a serious gap in the identification of suspected perpetrators of terrorist or serious crimes.

Introducing the possibility of running law enforcement searches with latents in EURODAC depends on the migration of EURODAC to a new IT system, the Biometric Matching System. BMS will serve as a common platform providing biometric matching services to the Schengen Information System II (SIS II), Visa Information System (VIS) and EURODAC. The integration of EURODAC in BMS is expected to start in 2011.

5.3. Objectives, expected results and related indicators of the proposal in the context of the ABM framework

The main objectives of the proposal is to to facilitate prevention, detection and investigation of terrorist offences and other serious criminal offences, access for consultation for law enforcement purposes.

The indicators would be the statistics on the operation of EURODAC, eg. those on comparisons of fingerprints requested for law enforcement purposes.

5.4. Method of Implementation (indicative)

Centralised Management

directly by the Commission

indirectly by delegation to:

- executive Agencies
- bodies set up by the Communities as referred to in art. 185 of the Financial Regulation
- national public-sector bodies/bodies with public-service mission
- Shared or decentralised management***
 - with Member states
 - with Third countries
- Joint management with international organisations (please specify)***

In the future, the operational management of EURODAC could be transferred to a Agency responsible for SIS II, VIS and other IT systems in the area of Freedom, Security and Justice. Regarding the setting up of this Agency, a separate proposal will be presented by the Commission, assessing the relevant costs.

6. MONITORING AND EVALUATION

6.1. Monitoring system

Monitoring of the efficiency of the changes introduced by the present proposal is to be performed in the framework of the annual reports on the activities of the EURODAC Central Unit, as well as the evaluation of the practices of access for law enforcement purposes.

Monitoring of data protection issues will be performed by the European Data Protection Supervisor.

6.2. Evaluation

6.2.1. Ex-ante evaluation

The ex-ante evaluation has been included in the impact assessment.

6.2.2. Measures taken following an intermediate/ex-post evaluation (lessons learned from similar experiences in the past)

The Commission published its report on the evaluation of the Dublin system in June 2007, covering the first 3 years of the operation of EURODAC (2003-2005). Whilst acknowledging that the Regulation is applied in a generally satisfactory way, it identified certain issues related to the efficiency of the current legislative provisions and announced the issues which have to be tackled in order to improve EURODAC's support to facilitate the application of the Dublin Regulation.

6.2.3. Terms and frequency of future evaluation

Regular evaluation is proposed to be ensured by the Commission and, after its set-up, also the Management Authority.

7. ANTI-FRAUD MEASURES

In order to combat fraud, corruption and other unlawful activities, the provisions of Regulation (EC) No 1037/1999 shall apply without restriction.

8. DETAILS OF RESOURCES

8.1. Objectives of the proposal in terms of their financial cost

Commitment appropriations in EUR million (to 3 decimal places)

(Headings of Objectives, actions and outputs should be provided)	Type of output	Av. cost	Year 2010		Year 2011		Year 2012		Year 2013		Year n+4		Year n+5 and later		TOTAL		
			No. outputs	Total cost	No. outputs	Total cost	No. outputs	Total cost	No. outputs	Total cost	No. outputs	Total cost	No. outputs	Total cost	No. outputs	Total cost	
OPERATIONAL OBJECTIVE No.1 ³⁵																	
Requirements deriving from the EURODAC Regulation																	
Action 1 Implementing new functionalities in the EURODAC central system																	
New functionalities Output 1 – changes other than for Law Enforcement			0.000		0.100			0.000		0.000							0.100

³⁵

As described under Section 5.3.

Access																	
New functionalities Output 2 – changes for Law Enforcement Access						2.000		0.000		0.000							2.000
Overheads and miscellaneous (15%)				0.000		0.315		0.000		0.000							0.315
TOTAL COST				0.000		2.415		0.000		0.000							2.415

Costs are calculated on the basis of the assumption that the EURODAC system is served by the BMS and hosted together with the BMS/VIS system. Due to the above, only costs for 2011 are shown in the tables. The estimate of 2,415 million includes 3-year-long (2011-2012-2013) maintenance/support services for the new setup of EURODAC to be delivered in 2011, so no further costs have to be foreseen for the coming two years covered by this quasi-warranty. Further costs for the maintenance of the added functionalities will therefore only arise after 2013.

Costs above include costs of 3 years of maintenance, and would consist of IT-related services, software and hardware and would cover the upgrade and customisation to the BMS/EURODAC system to allow searches for law enforcement purposes and also the changes for the original asylum purpose unrelated to law enforcement access. The amounts in the original financial fiche attached to proposal COM(2009) 825 of 3 December 2008 are kept in the current one for the sake of clarity. They figure as "output 1" alongside with the costs of the changes required for this specific proposal, marked as "output 2".

8.2. Administrative Expenditure

8.2.1. Number and type of human resources

Types of post		Staff to be assigned to management of the action using existing and/or additional resources (number of posts/FTEs)					
		Year 2010	Year 2011	Year 2012	Year 2013	Year n+4	Year n+5
Officials or temporary staff ³⁶ (XX 01 01)	A*/AD	0	0	0.0	0.0		
	B*, C*/AST	0	2.0	1.0	1.0		
Staff financed ³⁷ by art. XX 01 02							
Other staff ³⁸ financed by art. XX 01 04/05							
TOTAL		0	2.0	1.0	1.0		

8.2.2. Description of tasks deriving from the action

Deal with administrative and financial issues related to the contract with the system provider.

Follow-up the implementation of the changes on the EURODAC IT system.

Follow-up the tests by the Member States.

Helpdesk towards Member States for new users.

8.2.3. Sources of human resources (statutory)

- Posts currently allocated to the management of the programme to be replaced or extended
- Posts pre-allocated within the APS/PDB exercise for year n
- Posts to be requested in the next APS/PDB procedure
- Posts to be redeployed using existing resources within the managing service (internal redeployment)
- Posts required for year n although not foreseen in the APS/PDB exercise of the year in question

³⁶ Cost of which is NOT covered by the reference amount.

³⁷ Cost of which is NOT covered by the reference amount.

³⁸ Cost of which is included within the reference amount.

8.2.4. *Other Administrative expenditure included in reference amount (XX 01 04/05 – Expenditure on administrative management)*

EUR million (to 3 decimal places)

Budget line (number and heading)	Year n	Year n+1	Year n+2	Year n+3	Year n+4	Year n+5 and later	TOTAL
1 Technical and administrative assistance (including related staff costs)							
Executive agencies ³⁹							
Other technical and administrative assistance							
- <i>intra muros</i>							
- <i>extra muros</i>							
Total Technical and administrative assistance							

8.2.5. *Financial cost of human resources and associated costs not included in the reference amount*

EUR million (to 3 decimal places)

Type of human resources	Year 2010	Year 2011	Year 2012	Year 2013	Year n+4	Year n+5 and later
Officials and temporary staff (18 01 01)	0.000	0.244	0.122	0.122		
Staff financed by Art XX 01 02 (auxiliary, END, contract staff, etc.) (specify budget line)						
Total cost of Human Resources and associated costs (NOT in reference amount)	0.000	0.244	0.122	0.122		

Calculation– *Officials and Temporary agents financed under art. 18 01 01 01*

³⁹ Reference should be made to the specific legislative financial statement for the Executive Agency(ies) concerned.

AD/AST – 122.000 EUR per year x 2.0 persons = 244.000 EUR (2011)

AD/AST – 122.000 EUR per year x 1.0 persons =122.000 EUR (2012-2013)

8.2.6. Other administrative expenditure not included in reference amount

EUR million (to 3 decimal places)

	Year 2010	Year 2011	Year 2012	Year 2013	Year n+5	Year n+5 and later	TOTAL
18 01 02 11 01 – Missions	0.000	0.004	0.000	0.000			0.004
XX 01 02 11 02 – Meetings & Conferences	0.000	0.080	0.020	0.000			0.100
XX 01 02 11 03 – Committees ⁴⁰							
XX 01 02 11 04 – Studies & consultations							
XX 01 02 11 05 - Information systems							
2 Total Other Management Expenditure (XX 01 02 11)							
3 Other expenditure of an administrative nature (specify including reference to budget line)							
Total Administrative expenditure, other than human resources and associated costs (NOT included in reference amount)	0.000	0.084	0.020	0.000			0.104

⁴⁰ Specify the type of committee and the group to which it belongs.