



Analysis

11 Years of Eurodac

Chris Jones

On 15 January 2003 Eurodac, the EU-wide database of asylum-seekers' and irregular migrants' fingerprints, came into use. Eleven years on, it holds the personal data of nearly 2.3 million individuals and has been transformed into a policing as well as migration database.

The Eurodac system

Proposals for Eurodac (an abbreviation of European Dactyloscopy or fingerprint identification) were the subject of discussions in secretive Council working parties since at least 1994. [1] A Council Regulation was passed in 2000 following "consultation" of the European Parliament. [2] Three years later, a Commission press release announced that:

"EURODAC, a system for the comparison of fingerprints of asylum applicants and certain groups of illegal immigrants, will become operational on 15 January in the Member States of the European Union (with the exception of Denmark, for the time being) and in the third countries bound by the EURODAC Regulation (Norway and Iceland).

"The aim of this database is to assist in determining which state is responsible for considering an application for asylum according to the mechanism and criteria set up by the "Dublin Convention"... It is therefore an important tool in the development of the Common European Asylum System called for by the European Council at its meeting in Tampere (Finland), in October 1999." [3]

The system is also used to determine whether individuals have been apprehended by a Member State's authorities "in connection with the irregular crossing of an

external border”, and to see whether “aliens found illegally present in a Member State” have previously applied for asylum within the EU, Norway or Iceland.

The Eurodac system comprises the Central Unit, initially operated by the Commission but now managed by the EU Agency for Large-Scale IT Systems, a national unit in each Member State, and the infrastructure for transmitting data between national units and the Central Unit.

All participating states are obliged to “promptly take the fingerprints of all fingers of every applicant for asylum of at least 14 years of age”. This is subsequently transmitted to the Central Unit database and stored for ten years, along the following information:

- Member State of origin, place and date of the application for asylum;
- Sex;
- Reference number used by the Member State of origin;
- Date on which the fingerprints were taken;
- Date on which the data were transmitted to the Central Unit;
- Date on which the data were entered in the central database;
- Details in respect of the recipient(s) of the data transmitted and the date(s) of transmission(s).

Under amended legislation coming into force in July 2015, this data will be supplemented by further information:

- Operator user ID;
- The date of the arrival of the person concerned after a successful transfer under the Dublin Regulation;
- The date when the person concerned left the territory of the Member States, if it is established that they have done so;
- The date when the person concerned left or was removed from the territory of the Member States, if that person was subjected to a return or removal order;
- The date when the decision to examine the asylum application was taken, when a Member State decides to examine an individual's application.

Similar provisions apply to “aliens apprehended in connection with the irregular crossing of an external border”. This covers “every alien of at least 14 years of age who is apprehended by the competent control authorities in connection with the irregular crossing by land, sea or air of the border of that Member State having come from a third country and who is not turned back”. The authorities are obliged to collect and transmit the following data to the Central Unit, which is stored for two years:

- Fingerprint data;
- Member State of origin, place and date of the apprehension;
- Sex;
- Reference number used by the Member State of origin;
- Date on which the fingerprints were taken;
- Date on which the data were transmitted to the Central System.

This will be supplemented in July 2015 by the inclusion of data on the “operator user ID”.

As of 2012 the Central Unit database held 2,296,670 entries, more than double the number held in 2007 (1,086,246) when the Commission’s annual reports on Eurodac first published the statistics. 2013 should be the first year in which information taken from asylum-seekers in 2003 begins to be deleted, due to the 10 year retention limit, although the figures for 2013 are yet to be published and it remains to be seen whether the report will remark upon the issue. Charts and tables documenting the growth of Eurodac over the last decade are available below.

A number of changes to the system will come into force on 20 July 2015, based on legislation agreed last year by the Council and the Parliament. [4] For example, the length of time information on people apprehended in connection with the irregular crossing of an external border can be held has been decreased from two years to 18 months (Article 16), and the European Data Protection Supervisor, rather than a joint supervisory body, will have responsibility for auditing and monitoring the processing of personal data in cooperation with national authorities. Other changes include:

“[A] new 72-hour deadline to send the fingerprints to the Eurodac system; a new provision (Article 10) on additional information concerning asylum-seekers, to make sure that the correct person is sent to another Member State following a fingerprint match... a ban on transmitting Eurodac data to third states in most cases (Article 35); consequential amendments to the EU legislation establishing an agency for managing JHA IT systems (Article 38); publication of information on authorities using Eurodac (Article 43); transitional rules (Article 44); and repeal of the prior legislation (Article 45).”

Law enforcement access

The most notable – and controversial – change introduced is the provision of access to the system for Europol and national law enforcement agencies, for example for comparing fingerprints found at a crime scene (known as ‘latent fingerprints’). This change came after several years of lobbying by national government and law enforcement representatives. A previous attempt to amend the legislation in such a manner in 2009 lapsed after the Lisbon Treaty entered into force. [5]

Under the new legislation, each Member State is to draw up a list of “competent authorities” who may have access to the system. Europol must do likewise, and under Article 43 of the new Regulation both lists should be published by the Commission annually in the Official Journal of the European Union. Under Article 5(1), “agencies or units exclusively responsible for intelligence relating to national security” are excluded from being granted access, although given the inability of the EU to legislate on issues of national security [6] it is unclear how this provision can be enforced.

Access will be given to the designated law enforcement authorities if two conditions are fulfilled. First, access must be for “the prevention, detection or investigation of terrorist offences or other serious criminal offences” as outlined in the European

Framework Decision on combating terrorism and the European Arrest Warrant. It must also be “necessary in a specific case”, and there must be reasonable grounds to consider the comparison “will substantially contribute to the prevention, detection or investigation of any of the criminal offences in question”.

The second condition relates to other possible sources of the same information and the reasoning behind the access. Access is only permitted if:

- No match was found in national databases;
- No match was found in other Member States’ databases, accessible through the network of national DNA databases established by the Prüm Decision;
- No match was found in the Visa Information System database.

These conditions relate to what the European Parliament’s Civil Liberties Committee said were “stricter data protection provisions and new safeguards” which mean there has to be “an overriding public security concern which makes the searching of the database proportionate”. [7]

Information on recognised refugees as well as applicants for international protection will also be available under the new rules (Article 18). The Parliament, which originally wanted to prevent access to recognised refugees’ data, “caved in” to pressure from the Commission and the Council. Law enforcement access will now be possible for three years after an individual has been granted refugee or subsidiary protection status. As noted in a previous *Statewatch* analysis, this assumes that “persons whose refugee or subsidiary protection status has been recognised are more likely to be potential criminals.” [8]

There was significant opposition to permitting any access at all for law enforcement authorities. The European Data Protection Supervisor [EDPS] condemned the proposal for going against the basic data protection principle of purpose limitation and for singling out a particular social group for treatment not applied to others:

“Just because the data has already been collected, it should not be used for another purpose which may have a far-reaching negative impact on the lives of individuals. To intrude upon the privacy of individuals and risk stigmatising them requires strong justification and the Commission has simply not provided sufficient reason why asylum seekers should be singled out for such treatment.” [9]

The proposal was also “strongly” opposed by the Meijers Committee, made up of experts on international immigration, refugee and criminal law, Europol’s Joint Supervisory Body for data protection, which said they had “seen no evidence from the Commission to prove such access is necessary,” [10] and the UN High Commissioner for Refugees. [11] Nevertheless, the legislation passed through the Parliament with nearly three-quarters (502 or 73%) of MEPs voting in favour. [12]

A 2010 study on law enforcement information exchange in the EU noted that “according to [Member States], access to “non police data” such as EURODAC, EU-PNR [Passenger Name Record] should be accessible to the police authorities in the future.” Member States have got their wish with access to the data held in Eurodac,

although discussions on an EU PNR system have stalled after the Parliament's civil liberties committee voted against legislation in April 2012. [13] Nevertheless, giving law enforcement authorities access to data originally collected with the aim of establishing responsibility for asylum claims and controlling migration sets a dangerous precedent with regard to other databases.

The backbone of an unjust asylum system?

While law enforcement agencies across Europe will now in certain cases be able to access information contained in Eurodac, its primary purpose remains the same: "to assist in determining which Member State is to be responsible pursuant to Regulation (EU) No 604/2013 [the 'Dublin III' Regulation] for examining an application for international protection lodged in a Member State by a third-country national or a stateless person".

Under the Dublin system, those seeking asylum or other forms of international protection within the EU are obliged to make an application in the first Member State that they reach. 'Welcome to Europe', an independent website that attempts to provide information on EU and national migration regimes, puts it bluntly: "You cannot choose the country in which you wish to apply for asylum." [14] Hence an EU-wide fingerprint database: if someone applying for asylum in the UK is found to have been fingerprinted whilst making an application in Germany, they can be removed to Germany, although a hierarchy of different criteria apply when determining the state responsible for examining an application. [15]

According to the European Commission:

"The objective [of Eurodac] is to avoid asylum seekers from being sent from one country to another, and also to prevent abuse of the system by the submission of several applications for asylum by one person." [16]

It is unclear whether this aim has been achieved. As the statistics in the charts below demonstrate, the number of multiple asylum applications recorded in the Central Unit has increased from 17,287 in 2003 to 78,591. While this is probably indicative of an increased number of asylum applications and more systematic use of Eurodac by national authorities, it also suggests that many asylum-seekers are not satisfied with their initial asylum applications.

The vast divergence of standards across Member States has also led in some cases to asylum-seekers mutilating themselves in order to try and circumvent identification in Eurodac and transfer to other states. There have been numerous documented instances of individuals mutilating their fingerprints with methods such as placing their fingers on burning hobs or using knives, razors, glue or acid. [17]

Numerous EU Member States have halted Dublin transfers to Greece in recent years due to its appalling reception conditions and failing asylum system. This followed repeated calls from the UN High Commissioner for Refugees (UNHCR), amongst others, [18] to suspend the transfers until the Greek system was improved. [19] The UNHCR has made similar statements in relation to transfers to Hungary [20] and, most recently, Bulgaria. [21] States with responsibility for borders at the edge of the

EU have seen a disproportionate burden fall upon them under the Dublin system, as they are the first point of entry and contact with the authorities for a vast number of asylum-seekers. [22] Furthermore, as research by the Jesuit Refugee Service (JRS) and the European Council on Refugees and Exiles (ECRE) have argued:

“The consequences of these divergent practices [amongst states] have been enormously detrimental to asylum seekers. Many people seeking asylum are transferred from one country to the next without ever have the chance to have their asylum application fully examined. Families are torn apart by the Dublin transfer process because governments are too focused on removing asylum seekers to the EU country that they first entered, rather than working to keep families together. Asylum seekers spend months in detention centres, and even when they are not detained there is no guarantee that they can have access to decent housing and welfare support.” [23]

Similar arguments have been made over the years by numerous other organisations. [24]

Last year the Dublin legislation was updated (the ‘Dublin III’ Regulation was agreed by the Council and Parliament in June and came into force in December), [25] but it remains to be seen whether it will lead to improvements in the functioning of the system. The JRS and ECRE have noted that it “has the potential to remedy some of the serious gaps in protection” under Dublin II, but this “depends on how the Dublin III Regulation is applied at a national level... Improvements on paper will not lead to improvements in practice as long as there is not a level playing field.” A previous *Statewatch* analysis examining the legislation underpinning the Common European Asylum System noted that:

“In order to reduce divergences in application of the EU rules and ensure their correct implementation it will probably be necessary to take further steps, not only to adopt further legislation harmonising standards but to think of new methods of ensuring its implementation, for example a vigorous enforcement policy by the Commission, the creation of a common asylum court or joint processing of applications.” [26]

Taking data protection seriously?

In the past, a need to enforce the existing rules governing Eurodac more vigorously has also been highlighted. The Eurodac Supervision Coordination Group, made up of the European Data Protection Supervisor and national data protection authorities, remarked in 2009 that in many Member States the information on data protection and individuals’ rights provided to data subjects:

“[S]eems to be incomplete, in particular on the consequences of being fingerprinted, the transmission of personal data to other countries, and the right of access, rectification and deletion; the information is not intelligible... The lack of knowledge of the rights afforded by law to the data subjects may explain the very few requests presented for the access to personal data. Notably, in general the countries where such requests are being presented are the same ones in which the information which is being provided to data

subjects is deemed to be complete, adequate and in compliance with Eurodac Regulation.” [27]

In 2007, in the first inspection report, the Group highlighted issues regarding the national authorities responsible for Eurodac:

“[I]n several Member States, the DPAs [data protection authorities] have had a very difficult job in identifying all authorities with Eurodac-related responsibilities, let alone to identify which one was the actual data controller... this led in some Member States to a situation where none of the authorities wanted to acknowledge its responsibilities for any problem that might arise in the operation of Eurodac. It even seems that, in two Member States, the Eurodac users were not even known to one another, nor was their exact role in the processing.” [28]

National DPAs subsequently took “action to request that the identity of the data controller is communicated to them.” A September 2013 list shows a number of Member States with numerous authorities afforded access to Eurodac, [29] but a lack of follow-up reports by the Supervision Coordination Group means it is unclear whether the situation identified in 2007 has been remedied.

The new provisions permitting law enforcement access may raise a whole range of new issues. The minutes of the Supervision Coordination Group’s meeting from October 2013 note that a possible future action could be:

“[T]he close monitoring of the new rules that allow also law enforcement authorities to have access to Eurodac data. This could take the form of a future visit to the Eurodac Central System, and the national systems of some Member States, to check the embedment of the privacy by design principle and data protection requirements foreseen by the Eurodac Recast.” [30]

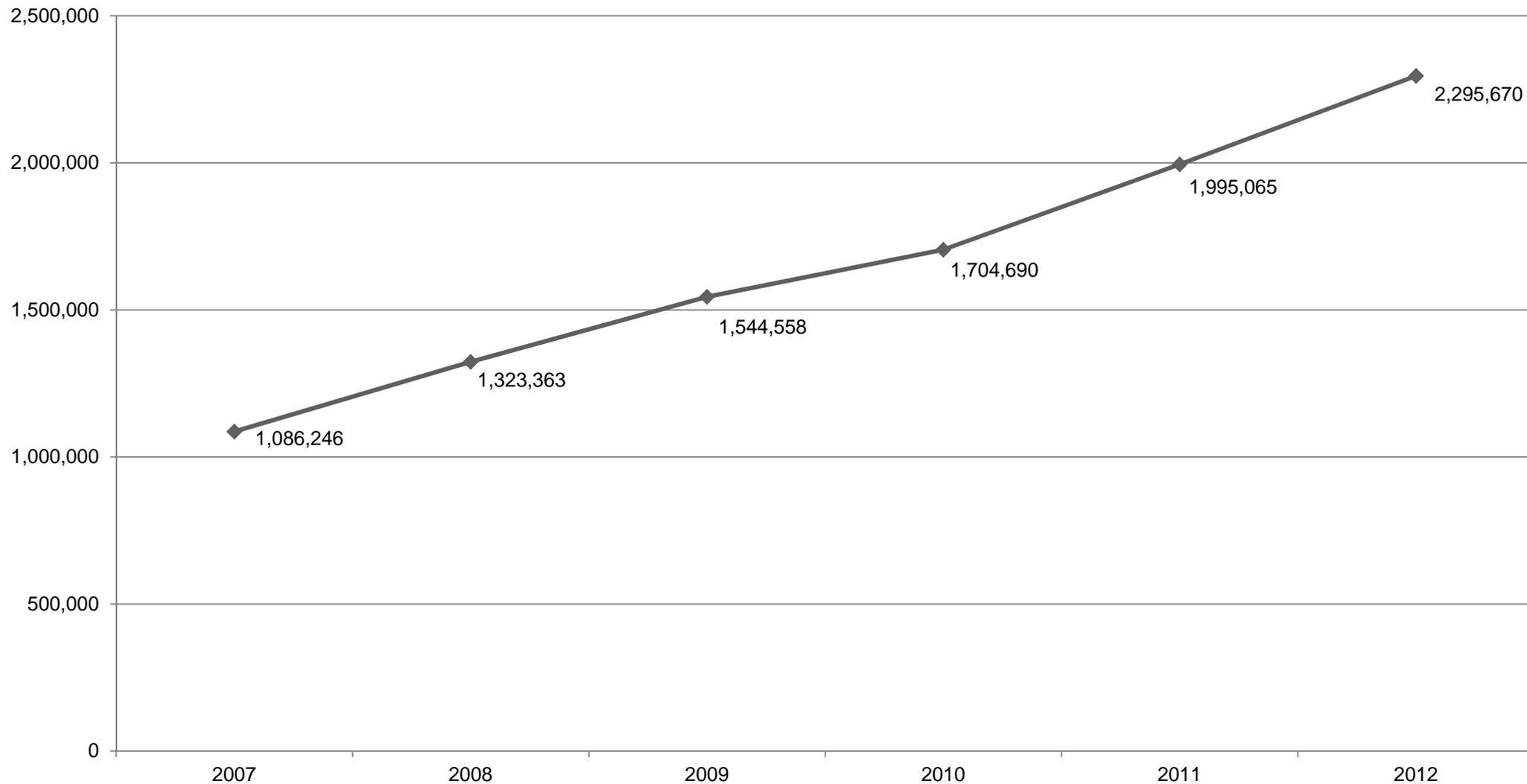
2.3 million and counting

While the number of entries made in Eurodac’s central database has varied from year to year, it seems almost certain it will continue to grow whilst wars, civil unrest and poverty in the Middle East, Africa and elsewhere lead people towards a European Union determined to construct a ‘Common European Asylum System’. [31] At the last count (see the charts below), the Central Unit contained the fingerprints and other personal data of nearly 2.3 million people. This vast amount of data will likely present an increasingly tempting repository for law enforcement authorities who, having already obtained some limited access, may be inclined to seek less stringent rules for access. This is particularly so given the growing trend for the police to seek to gain access to data collected for purposes other than policing. [32]

Aside from the concerns raised by the database itself, Eurodac will also continue to be used to enforce Europe’s asylum system. As noted above, the new Dublin III Regulation “has the potential to remedy some of the serious gaps in protection” under Dublin II. However, it remains to be seen whether Member States will be willing or able to take their new obligations seriously.

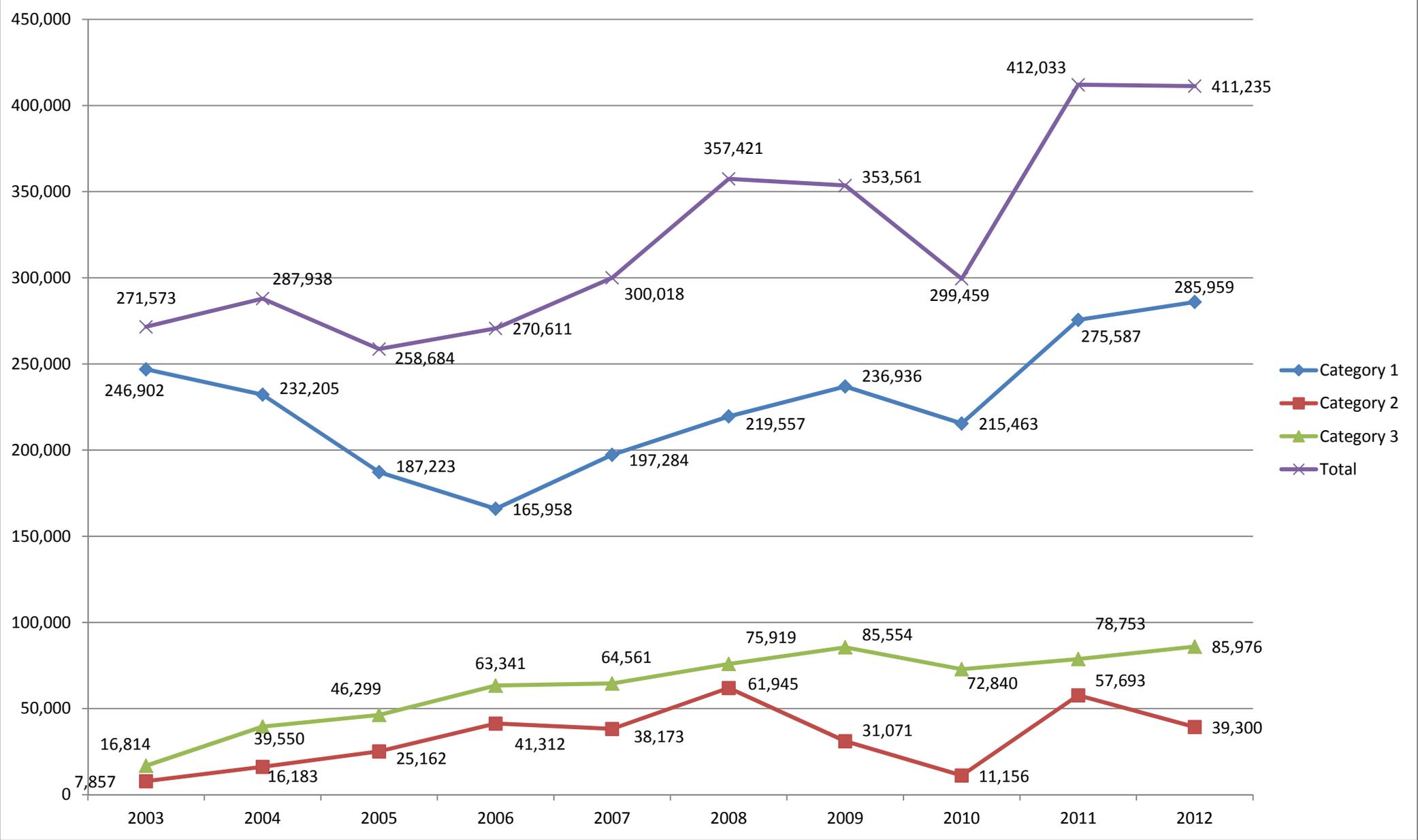
The charts and tables that follow are based on the Commission's annual reports on the activities of the Eurodac Central Unit, and give some indication of the development of the central database and its functions.

Total entries in the Eurodac Central Unit database



	2007	2008	2009	2010	2011	2012
Total entries in Eurodac database	1,086,246	1,323,363	1,544,558	1,704,690	1,995,065	2,295,670
Number of new entries		237,117	221,195	160,132	290,375	300,605

Successful transactions



	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012
Category 1	246,902	232,205	187,223	165,958	197,284	219,557	236,936	215,463	275,587	285,959
Category 2	7,857	16,183	25,162	41,312	38,173	61,945	31,071	11,156	57,693	39,300
Category 3	16,814	39,550	46,299	63,341	64,561	75,919	85,554	72,840	78,753	85,976
Total	271,573	287,938	258,684	270,611	300,018	357,421	353,561	299,459	412,033	411,235

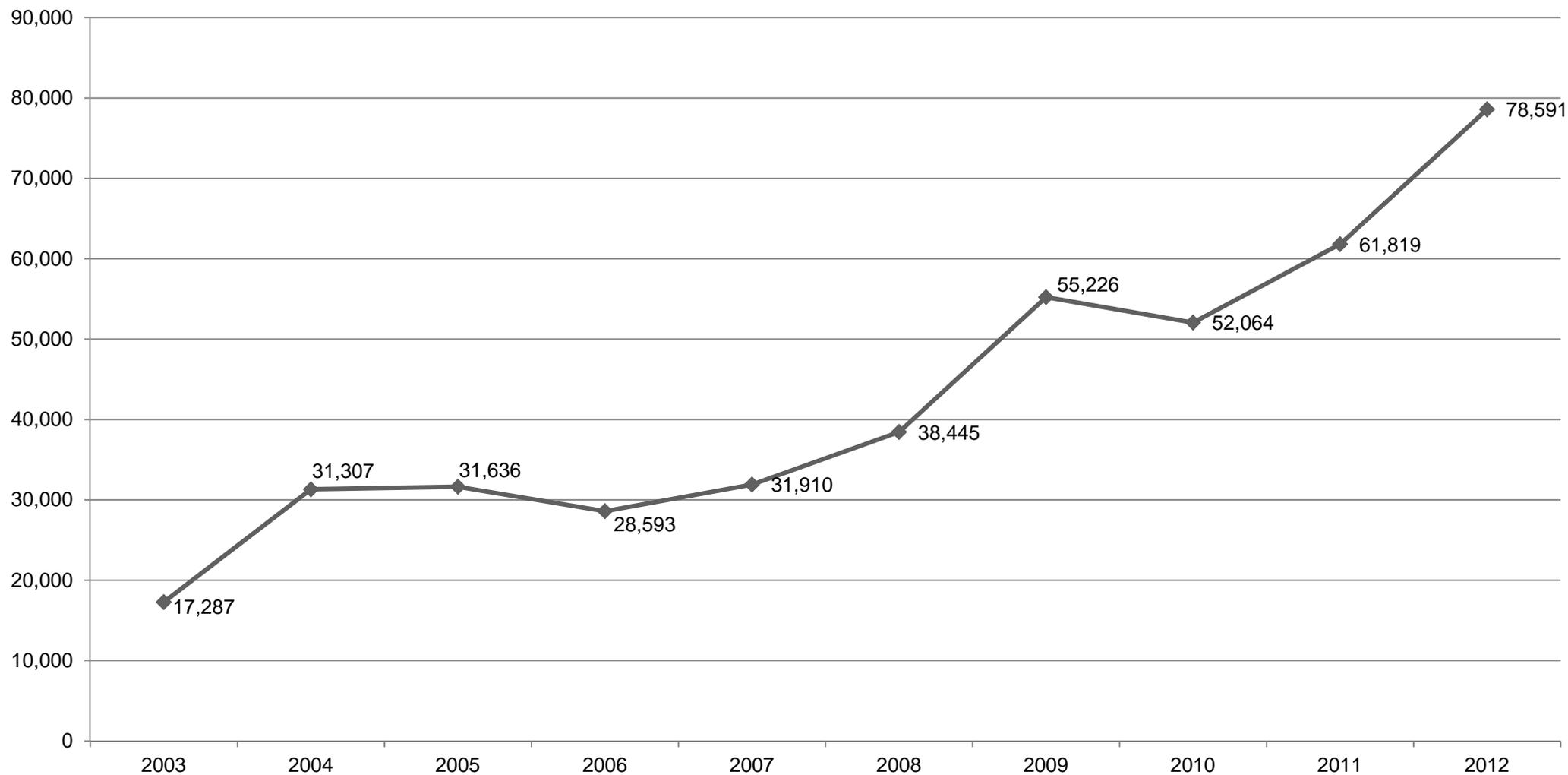
Successful transaction: A “successful transaction” is a transaction which has been correctly processed by the Central Unit, without rejection due to a data validation issue, fingerprint errors or insufficient quality.

Category 1: data of asylum applications. Fingerprints (full 10 print images) of asylum applicants sent for comparison against fingerprints of other asylum applicants who have previously lodged their application in another Member State. The same data will also be compared against the “category 2” data (see below). This data will be kept for 10 years with the exception of some specific cases foreseen in the Regulation (for instance an individual who obtains the nationality of one of the Member States) in which cases the data of the person concerned will be erased;

Category 2: data of aliens apprehended in connection with the irregular crossing of an external border and who were not turned back. This data (full 10 print images) are sent for storage only, in order to be compared against data of asylum applicants submitted subsequently to the Central Unit. This data will be kept for two years with the exception that cases are deleted promptly when the individual receives a residence permit, leaves the territory of the Member State or obtains the nationality of one of them;

Category 3: data relating to aliens found illegally present in a Member State. These data, which are not stored, are searched against the data of asylum applicants stored in the central database. The transmission of this category of data is optional for the Member States.

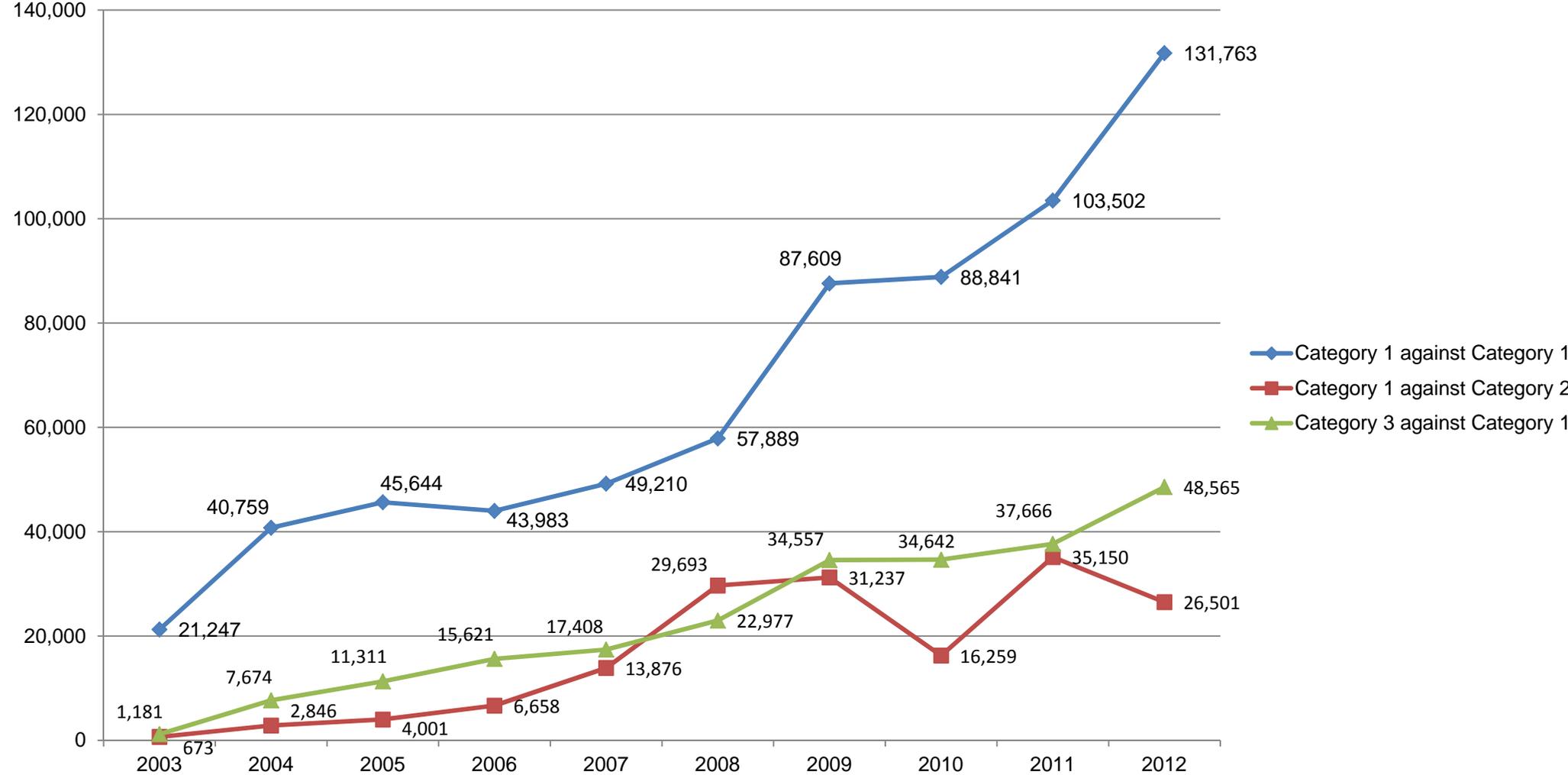
Multiple asylum applications



	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012
Multiple asylum applications	17,287	31,307	31,636	28,593	31,910	38,445	55,226	52,064	61,819	78,591

Multiple asylum applications: figures which indicate that asylum applicants have already lodged at least one asylum application before (in the same or in another Member State).

Comparative transactions



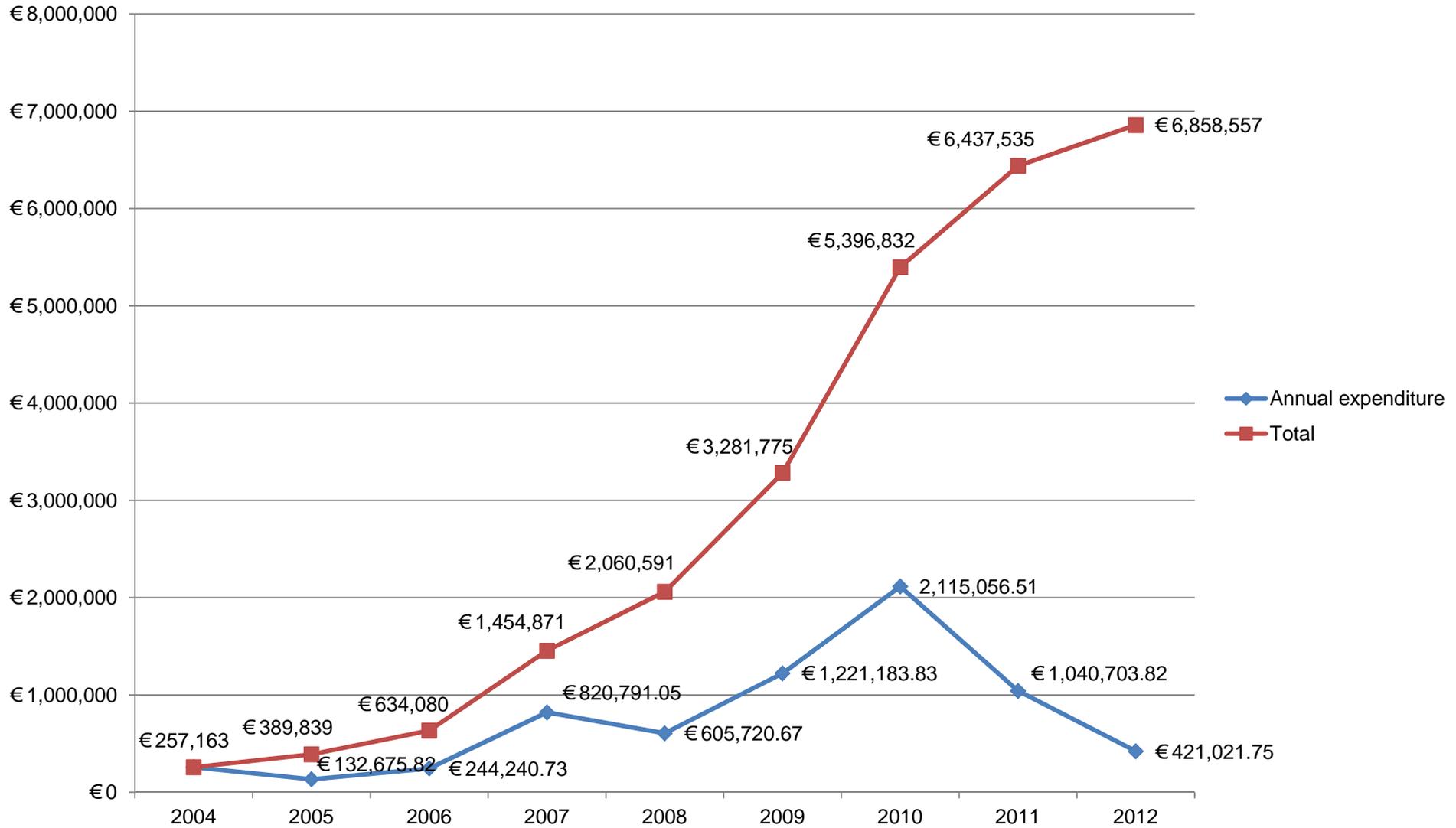
	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012
Category 1 against Category 1	21,247	40,759	45,644	43,983	49,210	57,889	87,609	88,841	103,502	131,763
Category 1 against Category 2	673	2,846	4,001	6,658	13,876	29,693	31,237	16,259	35,150	26,501
Category 3 against Category 1	1,181	7,674	11,311	15,621	17,408	22,977	34,557	34,642	37,666	48,565

Category 1 against Category 1: a “category 1 against category 1” hit means that the fingerprints of an asylum seeker have been recognised by the Central Unit as a match against the stored fingerprints of an existing asylum applicant. This hit is ‘local’ when the asylum seeker has already applied for asylum in the same Member State and ‘foreign’ when he/she has already applied for asylum in another Member State.

Category 1 against Category 2: these hits give an indication of routes taken by persons who irregularly entered the territory of the European Union, before applying for asylum.

Category 3 against Category 1: these hits give indications as to where irregular migrants first applied for asylum before travelling to another Member State. It has to be borne in mind, however, that submitting "category 3" transactions is not mandatory and that not all Member States use the possibility for this check systematically.

Costs



	2004	2005	2006	2007	2008	2009	2010	2011	2012
Annual expenditure (€)	257,163	132,675.82	244,240.73	820,791.05	605,720.67	1,221,183.83	2,115,056.51	1,040,703.82	421,021.75
Total (€)	257,163	389,839	634,080	1,454,871	2,060,591	3,281,775	5,396,832	6,437,535	6,858,557

Notes

- [1] [‘EU: New Council Directorate’](#), *Statewatch*, vol. 4 no. 2, March-April 1994
- [2] [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; ‘Asylum: Eurodac system for the comparison of the fingerprints of applicants and foreigners, Dublin Convention’](#), *European Parliament Legislative Observatory*, 1999/0116(CNS)
- [3] European Commission, [‘Identification of asylum seekers – EURODAC operational tomorrow’](#), 14 January 2003
- [4] [Regulation \(EU\) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of ‘Eurodac’ for the comparison of fingerprints for the effective application of Regulation \(EU\) No 604/2013 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 requests for the comparison with Eurodac data by Member States’ law enforcement authorities and Europol for law enforcement purposes, and amending Regulation \(EU\) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice \(recast\)](#)
- [5] [‘Asylum: requests for comparisons with EURODAC data by Member States’ law enforcement authorities and Europol for law enforcement purposes’](#), *European Parliament Legislative Observatory*, 2009/0130(CNS),
- [6] Article 4(2) of the Lisbon Treaty states that “national security remains the sole responsibility of each Member State.”
- [7] Council of the European Union, [‘Common European Asylum System: Council adopts the Eurodac regulation’](#), 20 June 2013, 11160/13
- [8] Steve Peers, [‘The second phase of the Common European Asylum System: A brave new world – or lipstick on a pig?’](#), *Statewatch Analysis*, 8 April 2013
- [9] European Data Protection Supervisor, [‘EURODAC: erosion of fundamental rights creeps along’](#), 5 September 2012; European Data Protection Supervisor, [‘Opinion of the European Data Protection Supervisor on the amended proposal for a Regulation of the European Parliament and of the Council on the establishment of ‘EURODAC’ for the comparison of fingerprints for the effective application of Regulation \(EU\) No \[.../...\] \[.....\] \(Recast version\)’](#), September 2012
- [10] Meijers Committee, [‘Note Meijers Committee on the EURODAC proposal \(COM\(2012\) 254\)’](#), 10 October 2012; Joint Supervisory Body of Europol, [‘Opinion of the Joint Supervisory Body of Europol \(Opinion 12/52\) with respect to the amended proposal for a Regulation of the European Parliament and of the Council on the establishment of EURODAC’](#), 10 October 2012
- [11] UNHCR, [‘An efficient and protective Eurodac’](#), November 2012
- [12] [‘Establishment of ‘Eurodac’ for the comparison of fingerprints’](#), *VoteWatch Europe*
- [13] [‘Civil Liberties Committee rejects EU Passenger Name Record proposal’](#), *European Parliament*, 24 April 2013
- [14] [‘Dublin II’](#), *Welcome to Europe*
- [15] See Chapter III, [Regulation \(EU\) No 604/2013 of the European Parliament and of the Council of 26 June 2013 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 \(recast\)](#)
- [16] European Commission, [‘Dublin II Regulation’](#), 18 November 2011
- [17] Harriet Grant and John Domokos, [‘Dublin regulation leaves asylum seekers with their fingers burnt’](#), *The Guardian*, 7 October 2011
- [18] Pro Asyl, [“‘The situation in Greece is out of control’ – Research into the situation of asylum seekers in Greece’](#), October 2008
- [19] UNHCR, [‘Observations on Greece as a country of asylum’](#), December 2009
- [20] [‘EU: Hungary still not safe for Dublin II migrants’](#), *Statewatch News Online*, October 2012
- [21] [‘UNHCR: All transfers to Bulgaria should be halted due to a real risk of inhuman or degrading treatment’](#), *Asylum Information Database*, 3 January 2014
- [22] Vitoria Smythies and Lara Ramazzotti, [‘The Dublin Regulation: A Critical Examination of a Troubled System’](#), *internationalrefugeelaw*, 26 August 2013
- [23] [‘Dublin III Regulation enters into force today’](#), *Electronic Immigration Network*, 19 July 2013

- [24] AWO et al., [‘Allocation of refugees in the European Union: for an equitable, solidarity-based system of sharing responsibility’](#), March 2013; Migreurop, [‘European borders – Controls, detention and deportation’](#), 2010
- [25] [Regulation \(EU\) No 604/2013 of the European Parliament and of the Council of 26 June 2013 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 \(recast\)](#)
- [26] Steve Peers, [‘The second phase of the Common European Asylum System: A brave new world – or lipstick on a pig?’](#), *Statewatch Analysis*, 8 April 2013
- [27] Eurodac Supervision Coordination Group, [‘Second Inspection Report’](#), 24 June 2009
- [28] Eurodac Supervision Coordination Group, [‘Report of the first coordinated inspection’](#), 17 July 2007
- [29] [‘Eurodac Responsible Authorities under article 15 of Regulation 2725/2000’](#), September 2013
- [30] Eurodac Supervision Coordination Group, [‘Summary report’](#), October 2013,
- [31] Steve Peers, [‘The revised ‘Dublin’ rules on responsibility for asylum-seekers: The Council’s failure to fix a broken system’](#), *Statewatch Analysis*, April 2012
- [32] 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 sent by Member States’ law enforcement authorities and Europol for law enforcement purposes’](#), 7 October 2009

© Statewatch ISSN 1756-851X. Personal usage as private individuals/"fair dealing" is allowed. We also welcome links to material on our site. Usage by those working for organisations is allowed only if the organisation holds an appropriate licence from the relevant reprographic rights organisation (eg: Copyright Licensing Agency in the UK) with such usage being subject to the terms and conditions of that licence and to local copyright law.