GOVERNMENT DATA
COLLECTION

Are people at risk?

European Monograph

SIS II - VIS - EURODAC - ECRIS

Ligue des droits de l'Homme
FONDÉE EN 1898

aedh

Humanistische Union

HUNGARIAN CIVIL LIBERTIES UNION
HCLU

Ligue des Droits de l'Homme
Action Luxembourg Ouvert et Solidaire

MEDEL
Magistrats Européens pour la Démocratie et les Libertés

Avril 2014

TABLE OF CONTENTS

The information contained in this document is up to date at the end of January 2014.

1. INTRODUCTION

Institutional filing is also practiced on the European Union (EU) level. This document presents four European systems that collect data on individuals: the Schengen Information System II (SIS II) on persons wanted or refused entry to the EU, the Visa Information System (VIS) on visa applicants, the EURODAC system on asylum seekers and the ECRIS system on criminal records. These systems contain information on many of the people present in the EU, whether they are EU nationals or not.

These systems were all created by common policies, but ECRIS differs in terms of operations (it is based on a decentralised structure in each Member State), management (which is mainly national) and data protection regime (which is covered in the Council Framework Decision 2008/977/JHA of 27 November 2008).

Presentation of the European data protection frameworks[1]

1.1. Directive 95/46/CE

Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, commonly called Directive 95, sets out the rules and principles governing personal data processing by private or public sector organisations, with the exception of processing that takes place in the course of an activity that falls outside the scope of Community law (police, criminal justice, etc.). It also establishes the rights of individuals and the obligations of data processors.

The Directive establishes general principles applicable to lawful data processing: the consent principle, the legality principle, the purpose principle, the proportionality principle, the accuracy principle, the data minimization principle and the data processing time limit principle. It also sets out the rights of the data subjects, in particular:

• the right to obtain information on the conditions under which personal data is collected and processed, the right to access personal data collected about him/her, and the right to correct inaccurate data;

• the right to object to the processing of his/her data on compelling grounds;

• the right not to be subject to a decision which significantly affects him/her and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him/her.

The Directive also sets out the obligations of data controllers, in particular:

• the obligation to process data in line with general processing principles and the obligation to inform the data subject;

• the obligation to respect data confidentiality and security;

• the obligation to notify data protection authorities of any personal data processing in line with relevant national legislation.

The Directive establishes rules for the international transfer of personal data, which involves assessing whether the third country ensures an adequate level of data protection.

The Directive includes rules giving data subjects the right to lay complaints concerning breaches of their rights. It also includes rules on the possibility to file administrative or legal appeals. It describes the sanctions applicable to breaches of the Directive's rules and principles. In addition, it creates rules for the independent supervision of personal data processing on the national level, and for the cooperation of data protection authorities on the European level.

1. This document is based on the texts available at the time of writing (November 2013), Directive 95/46/EC and the European Commission's initial proposals for reform dated 25 January 2012. These initial texts were amended and voted on by the European Parliament's LIBE Committee on 21 October 2013. The newly adopted version of these texts was not yet available.

Personal data that is processed by companies or administrations based in the EU can only be processed under the conditions set out in the Directive. These conditions make it possible for data to move freely within the EU.

The Directive is currently being reviewed. The European Commission considered this revision was necessary for several reasons. Firstly, technological evolutions have led to major changes in the ways in which personal data is collected, processed and shared in the new digital environment. Secondly, personal data has become an asset for companies carrying out economic activities. The revision aims to strengthen individuals' rights within a secure legal environment while ensuring the free flow of personal data for companies.

The revision has also put forward new concepts such as the right to be forgotten, the right to data portability, the obligation for data controllers to incorporate privacy by design and privacy by default mechanism, the banning of profiling, the obligation to carry out data protection impact assesssments, the obligation for large companies and public sector organisations to appoint privacy officers, the obligation for data controllers to keep a record of data processing operations and the obligation to report security breaches to the data subject and the data protection authority.

In addition to the regulation, a new directive will be drafted on data protection in the police and judicial cooperation fields. These fields are currently governed by Council Framework Decision 2008/977/JHA of 27 November 2008.

The Directive's revision has led to considerable debate. At the time of writing[2], the revision project is still underway. As the mandates of European members of parliament will soon expire, it is impossible to predict the document's final form. The European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee) has sent proposed texts to the Council, which are currently under discussion.

1.2. European Data Protection Authorities

An important part of the data protection regime is the creation of an independent monitoring system. This system incorporates the European Data Protection Supervisor, the Article 29 Working Party and national data protection authorities.

The **European Data Protection Supervisor** (EDPS) monitors the processing of personal data by EU institutions and bodies, advises on policies and legislation that affect privacy and cooperates with data protection authorities to ensure consistent data protection[3].

When monitoring EU institutions and bodies, the EDPS has considerable influence and coercive power. However, when advising on policies and legislation, it only acts in a consultative capacity, even though its impact studies, preliminary opinions, formal opinions and observations are very thorough. The EDPS has the power to refer cases to the Court of Justice of the European Union, but it does so rarely. It cooperates with other data protection authorities, in particular the Article 29 Working Party (Art. 29 WP) to promote consistency in the application of personal data protection rules throughout the EU. In the police and judicial protection fields, its role is limited to encouraging respect for data protection. However, it works with national data protection authorities to monitor the EURODAC system. Many observers hoped that the European Commission's revision of the 1995 Directive would widen the scope of the EDPS's powers, especially in the police and judicial cooperation fields. This does not seem to be the case. The LIBE Committee's proposed amendments could be seen as a tentative step in this direction, but its proposals are much less ambitious than those of rights and freedom defenders.

2. November 2013
3. Taken from the EDPS website.

The **Article 29 Working Party** (Art. 29 WP) was created pursuant to Article 29 of Directive 95/46/EC. It is an independent consultative body that works with the European Commission. It is composed of representatives from each national data protection authority, a representative from the EDPS and a representative from the European Commission (who does not have the right to vote)[4]. It provides expert opinions and promotes the uniformity of data protection principles in Member States by way of recommendations on subjects it considers important (in particular in the field of new technologies). Its opinions and reports are authoritative. The Art. 29 WP examines any questions on the implementation of national measures adopted under Directive 95/46/EC in order to contribute to the uniform application of such measures throughout the EU, and informs the Commission of any divergent practices in Member States. It also issues opinions (that are subsequently made public) on the level of data protection in third countries.

The proposed General Data Protection Regulation establishes an **independent European data protection board** to replace the Art. 29 WP[5]. Under this proposal, the board would have more power than the Art. 29 WP in order to ensure the Regulation is consistently applied, in particular by issuing guidelines and opinions on measures with Europe-wide impacts as part of the new consistency mechanism for national data protection authorities[6].

Under the proposed Police and Criminal Justice Directive, the board has similar powers as those established under the proposed Regulation. In particular, its responsibilities include coordinating national data protection authorities[7].

National data protection authorities, created by each Member state, are responsible for monitoring the implementation and application of the 1995 Directive on the national level. They have the power to investigate, intervene and launch legal proceedings. However, they often suffer from a lack of resources. In addition, as the 1995 Directive gave Member States considerable leeway in setting up these organisations, there are discrepancies in terms of the powers accorded to national data protection authorities and the procedures that data controllers must respect. This is because the Art. 29 WP has a non-binding advisory status only.

The proposed revision introduces the **one-stop shop principle**. Under this principle, if a company operates in several Member States, it is the data protection authority in the company's main country of operation that decides whether a breach of data protection rules has taken place. This decision is then shared with other national data protection authorities under a cooperation mechanism. The European Data Protection Board issues opinions and, in case of disagreement, the European Commission can adopt implementing acts[8]. At the time of writing, Board discussions were underway. The exact procedure for this mechanism is therefore unknown at this stage.

Under the proposed Police and Criminal Justice Directive, data protection authorities have fewer and more vaguely defined powers, which paves the way for different interpretations in different Member States. The Directive provides for the establishment of a specific national data protection authority, but Member States can designate another supervisory authority for the purposes of the Police and Criminal Justice Directive and another one for the purposes of the regulation. However, if the personal data of EU citizens is to be treated equally and efficiently, an independent European authority – such as the EDPS – must be able to monitor data processing, ensure consistency and hear appeals.

4. Member States in the European Economic Area (Iceland, Liechtenstein and Norway) have observer status, as do some candidate countries (Croatia – now a Member State – and the Former Yugoslav Republic of Macedonia).
5. Proposal for a General Data Protection Regulation, Art. 64.
6. Explained briefly below. See also: Proposal for a General Data Protection Regulation, Arts. 57-60.
7. Proposed Police and Criminal Justice Directive, Art. 49.
8. Proposed Regulation, Art 57.

1.3. The Council of Europe's Convention 108

The Council of Europe's (COE) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, commonly called **Convention 108**, dates back to 1981. It was the first legally binding international instrument of universal scope in the data protection field. The COE has 47 members, including the EU's 28 Member States, but any third country can ratify the Convention[9]. The Convention was drafted to avoid abuses in personal data collection and processing following technological advances in the 1970s that led big companies and public administrations to develop large databases. It applies to both the public and private sectors. The European Court of Human Rights in Strasbourg can hear any cases on the non-respect of Convention 108, because it is linked to the Convention of Human Rights by way of Article 8 on the respect for private life.

As **Directive 95/46/EC** does not apply to data processing for **police and judicial cooperation in criminal matters** on the EU level, the **Council Framework Decision 2008/977/JHA** was issued to cover cross-border operations in this field[10]. Consequently, Convention 108 is the only document to cover national data collection and processing in this field (with no cross-border element) in the EU.

Convention 108 is currently being **modernised** to take into account new technological challenges. This modernisation also aims to strengthen the mechanism monitoring the application of the Convention in Member States who have ratified it, and open up the ratification process to regional or international entities such as the EU. The most recent modernisation proposals of November 2012 are currently being finalised by an ad hoc committee before being submitted to the Council of Europe's Committee of Ministers.

The modernisation process, which began one year before the proposed revision of the 1995 Directive, aims to incorporate considerations on effective national and regional experience to strengthen individuals' rights and promote a high-quality protection model to CoE Member States. It also aims to integrate the provisions currently contained in the Additional Protocol of 2001 on data protection authorities and data transfers to countries that are not party to the Convention. The new Convention would also apply the "privacy by design" principle to products and services intended for data processing. It also includes a monitoring and follow-up mechanism for implementation by parties[11].

Examining this globally oriented proposal involves consulting several non-European states that have already adopted laws on personal data protection, international organisations and non-profit organisations representing stakeholders[12].

9. The first non-European country to ratify the Convention was Uruguay, underlining the document's universal scope.
10. Generally speaking, the Framework Decision has been criticised for not sufficiently protecting individuals' data.
11. The text proposed by the Convention's committee on 18 December 2012 is available in French: http://www.coe.int/t/dghl/standardsetting/dataprotection/CAHDATA/CAHDATA(2013)01_F_vers_13_11_2013.pdf and English: http://www.coe.int/t/dghl/standardsetting/dataprotection/CAHDATA/CAHDATA(2013)01_En_%20Working%20doc_Conv%20108%20.pdf
12. http://www.coe.int/t/dghl/standardsetting/dataprotection/CAHDATA/CAHDATA(2013)ToR_E_04%2011%202013.pdf

2. SCHENGEN INFORMATION SYSTEM II (SIS II)

2.1. Framework

2.1.1. Links with other EU policies

2.1.1.1. The Schengen policy

The first version of the Schengen Information System (SIS) – which resulted from the Schengen policy launched in 1985 – began operating in 1995. The Schengen policy involved the abolition of internal border controls to make it possible for people to move freely within the Schengen Area. It also involved the tightening of external border controls.

A central shared database listing persons and objects wanted in each Member State was created. This allowed national police forces and border officials in different Member States to arrest a person or refuse him/her entry into the Schengen Area. This database also made it possible to track people's movements within the Schengen Area.

This cooperation between Member States led to the signature in Schengen (Luxembourg) of the initial Schengen Agreement, which progressively abolished internal borders. It was followed by a Convention implementing the Agreement in 1990. When it took effect in 1995, seven countries were signatories. Based on an intergovernmental agreement, the Schengen Agreements are today part of EU legislation.

The States that participate in SIS II are the 22 EU Member States in the Schengen Area[13], four non-EU countries in the Schengen Area (Iceland, Lichtenstein, Norway and Switzerland) and the United Kingdom and Ireland (for police and judicial cooperation). A total of 28 countries are today party to SIS II. In early 2014, Romania, Bulgaria and Cyprus will also begin using SIS II. Croatia's use of the system will depend on the date the country is authorised to become part of the Schengen Area.

2.1.1.2. A stronger tool to combat terrorism

Since the terrorist attacks of 11 September 2001, Member States have stepped up cooperation activities to combat terrorism. SIS, which is considered to play a key role in the security of the Schengen Area, has undergone technological improvements so it can be used for terrorist investigations and to prevent terrorist attacks[14].

The scope of SIS has been extended to cover new Member States (countries part of the EU and EEA enlargement[15]) and new functionalities. Other authorities, such as EUROPOL[16] and EUROJUST[17], now have access to the new version of the system, called SIS II. New categories and types of data have been created, including for example biometric data (photos and fingerprints). The overall aim of the second-generation SIS system is to collect more data and ensure better cooperation between police authorities, so as to apply laws more effectively.

13. At the time of writing – 31 October 2013 – these countries are Austria, Belgium, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Slovakia, Slovenia, Spain and Sweden.
14. The connection between the second-generation SIS and the EU's counterterrorism strategy can be found in Council Regulation (EC) 871/2004 of 29 April 2004 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism; in Council Decision 2005/211/JHA of 24 February 2005 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism; and in the European Union Counter-Terrorism Strategy.
15. European Economic Area
16. The EUROPOL (European Police Office) agency was created by the EUROPOL Convention in 1995 (since replaced by Council Decision 2009/371/JHA). EUROPOL is the EU's law enforcement agency, and helps Member States with their international investigations.
17. EUROJUST (European Union Judicial Cooperation Unit) was created by Council Decision 2002/187/JHA (since amended by Council Decision 2009/426/JHA in 2009). It is the European agency in charge of judicial cooperation in criminal cases, and assists Member States in this field.

2.1.1.3. A tool to create an “area of freedom, security and justice”

The aim of creating an area of freedom, security and justice where citizens can move about freely (without facing obstacles such as borders, administrative burdens or discrimination) features in long-term strategies identifying priorities for the years ahead, including the Tampere programme, the Hague Programme and, more recently, the Stockholm programme (which ends in 2014).

This aim has led to a wide range of policies and issues: the fight against discrimination, police and judicial cooperation, free movement, asylum and immigration policies, the fight against terrorism, etc. Because SIS II is a preventative and investigative tool that makes it possible to observe movements within and at the border of the Schengen Area, it is considered essential in attaining this objective.

2.1.2. Purpose of SIS II

Many different organisations have access to SIS II: national border control agencies; police, customs and judicial authorities; visa issuing authorities; vehicle registration authorities and European agencies such as EUROPOL and EUROJUST. The international agency INTERPOL will also be given access to the system once it signs an agreement with the EU. SIS II is a central database where Member States’ authorities record “alerts” on people or objects for the purposes described in the Schengen Convention.

When a third-country national enters into the Schengen Area or lodges a visa application with a European embassy or consulate, a query is launched in SIS II to ensure there is no alert for the applicant. If no alert exists and the applicant satisfies all the other criteria required to obtain a visa, the issuing authority can approve the request. If there is an alert on the applicant, his/her application is automatically refused. Of all the complaints relating to SIS filed with data protection authorities, over half concern third-country nationals who have been refused visas. Alerts are based on national decisions that may not be justified or respect the strict conditions imposed by the law. Rules for creating SIS II alerts can vary from one Member State to another, which is evidence of a lack of consistency. For these reasons, SIS II is a high-risk database as far as data protection and discrimination is concerned.

With respect to objects, the system is mostly used to create alerts for stolen vehicles. For example, if a car is stolen in one Member State, its data is recorded in SIS II and checked against cars entering or exiting the Schengen Area.

However, the second-generation SIS II system has also become a tool supporting investigations by national and European law enforcement authorities. Considering the increased volume of information that the database can now legally process and the increased number of people who can access the system, SIS II is a high-risk investigation and information transfer tool.

2.1.3. The SIS II legal framework

2.1.3.1 Texts implementing SIS II

The first version of SIS was created by two instruments in the Schengen Agreements of 19 July 1999: the Schengen Agreement on the gradual abolition of checks at the common borders, and the Convention implementing the Schengen Agreement. To adapt to the EU’s changing structure, these agreements were incorporated into EU law.

SIS II is governed by three laws, which each cover different fields of activity. Council Decision 2007/533/JHA[18] covers police and judicial cooperation; Regulation 1987/2006[19] of the European Parliament and of the Council covers issues related to visas, asylum, immigration and the free movement of persons; and Regulation 1986/2006[20] of the European Parliament and of the Council covers the services responsible for issuing vehicle registration certificates.

2.1.3.2. Data protection texts

The Council of Europe's Convention 108 and Recommendation 87 on personal data processing in the police field set out the legal data protection principles for data processed by SIS II. As Directive 95/46/EC only applies to processing operations covered by Community law (and not to police or judicial activities), it is applicable only with respect to the independent status of national data protection authorities, which have the power to monitor the national elements of SIS II (the N-SIS) in each Member State.

2.1.3.3. Texts on the involvement of specific actors

The laws on SIS II also contain references to the EU legislation creating the EU-LISA[21], EUROPOL and EUROJUST agencies to underline aspects of their activities using SIS II.

2.2. Scope of SIS II

2.2.1. Impact on citizens: entering and moving around the EU

SIS II was originally a tool for finding people and objects that aiming to prevent cross-border crime and protect the external borders of the Schengen area. It has since become a means of excluding people, primarily thanks to its use by police authorities. The principle of free movement within the Schengen area seems only to apply to nationals of Member States. Third-country nationals entering the EU are subject to extensive restrictions and checks. These restrictions are even stricter for people in difficult situations, such as immigrants and asylum seekers, whose personal data is often entered into the system without it being possible for them to check whether these alerts respect the principles of legality and proportionality. The system therefore has a major impact on the right to freedom of movement.

2.2.2. Data collected

Following the SIS II upgrade, the amount and types of data collected have significantly increased. There are two main categories of data (divided into subcategories): people and objects.

18. Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II)
19. Regulation (EC) 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)
20. Regulation (EC) 1986/2006 of the European Parliament and of the Council of 20 December 2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates
21. Regulation (EU) 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (EU-LISA). This agency is responsible for the operational management of SIS II, VIS (the Visa Information System) and EURODAC (the database on asylum seekers, applicants for international protection and illegal immigrants). EU-LISA's headquarters are in Tallinn (Estonia), its operations are in Strasbourg (France) and its backup computer is in Sankt Johann Im Pongau (Austria).

2.2.2.1. Alerts on individuals

SIS II records alerts on different categories of individuals (whether they are EU nationals or not):

• persons wanted for arrest for surrender purposes on the basis of a European Arrest Warrant and persons wanted for extradition purposes;

• missing persons;

• persons sought to assist with a judicial procedure (whether they are witnesses, suspects or defendants;

• persons subject to covert surveillance or specific checks.

The following data can be collected on individuals:

• **personal data:** last name(s) and first name(s), name(s) at birth, previous name(s), aliases, place and date of birth, and sex;

• **physical data:** objective physical characteristics not subject to change;

• **biometric data:** photographs and fingerprints;

• **contextual data:** whether the person is armed, violent or has escaped;

• **alert information:** the name of the authority that issued the alert, the reason for the alert, a reference to the decision behind the alert, link(s) to other alerts in SIS II, the type of offence and measures to be taken.

2.2.2.2. Alerts on objects

As far as **objects** are concerned, alerts have the following objectives:

• discreet surveillance or specific checks: this includes vehicles, boats, aircraft and containers;

• seizure or use as evidence in criminal proceedings: this includes motor vehicles, trailers, firearms, blank official documents, identity papers, registration certificates and/or number plates, banknotes, securities and means of payment[22].

2.2.2.3. Other data exchanges

Other data can also be exchanged on a conditional basis. This includes:

• european arrest warrants for persons sought for surrender purposes;

• data stolen from victims in cases of suspected identity theft (for example, personal details, physical appearance, biometric information, etc.).

In addition, SIRENE bureaux, which connect authorities in each participating Member State, collect their own supplementary information to help further activities.

2.2.2.4. Data retention period

Different types of alerts are retained for different lengths of times.

For **alerts on persons**, data protection principles are applied. As a result, alerts are only kept for the time required to meet the purposes for which they are created. For example, a missing person who has been found should no longer appear in SIS II.

Therefore, three years after **alerts are created on wanted persons**, participating Member states must determine whether to delete them or not. For discreet surveillance and specific checks, this period is reduced to one year after the creation of the alert.

22. Council Decision 2007/533/JHA of 12 June 2007, Article 38 (2): "(a) motor vehicles with a cylinder capacity exceeding 50cc, boats and aircrafts; (b) trailers with an unladen weight exceeding 750 kg, caravans, industrial equipment, outboard engines and containers; (c) firearms; (d) blank official documents which have been stolen, misappropriated or lost; (e) issued identity papers such as passports, identity cards, driving licenses, residence permits and travel documents which have been stolen, misappropriated, lost or invalidated; (f) vehicle registration certificates and vehicle number plates which have been stolen, misappropriated, lost or invalidated; (g) banknotes (registered notes); (h) securities and means of payment such as cheques, credit cards, bonds, stocks and shares which have been stolen, misappropriated, lost or invalidated."

If an extension of the retention period is considered necessary, participating Member States must provide justification for their decision and keep statistics on requests for extensions. In the absence of any action by the issuing country, the alert is automatically deleted.

However, SIS II legislation does not set a clear maximum retention period for alerts. It does state that this period should be "short" and determined by national law. Four months before the end of the retention period, the central SIS II database (CS-SIS) sends a notification to the issuing Member State to decide whether or not to keep the alert.

For **objects** that are wanted for seizure or use as evidence in criminal proceedings, alerts are retained for ten years. For objects subject to discreet surveillance and specific checks, the retention period is five years.

Personal data exchanged as supplementary information by national SIRENE bureaux is kept for the time required to meet the purposes of collection. Otherwise it is deleted a maximum of one year after the alert was created for the person concerned. However, Member States can keep this information in national databases, in which case the retention period is determined by national legislation.

2.2.2.5. Operational capacities

In January 2012, there were over 42 million entries in the first version of SIS. These included:
• 40.8 million entries on objects;
• 1.2 millions entries on individuals.

Of the entries on individuals, 692,000 concerned "undesirable" aliens[23].

In SIS II, there are around 45 million alerts, including:
• 39 million alerts on lost or stolen documents;
• 5 million alerts on stolen cars.

SIS II has an operational capability of 70 million alerts and, according to system tests prior to implementation, it can manage up to 100 million alerts without requiring technological upgrades[24]. SIS II was designed with flexibility in mind…

2.3. SIS II operations

2.3.1. Technical architecture

SIS II is composed of:

• a **central system** (Central SIS II), which is composed of the central SIS II database and a standard national interface (NI-SIS) for each participating Member State;

• **national systems** in each participating Member State. These national databases (N.SIS II) communicate with the central system via the NI-SIS interface. N.SIS II systems contain a complete or partial "national copy" of the SIS II database, which is used for queries run in Member States on information contained in Central SIS II;

• a **communications infrastructure** linking CS-SIS to the different NI-SIS, which provides an encrypted virtual network for SIS II data exchanges and SIRENE bureaux data exchanges.

23. Source: Council of the EU (2012), Note from the French Delegation – Document 8281/12, 28 March 2012.
24. Source: European Commission Memo Questions and Answers: Schengen Information System (SIS II) 9 April 2013.

Other participating Member States cannot directly access national data contained in another N.SIS II. To consult this information, they must carry out a search in Central SIS II. If the search yields a hit, the requesting authority must then contact the national authority that created the alert.

2.3.2. Operational procedures

Actors responsible for different operations

On the national level, N.SIS II offices in each participating Member State transmit alerts to Central SIS II. These offices are also responsible for N.SIS II operations and security. This means they give the relevant authorities access to SIS II, while taking steps to ensure all national actors meet legislative requirements. Often these offices are located in police departments or Interior Ministries. In many Member States, the police's IT or ICT department is in charge of N.SIS II[25].

The role of **SIRENE bureaux** is to provide requesting authorities with supplementary information related to alerts and to check the quality of information entered into SIS II. These bureaux therefore have full access to the SIS II system.

Each authority is responsible for the alerts they create.

On the European level, the **EU-LISA** agency is responsible for the operational management of the information systems SIS II, VIS and EURODAC. In particular, it adopts and implements security measures, checks the separation of data in the three systems and ensures respect for data protection principles.

2.3.2.1. Actors with full or partial access to SIS II

The right to consult SIS II varies from actor to actor.

Actors with full access to SIS II include:

- in the field of border control: authorities responsible for identifying third-country nationals;
- in each Member Sate: the police, customs and judicial authorities designated by participating Member States.

Actors with partial access to SIS II only have access to information that is necessary for them to carry out their duties. This includes:

- for immigration data: authorities responsible for issuing visas (embassies/consulates) and central immigration authorities;
- for number plate checks and information connected with vehicle declarations: authorities responsible for registering vehicles;
- for alerts in connection with arrests, discreet surveillance, specific checks, or objects wanted for seizure or use as evidence in criminal proceedings: EUROPOL;
- for alerts in connection with arrests and judicial affairs: EUROJUST.

If an agreement is signed between the EU and INTERPOL, the latter organisation may be given partial access to SIS II data on stolen, misappropriated, lost or invalidated passports. Before this agreement is concluded, the EU has requested that INTERPOL (and countries which have delegated members to INTERPOL) provide an adequate level of personal data protection and respect for fundamental freedoms. In any case, no data transfer can take place without INTERPOL obtaining prior approval from the EU Member State that created the alert. In return, EU countries will be given direct access to information in the INTERPOL database on missing or stolen travel documents.

25. List of N.SIS II Offices and the national SIRENE Bureaux:
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2013:103:0117:0124:EN:PDF

2.3.2.2. Data safety guarantees

2.3.2.2.1. General security measures

Participating Member States, including SIRENE bureaux and the EU-LISA agency for operational management, are responsible for the system's overall security. This includes protecting infrastructure, monitoring who accesses data (through logs), managing data (access, use, transfers, etc.) and evaluating the system (with audits). All persons working with SIS II are bound by professional secrecy.

Member States are legally responsible if individuals' rights are breached. They must impose sanctions if SIS II is used fraudulently or if supplementary information is illegally exchanged.

The interlinking of alerts must respect the conditions set for each alert.

Every two years, EU-LISA publishes a report for European institutions on SIS II's technical operations and its communications infrastructure, including any supplementary data transmissions. Every four years, the European Commission completes an overall evaluation of SIS II and supplementary data transfers.

The data processed cannot be reused for other administrative purposes.

Joint supervision of SIS II is carried out by the Schengen Joint Supervisory Authority (Schengen JSA), which publishes opinions on personal data protection issues. The JSA also assesses difficulties in interpreting or applying the legislation and, more generally, any difficulties concerning the exercise of the individuals' rights. In addition, it drafts proposals to resolve any problems encountered.

This cooperation also involves carrying out audits and inspections.

2.3.2.2.2. Supervision of SIS II access

Given the many actors able to consult SIS II, several legislative procedures have been created to monitor access to the system. These include:

- recording when national authorities, EUROJUST and EUROPOL access SIS II;
- continually updating the list of people who can access SIS II;
- monitoring transfers to check which actors have the right to receive personal data;
- monitoring data entry to check which personal data has been recorded, when it was recorded, who recorded it and why it was recorded.

These procedures also apply to EUROJUST and EUROPOL.

2.4. SIS II: Difficulties and risks

2.4.1. Difficulties

The legislation governing SIS II is extremely complex and difficult to control. It is based on an outdated vision of the EU's competencies.

2.4.2. Risks

Lack of control

The wide scope of SIS II, which is expected to be more extended, means it requires powerful technology. However, given the hacking of the Danish N.SIS II less than two months after it was launched[26] and the seven-year delay in implementing the system, questions can legitimately be asked as to whether SIS II is really under control – on the national and European levels, and from a security perspective.

26. As mentioned in the European Data Protection Supervisor's June 2013 newsletter.

The risks of a flexible, security-oriented tool

SIS and SIS II were designed to help Member States meet security requirements following the implementation of the Schengen policy. These requirements were strengthened after the terrorist attacks of 11 September 2001.

Since then, other agencies such as EUROPOL, EUROJUST and even INTERPOL have been added to the system. Even though there is currently no evidence that their presence has led to increased danger (as the system has only been operational for a short period of time), the European Data Protection Supervisor and the Schengen Joint Supervisory Authority have both criticised their inclusion, or at least the lack of justification and clarification concerning their roles.

Although SIS II was designed as a search tool, there is a risk that it will become an investigation tool. The massive amount of information in SIS – plus the information in SIS II and the introduction of biometric data – make it the EU's largest information system. If data is insufficiently protected and actors inadequately monitored, this could have serious repercussions for the individuals concerned. In addition, SIS II legislation states people will be identified on the sole basis of their fingerprints "as soon as this becomes technically possible"[27], despite the fact that experts consider this kind of data to be unreliable when used without additional data. Nor does the legislation specify what alternative measures should be taken when it is impossible to collect fingerprints.

The limitations of legislative texts

The conditions under which an individual can access his/her data in SIS II are governed by national legislation. This right of access can be direct or indirect. If the right is indirect, authorities in participating Member States have no set deadline for informing third-country nationals or national data protection authorities that their data is recorded in SIS II. Generally, individuals become aware their data is recorded in the system when they attempt to legally enter the Schengen Area or when they unsuccessfully apply for a visa. The national data protection authority becomes aware of this situation when the individuals concerned file complaints.

This situation has a serious impact on the freedom of movement of third-country nationals. They suffer additional discrimination in filing appeals – as they cannot enter the Schengen Area, they cannot defend themselves in person.

27. See Article 2(c) of Council Decision 2007/533/JHA and Article 22(c) of Regulation 1987/2006: "as soon as this becomes technically possible, fingerprints may also be used to identify a person on the basis of his biometric identifier".

3. VISA INFORMATION SYSTEM (VIS)

3.1. The common visa policy meets the fight against terrorism

In order to permit the free movement of people in the Schengen Area, the EU introduced a **common visa policy** to prevent "consulate shopping". This is when a third-party national, who is refused a visa to one Schengen country, requests a visa from another Schengen country. The common visa policy applies to short-term visas (visas valid for less than three months which must be used within six months of being issued) and transit visas for the EU territory or airport transit areas. For all other visas, Member States set their own visa policies.

The common visa policy is based on five main elements. One of these elements is VIS, the database allowing Schengen States to exchange data (for example, photographs, fingerprints, names, etc.) on visa applicants. VIS is also part of the **Stockholm Programme**'s policy on reinforcing external border controls. It is used as part of **counter-terrorism activities**, which explains why law enforcement agencies and EUROPOL have the right to access VIS data if that will substantially contribute to the prevention or detection of terrorist offences[28]. Finally, VIS and EURODAC are two of the elements necessary for the implementation of the **Dublin III Regulation**, which aims to determine which state is responsible for processing asylum applications. With respect to VIS, the Member State that issued a visa to an asylum seeker is responsible for processing the resulting application for asylum. National authorities in charge of asylum applications can consult VIS for this purpose. On the European level, the EU-LISA agency is responsible for the operational management of VIS (see the section on SIS II).

3.2. Purpose of VIS: monitoring access to the Schengen Area

By recording information on visa applicants and making it available to all Schengen States and EUROPOL, VIS aims to monitor who enters and immigrates to the Schengen Area. The system seeks to ensure that successful visa applicants are not wanted persons and/or that they will not remain in the Schengen Area illegally.

3.2.1. Using VIS to issue visas and identify individuals

VIS is not only used when an individual applies for a visa. It is also used during the visa's validity period and for future requests lodged by the same individual.

When the individual applies for a visa, the authority responsible for issuing visas in the Schengen State collects data on the applicant's identity (including biometric data) and stay (see the table below for information on the data collected). The authority also records the individual or company sponsoring the applicant and/or bearing the costs of his/her stay.

The authority creates a visa applicant file in VIS where all the applicant's data is sent. Next, the authority checks whether the applicant has made any other applications in the last five years. If there is a pending application, the authority refers the applicant back to the original country of filing to prevent "visa shopping". If there is a successful application, it is linked to the current application. The outcomes of previous applications are taken into account for future applications. Connecting files makes it easier for the relevant authorities to select applicants and therefore monitor those entering the EU. If a visa is refused, withdrawn or given a reduced validity period, the reasons for these decisions are recorded in VIS.

28. Regulation (EC) 767/2008, Article 3.

Most of the complaints filed with the EDPS on VIS concern unsuccessful visa applications. It is important to note that just because a visa is refused once it should not necessarily be refused subsequently. Each application should be judged on the information available at the time of processing.

In addition, for group travel, individual visa applications are linked to those of the rest of the party. This is true for groups where the individuals know each other (family or friends), but also for groups where individuals do not know each other (for example, individuals travelling together for a group holiday organised by a travel agency).

The authorities responsible for issuing visas enter, correct and delete data in the system. The data controller is often part of the visa issuing authority, but can also be part of another authority, depending on the situation in each Member State[29].

If a visa application is successful, VIS is used when controls take place at Schengen borders and within the Schengen Area. The national authorities in charge of these controls have access to VIS.

3.2.2. EU security policies: using VIS for law enforcement

In order to prevent, detect and investigate terrorist offences and other serious criminal offences, EUROPOL and national authorities also have access to VIS.

The EUROPOL agency accesses VIS to collect and analyse information and intelligence for counter-terrorism, drug-trafficking and serious international crime prevention purposes. EUROPOL must anonymise the data collected so that individuals can no longer be identified. To consult VIS, the EUROPOL unit concerned requests permission from the participating Member State that entered the data in the system.

National authorities have more flexibility. They can carry out searches using a wide range of data when processing visa applications. This includes using the contact details of the person who issued an invitation to the applicant and/or who is paying for the applicant's living expenses during his/her stay. If the search yields a hit, national authorities can consult other data from the application form and photographs. To access VIS, they must request permission from an authority designated by a participating Member State, which forwards the request to the central national authority.

National authorities have access to more information in VIS than EUROPOL. They can consult several different types of data, which increases data vulnerability. To prevent abuses, these authorities, and the authorities that give them access to the system, must take precautions.

3.3. VIS operational capabilities

At the time of writing[30], VIS had not been rolled out on a worldwide basis. Following the launch of operations in October 2011, the database is now operational in 11 of the 23 planned regions[31].

When it reaches full capacity, the VIS system will be the world's largest biometric database, containing the ten fingerprints of up to 70 million people applying for visas over a five-year period[32].

29. List of competent authorities the duly authorised staff of which shall have access to enter, amend, delete or consult data in the Visa Information System (VIS) (2012/C 79/05), 17.03.2012. Document available here: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:079:0005:0018:EN:PDF (accessed 14 November 2013).
30. November 2013.
31. The system has been launched in North Africa, the Near East, the Gulf region, West and Central Africa, East and Southern Africa, South America, Central Asia, South-East Asia and the Occupied Palestinian Territory. On 30 September 2013, the European Commission adopted a Decision on the last group of regions where VIS will be rolled out. This group concerns the Schengen States in that VIS also applies to visa applications at the borders of these countries. For more information, see:
http://eeas.europa.eu/delegations/westbank/documents/news/20131107_faqonvis_en.pdf
32. 32. European Commission press release: "Visa Information System (VIS): The JHA-Council reaches a political agreement on the VIS Regulation and VIS Decision", Brussels, 12 June 2007.
http://europa.eu/rapid/press-release_IP-07-802_en.htm (page accessed 14 November 2013).

It was anticipated that VIS would process up to 20 million visa requests per year from citizens of 134 countries, and that there would be 100,000 transactions per day. It was initially thought that this data would come from 30 states supporting up to 3,500 consular posts and 12,000 end-users[33].

33. Presentation by Daon, supplier of identity assurance software, on the EU Biometric Matching, 2008: http://www.nws-sa.com/biometrics/EU_Matching_CS.pdf (page accessed 14 November 2013).

3.4. Data collected and data collection: risks caused by the non-respect of data protection principles

<table>
<tr><td colspan="5">Data collected for visa applications</td></tr>
<tr><td colspan="4">Applicant's data</td><td>Data on the person issuing the invitation and/or bearing the costs of the applicant's stay</td></tr>
<tr><td colspan="3">Identity data</td><td>Stay and application information</td><td rowspan="2">Individual</td><td>Compagny</td></tr>
<tr><td>Administrative data</td><td colspan="2">Identity data</td><td>Stay information</td><td>Application information</td><td>Compagny</td></tr>
<tr><td rowspan="2">• Last name, name at birth (including previous names)
• First name(s)
• Sex
• Date, place and country of birth
• Current nationality and nationality at birth
• For minors: address and first and last name(s) of mother and father
• Current profession and employer
• For students: name of educational institution
• Type and number of travel document with the name of the issuing authority, date of issue and expiry date</td><td colspan="2">• Scanned photograph
• 10 fingerprints*</td><td rowspan="2">• Main destination
• Length of stay
• Purpose of travel
• Planned arrival and departure dates
• First border crossed or transit itinerary</td><td rowspan="2">• Application number
• Place and date application filed
• Type of visa requested
• The indication that a visa has been requested</td><td rowspan="2">• Last name
• First name
•Address</td><td rowspan="2">• Company name
• Address
• First and last name of a contact person</td></tr>
<tr><td colspan="2">* Exceptions:
• Children under 12 years of age
• People who are unable to provide fingerprints (for example, people with no hands, shaking hands or damaged fingertips)
• Heads of State and members of a national government, and the members of their official delegation when invited for an official purpose</td></tr>
</table>

Depending on the situation (whether the visa is refused, issued, extended or shortened), administrative information is added (e.g. name of the authority that made the decision). If the visa is refused, withdrawn, cancelled or shortened, reasons are indicated. There are seven reasons a visa can be refused, which range from false identity documents to insufficient means of returning to the country of origin[34]. In addition, a non-admission alert in SIS II automatically leads to the visa application being refused.

3.5. Disproportionate and discriminatory data collection

The Article 29 Working Party (Art. 29 WP) has recommended that the data of persons inviting applicants or bearing their costs not be recorded in VIS on the grounds that it is disproportionate given the database's purpose. If this data must be recorded, only central national authorities in charge of issuing visas should be able to consult it. The Art. 29 WP also considers that visa applicants should not be asked their birth nationality to avoid discrimination[35]. In addition, it has requested that the term "third-party national" be more precisely defined to make it possible to exclude from VIS all those who have obtained a residence permit in a Schengen State.

3.6. Disproportionate data retention periods

For stays of up to three months in the Schengen Area, visa applicants' data is recorded for five years[36]. Recording data for such a long period of time goes beyond supporting the visa application process, and amounts to controlling individuals who enters the Schengen area.

To avoid this situation, the Art. 29 WP has suggested establishing differentiated data retention periods depending on the outcomes of visa applications and their different elements[37]. For instance, the retention period would be shorter for visa applications refused on administrative grounds (because of a lack of travel documents or insufficient means of subsistence). Longer retention periods would apply to visa applications refused on more serious grounds such as criminal convictions. Among others, the Art. 29 WP suggests retention periods of a few weeks or months for administrative refusals, the automatic deletion of visa applications refused on public health grounds once the problem has been resolved, and the automatic deletion of links between applications filed for group travel once the visa has expired. If a visa has been refused because of an alert exists in SIS II, the Art. 29 WP recommends the VIS retention period be the same as the SIS II retention period.

3.7. Ten fingerprints and the impossibility of objecting to their collection

It is disproportionate to retain data on all ten fingerprints for a five-year period when the application is for a three-month visa and the purpose of the data collection is to identify or check the identity of the visa applicant or holder. Requesting all ten fingerprints implies that the person is a potential criminal.

This is especially important given that the only people excused from providing fingerprint information are those who are physically unable to do so or those for whom the reliability of the data would be questionable (for example, children under 12 years of age). If an individual refuses to provide his/her fingerprints, the visa application is not processed. There is no other alternative.

---

34. See Article 12 of Regulation 767/2008.
35. Opinion 2/2005 on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas (COM (2004) 835 final), Adopted on 23 June 2005, ARTICLE 29 Data Protection Working Party.
36. The start date of the data conservation period varies depending on the situation. See Article 23, Regulation 767/2008.
37. Opinion 2/2005 on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas (COM (2004) 835 final), Adopted on 23 June 2005, ARTICLE 29 Data Protection Working Party.

3.8. Data collection detrimental to data protection

Biometric data collection can take place outside Schengen embassies and consulates, and may be carried out by external service providers. However, service providers should only be used in exceptional circumstances and for appropriate reasons. Contracts concluded with service providers should contain confidentiality clauses in line with data protection principles. Even if these precautions are taken, outsourcing data collection means exposing visa applicants to further risks, in particular the risk that their personal data is misappropriated. This is especially dangerous in countries considered non-democratic and countries where corruption is widespread. In these countries that are not subject to the same data protection rules, outsourcing data collection should be prohibited, because it could affect an individual's right to privacy and even endanger him/her (for example, the service provider could inform the authorities or third parties that the person has applied for a visa).

3.9. VIS and individuals' rights

Citizens' rights are established in Chapter 6 of Regulation 767/2008/EC 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 (VIS Regulation).

3.9.1. Right to be informed

When data, photographs and fingerprints are collected for visa applications, the Schengen State responsible for the data collection must provide the following information in writing to applicants:

- the identity of the data controller, the national data protection authority and its contact details;
- the purposes of VIS data processing;
- the recipients of this data, including the national law enforcement agencies in charge of preventing, detecting and investigating terrorist offences and other serious criminal offences;
- the data retention period;
- the fact that the data collection is mandatory for the processing of the application;
- **the fact that they have rights with respect to the processing of their data**: the right to access their data, the right to correct erroneous data, the right to delete data that has been processed unlawfully, the right to obtain information on exercising their rights and the right to obtain the contact details of national data protection authorities with which they can file complaints concerning personal data protection.

This information must also be given to people who issue invitations to applicants or bear the cost of their stay in form(s) that they fill in and sign. If no form is available because information is not collected directly, the data controller must inform them when their data is recorded or, if data is communicated to a third party, when the data is first communicated.

3.9.2. Procedures for accessing, correcting and deleting data and filing appeals

Any person has the right to access data concerning him/her that is recorded in VIS, and to find out which Schengen State transmitted this data. He/she must be able to exercise this right without hindrance, at reasonable intervals and without excessive delays or costs. Access to personal data can be authorised by any Schengen State.

An individual can ask any Schengen State to correct or delete data. However, it is the Schengen State that processed the visa application that must actually correct or delete the data. The Schengen State contacted by the data subject must contact the Schengen State that processed the visa application and recorded the data within a 14-day period. The latter then has one month to check the accuracy of the data. The procedure for checking this information is established in national legislation.

Depending on the situation:

• if the data is erroneous or was not lawfully processed, the relevant Schengen State corrects or deletes it immediately and sends prompt written confirmation to the person concerned;

• if the data is not erroneous and was lawfully processed, the relevant Schengen State promptly informs the data subject in writing, and provides justification for its decision.

In the second situation, the Schengen State must also inform the data subject of his/her options for appealing the decision. This includes providing information on appeals options in the country concerned: filing a complaint with the relevant authorities or judicial institutions and obtaining assistance from national data protection authorities.

Any request to access, correct or delete data must be recorded by the Schengen State in which the data subject exercises this right.

The EU launched an information campaign on VIS the year it was implemented in the first third countries[38].

38. The different documents in this campaign are available here in French, English and German (page accessed 22/11/2013): http://ec.europa.eu/dgs/home-affairs/e-library/multimedia/publications/index_en.htm#0801262489da9f79/c_

4. “European Dactyloscopy” or EURODAC

Note: The following presentation is based on the new law adopted in June 2013, which is expected to come into force in July 2015.

EURODAC will contain data on individuals applying for asylum in EU Member States ("persons seeking international protection"), as well as third-country nationals and stateless persons who are apprehended when crossing irregularly an external border of the EURODAC territory or found staying illegally within this territory. EURODAC rules apply to all Schengen States, whether or not they are EU Member States[39]. That being said, Denmark does not participate even though it is a Schengen country, while the United Kingdom and Cyprus, which are not Schengen countries, take part in EURODAC.

On the European level, the main body involved is EU-LISA (see the section on SIS II). Furthermore, unlike SIS II and VIS, EURODAC is not made up of national systems connected to a central database; the central file is the only record.

In December 2009, there were a total of **1,544,558 entries**[40] in the earlier version of EURODAC, broken down as follows:

- 1,454,315 entries on persons seeking international protection[41]
- 90,243 entries on persons apprehended at the external border of a participating State[42]
- 42,053 persons staying illegally within the territory covered by EURODAC[43]

4.1. Connection with EU policies:

from the Schengen policy to the Stockholm Programme, from a tool for applying the Dublin III Regulation to a tool available to law enforcement authorities

The Schengen policy, which effectively removed internal borders within the Schengen Area and created a single external border, led to participating countries cooperating to combat illegal immigration. EURODAC also contributes to this general goal. In direct connection with the Schengen policy, EURODAC is also a part of the Common European Asylum System (CEAS) and, as such, is intended to facilitate application of the **Dublin III Regulation**, or Regulation 604/2013, used to determine which Member State is responsible for examining an application for international protection.

Furthermore, the **new Regulation (EU) 603/2013 establishing EURODAC** allows for Member State law enforcement agencies and EUROPOL to access data stored in EURODAC for the purpose of comparing personal data to prevent, detect and investigate terrorist activities and serious criminal offences. While EURODAC originally enabled only participating countries to exchange information in connection with an application for international protection or when a third-country national was found illegally staying in a Member State, the recent reform gives EURODAC a new role, which falls directly in line with implementation of the successive Hague and Stockholm Programmes. **The Stockholm Programme** sets out new priorities until 2014, and promotes an "open and secure" Europe where Member States must, for the purposes of law enforcement activities, exchange information.

---

39. On 25 November 2013, at the time of writing, the EU Member States concerned are Austria, Belgium, Denmark (not participating in EURODAC), Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, the Czech Republic, Slovakia, Slovenia, Spain and Sweden. The non-Member States concerned are Iceland, Liechtenstein, Norway and Switzerland.
40. Source: European Commission, Annual report to the European Parliament and the Council on the activities of the EURODAC Central Unit in 2009, COM/2010/0415 final, 2 August 2010
41. *Ibid.*
42. *Ibid*.
43. *Ibid*.

4.2. Purposes of EURODAC

4.2.1. Determine the country responsible for processing an application for international protection

The primary role of EURODAC is to determine which participating State is responsible for examining an application for international protection under the Dublin III Regulation, which uses hierarchical criteria to achieve this goal.

The first criteria are designed to facilitate family reunification. If these criteria do not apply, it must be determined whether the applicant irregularly crossed the border of a State from a third country, in which case this State is responsible for examining the application for international protection (this responsibility ends 12 months after the irregular crossing). Furthermore, when no participating State can be assigned responsibility based on the other criteria, the first State in which the application for international protection was lodged is deemed responsible for examining the application.

In this context, EURODAC can serve to implement the Dublin III Regulation by facilitating digital fingerprint comparisons to verify whether a person seeking international protection or a third-country national found to be illegally staying in a participating State has already lodged an application in another participating State, as well as to verify whether a person seeking international protection irregularly entered a participating State. These checks can be used to apply the appropriate Dublin III Regulation rules to determine which State is responsible for processing an application for international protection.

4.2.2. Help combat terrorism and serious crime: stigmatizing a vulnerable group

Under the new Regulation, each participating State will designate a competent authority in charge of preventing, detecting and investigating terrorist offences and other serious crimes, which will be authorized to request the comparison of fingerprints with EURODAC data.

However, national authorities and EUROPOL do not have unlimited access to EURODAC. They must request and justify a consultation, and fulfil a series of conditions. For example, they must have unsuccessfully checked other fingerprint databases to establish a person's identity. The comparison must also be needed for a specific case; systematic searches are strictly forbidden. As an example, EUROPOL can access EURODAC when the agency wants to compare a latent fingerprint found at a crime scene. Information EUROPOL obtains following a comparison with EURODAC data can only be processed with permission from the Member State that transmitted that data to the central system.

This new feature of the EURODAC system, namely access for law enforcement officials, was strongly criticised by the EDPS, Art. 29 WP, EURODAC Supervision Coordination Group and EUROPOL supervision group, who condemned the lack of evidence proving the necessity of such a change.

Allowing such access stigmatises persons seeking international protection by treating them as potential criminals when they are actually assumed to be a very vulnerable group. In addition, the EURODAC text does not identify which types of information can be shared with law enforcement officials when there is a hit.

4.3. Little data, but important data: for subsequent verifications and exchanges

As mentioned earlier, EURODAC will contain data on three categories of people. The data stored on individuals in the first two categories – individuals who have applied for international protection or individuals apprehended in connection with the irregular crossing of an external border – differ somewhat. **It should be noted that fingerprints can only be recorded if the individual in question is at least 14 years old.**

The data recorded for the first two categories of people are as follows:

Type of applicant	Applicant for international protection *Data collected when the application is lodged*	Third-country national or stateless person found illegally crossing an external border[44]
Personal data recorded	• All 10 fingerprints, or at least of the index fingerprints • Sex	• All 10 fingerprints, or at least of the index fingerprints • Sex
Administrative data recorded	• Member State of origin (or State where the application was lodged), place and date of the application for international protection[45] • Reference number used by the Member State of origin • Date on which the fingerprints were taken • Date on which data were transmitted to the central system • Operator user ID	• Member State of origin (so the State that entered the data), place of apprehension and date of the application for international protection[46] • Reference number used by the Member State of origin • Date on which the fingerprints were taken • Date on which data were transmitted to the central system • Operator user ID
Supplementary information recorded	Information on the applicant's status in connection with the application, as applicable: • Individual's arrival date, after a transfer • Date on which the individual concerned left the territory of the States covered by EURODAC for at least 3 months • Date on which a return decision was made regarding the individual, or on which the individual was expelled from the territory covered by EURODAC or left this territory following withdrawal or rejection of the application • Date on which the decision to examine the application was made	No other information is stored.
Retention period	**Stored for 10 years** in the central system. After expiry of this period, automatically deleted by the central system.	**Stored for 18 months** in the central system. After expiry of this period, automatically deleted by the central system.
Conditions for advance deletion	Acquired nationality of a participating State. The central system informs all States that entered the data of such a fact as soon as possible.	Obtained a residence permit, left the territory covered by EURODAC or acquired nationality of one of the participating States.

44. For third-country nationals or stateless individuals apprehended while irregularly crossing an external border, this refers to an individual in one of the following situations: a decision has not been made to turn the person back; a decision was made to turn the person back but the person remains physically on the territory of the Member States and is not kept in detention prior to removal on the basis of the decision to turn him or her back.
45. In the event of a transfer (Regulation 603/2013, Article 10(b)), this date is the date of transfer.
46. In the event of a transfer (Regulation 603/2013, Article 10(b)), this date is the date of transfer.

Clarifications: *In contrast to the case of individuals seeking international protection, data on third-country nationals and stateless individuals apprehended in connection with the irregular crossing of an external border is not automatically compared to determine criteria under the Dublin III Regulation. It is recorded for subsequent comparison with data sent to the central system as part of an application for international protection, in this case to help determine the Dublin III criteria to apply to ascertain which State is responsible for the application (see section 4.2.1). This data is also compared by law enforcement officials and EUROPOL when such bodies request a comparison.*

With regard to the third category of individuals, those apprehended (e.g. on public transport) **and discovered to be illegally staying in a EURODAC country**, only fingerprints are collected, and for the sole purpose of **comparison** to check if an application for international protection has already been submitted in a participating State. This is especially the case if the person declares that he or she has already lodged an application for international protection without indicating in which country, if the person says he or she has not lodged an application but opposes being returned to his or her country of origin because he or she would be in danger or if the person attempts to avoid being sent to a third country by preventing his or her identity from being established. This data **is not compared** with data on individuals apprehended while irregularly crossing an external border. It is **not stored** in EURODAC.

Finally, it has been observed that less personal data is exchanged in EURODAC relative to other systems presented in this monograph (which does not reduce their criticality). This can be explained by the fact that EURODAC is a fingerprinting system, which therefore primarily stores digital fingerprints. However, **this does not mean that other personal data, such as names and nationalities, is not stored or exchanged.** They are kept in national files, as indicated by the reference number used in EURODAC. Under the Dublin III Regulation, States exchange personal data on an applicant for international protection to determine the State responsible for that application. **Such exchanges constitute administrative cooperation**, and occur directly between States via a secure email system.

State use of EURODAC

Once fingerprints are collected, the competent authorities must promptly send the data to EURODAC's central unit, where they are automatically compared with stored fingerprints previously submitted by other Member States.

The Central System then communicates the hit or negative result to the Member State that requested the comparison.

- If there is no hit with fingerprints already stored in EURODAC, the central unit reports this to the inquiring State without sending any other information.

- If the prints of a person seeking international protection match prints already stored in EURODAC, the central unit transmits the data identified in the table above to the State that requested the comparison.

States only have access to information they transmit to EURODAC. They cannot access data from other States unless there is a hit with data already in the system. The national bodies responsible for amending or deleting inaccurate data should be the authorities responsible for applications and granting asylum in the Member State that entered the data.

4.4. Problem of proportionality

When a third-country national lodges an application for international protection in a participating State, that person's ten fingerprints, along with other data, are collected and recorded by the competent national authorities. But taking ten fingerprints to identify one person is not proportional to the objective. Taking ten fingerprints, when combined with the ability of law enforcement authorities and EUROPOL to access these prints, amounts to treating applicants as potential criminals.

4.5. Legal vacuum and inability to refuse fingerprinting

Since EURODAC is strictly a digital fingerprint system, collecting fingerprints is mandatory. If a person is temporarily unable to be fingerprinted, the prints will be taken "as soon as possible".

The texts specify that **the fact that it is temporarily or permanently impossible to take and/or to transmit fingerprint data**, due to reasons such as insufficient quality of the data for appropriate comparison, technical problems, reasons linked to the protection of health or due to the data subject being unfit or unable to have his or her fingerprints taken owing to circumstances beyond his or her control, **should not adversely affect the examination of the application for international protection lodged by that person.** However, this information is not included in any article of the text enacting EURODAC; it is only found in Recital 20[47]. The fact this is missing from the body of the text, as pointed out by the EURODAC Supervision Coordination Group, shows that there is a legal vacuum in the EURODAC texts. This raises the question of whether, given EURODAC's role, the person will still be included in the system and, especially, whether his or her application will still be processed.

Furthermore, it is important to note that an applicant's refusal to be fingerprinted can negatively impact the credibility of his or her application, which will be rejected because the individual will be perceived as not having made enough effort to help establish his or her true identity.

4.6. Risks related to the transfer of data to third countries

If a search results in a hit in EURODAC, **the data used for this search can be transferred to third countries, unless there are serious risks that could be detrimental to the applicant** (e.g. torture, inhuman or degrading treatment, or any other violation of basic human rights). This applies to data that is not stored in EURODAC's central system but which comes from a Member State and is communicated between Member States following a hit in the Central System. Given the ambiguity of the term «serious risks», this type of transfer should be prohibited to prevent any misinterpretation.

4.7. EURODAC and citizens' rights

Citizens' rights are identified in Article 29 of Regulation 603/2013.

Right to information:

A person whose data is entered in EURODAC shall be informed of:

- the identity of the controller, who is the person or organisation that defined the purposes and means of the processing of personal data, and of his or her representative, if any;
- the purpose for which his or her data will be processed in EURODAC, including a description of the aims of the Dublin III Regulation;
- in intelligible form, using clear and plain language, the fact that EURODAC may be accessed by Member States and EUROPOL for law enforcement purposes;
- the recipients of the data;
- the right of access to data;
- the right to request that inaccurate data relating to him or her be corrected or that unlawfully processed data relating to him or her be deleted;
- the right to receive information on the procedures for exercising these rights.

47. 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), Recital 20.

This information must be given at the time of fingerprinting, and no later than at the time when the data relating to him or her is transmitted to the central system (especially in the case of individuals found illegally staying on the territory of a participating State). This information must be provided in writing, and in a language the person understands. Where the person concerned is a minor, the information shall be provided in an age-appropriate manner.

Right to access information stored in the system:

• The person may obtain communication of the data relating to him or her which are stored in the central system, as well as the identity of the Member State that transmitted them to the central system.

• The individual shall be able to exercise this right without constraint, within a reasonable timeframe and at a reasonable cost.

• This right of access may be exercised in each participating State (but only one State can authorize access).

Right of correction and deletion:

• Any person may request that data which are inaccurate be corrected or that data recorded unlawfully be deleted. The correction and deletion shall be carried out without excessive delay by the Member State which transmitted the data.

• If data recorded in the Central System are factually inaccurate or were recorded unlawfully, the Member State which transmitted them shall correct or delete the data and confirm in writing to the data subject that it has taken action to correct or delete data relating to him or her.

• If the Member State does not agree that this is the case, it shall explain in writing to the data subject without excessive delay why it is not prepared to correct or delete the data. That Member State shall also provide the data subject with 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.

Furthermore, if the person applied for international protection, he or she has the right to assistance from the national data protection authority (DPA) to exercise these rights.

5. EUROPEAN CRIMINAL RECORDS INFORMATION SYSTEM (ECRIS)

5.1. European policies: free movement and reinforced mutual assistance in criminal matters

5.1.1. Free movement: "mobile" convictions

Free movement allows EU citizens and their families to move and live freely in any Member State. The EU has therefore decided to also make convictions "mobile", meaning European citizens cannot delete their judicial history by crossing borders.

5.1.2. Mutual assistance in criminal matters: systemising exchanges

This refers to cooperation between Member State judicial authorities to collect, for example, information and evidence for the purposes of criminal investigations or legal proceedings. ECRIS is a new tool for facilitating this type of cooperation, which itself is not new. The first European law on exchanging information from criminal records was the 1959 Council of Europe Convention on Mutual Assistance in Criminal Matters, which was ratified by all EU Member States. Within the EU, this text was supplemented with the Council Act of 29 May 2000 establishing the convention on mutual assistance in criminal matters between the Member States of the EU[48].

ECRIS goes beyond these texts by establishing regular, systematic cooperation. When a judicial authority in one State seeks information because it must render a verdict on a citizen of another State, the Member State of nationality must promptly report previous criminal convictions to the inquiring Member State. Under ECRIS legislation, the State of nationality must send all information on all of that person's convictions without necessarily sorting the convictions beforehand, according to the needs of the judicial authority requesting the information. This calls into question whether the principle of proportionality is being respected.

5.1.3. Tampere European Council and The Hague and Stockholm Programmes: recognising decisions in criminal matters without harmonisation

The conclusions reached in 1999 by the Tampere European Council reinforced that the EU aims to be an "area of freedom, security and justice", which requires the creation of a secure area in which individuals can move freely. More specifically to ECRIS, the Tampere conclusions indicated that judgements in criminal matters must be recognised in all Member States. The subsequent Hague and Stockholm Programmes continued to develop the measures necessary for a secure space for citizens, by reinforcing judicial cooperation between Member States. ECRIS is intended to directly contribute to the creation of this area by reinforcing the exchange of information extracted from criminal records between EU Member States.

Recognition across the EU does not challenge the plurality of judicial systems. Based on mutual trust, this scheme presupposes that each State has an acceptable judicial system and that it is not necessary to question convictions handed down under such systems, especially based on the definition of

48. Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union.

violations, crimes or non-indictable offences, or the length of time for which they are recorded. However, it is possible to imagine this leading to unequal treatment of EU citizens, for example in the case of abortion, which is punished after some weeks in some Member States but not in others[49]. Instead of eliminating such inequalities, ECRIS will cause them to persist and even give rise to an abuse of information exchanges.

5.1.4. The fight against terrorism: A threat to basic rights

The European Council's 2004 declaration on combating terrorism[50] establishes the fight against terrorism as a priority; to this end, it was decided that the exchange of information on criminal convictions had to be improved. The Hague Programme takes up this point, insisting on intensifying the exchange of information from criminal records, including information on the loss of certain rights following criminal convictions.

When it is understood that the fight against terrorism often breaches the minimum rules for protecting individuals' rights, it is worrying to see that ECRIS, which affects large numbers of people, fits into this context. It is all the more concerning given that the fight against terrorism is overused as a pretext.

Is it really reasonable to include one person who has committed a "minor" non-indictable offence, someone who has committed sexual offences and another person who has committed an act of terrorism in the same system? This approach automatically creates a conflict between the proportionality and purpose principles.

5.2. ECRIS objectives: keep records of convictions of EU citizens within the EU

ECRIS enables Member States to retain, within the convicted person's State of nationality, a history of all convictions handed down in all Member States, to achieve several aims.

5.2.1. Maintain complete, up-to-date criminal records of EU citizens

As a computerised system, ECRIS is designed to facilitate the transmission of information from a European citizen's criminal record between the Member States concerned. Specifically, it deals with information on criminal convictions handed down in criminal courts and, if possible, other information such as specific circumstances underlying the decision. A Member State that imposes a sentence on a citizen of another Member State will therefore use ECRIS to inform the convicted individual's State of nationality of that conviction. The convicted person's Member State of nationality will then add that conviction to the individual's criminal record. The objective is to enable each Member State to keep its citizens' criminal records complete and up-to-date, including even convictions from other Member States. This last point raises the practical question of how one State can record a conviction for a crime that does not exist under its own law.

---

49. For example: Take two women in the same situation, who terminated an unwanted pregnancy at the same stage of pregnancy. The abortion is recorded on one woman's criminal record in one State (which has banned abortion), but not on the other woman's. These two women then apply for the same civil servant position in the same country, with the same skills. If the civil service can consult each woman's «full» criminal record, it will know about one woman's abortion but not the other's. Behind every civil service is a person who reasons with his or her own conscience; even if that country's law forbids discrimination against job candidates based on past abortions, the more personal information unrelated to the purpose in question is revealed, the higher the risk of discrimination.
50. Declaration on combating terrorism, Brussels, 25 March 2004.

5.2.2. Inform judicial authorities of an accused individual's past convictions

Member States must also transmit information on their citizens' convictions (determined by another EU State) to other Member States' central authorities, upon request, for the purposes of criminal proceedings. This often occurs when a judicial authority must render a verdict concerning a citizen from another EU country and wants to know, among other things, if the person has a criminal history. However, as mentioned earlier, it seems that all convictions are sent, without sorting them according to the requestor's needs, which renders ECRIS's objective dangerous.

5.2.3. Know if an individual's rights have been revoked

ECRIS is also used to inform the appropriate stakeholders if a citizen has lost certain rights owing to a conviction. This information is available even without legal proceedings when the law of one country authorizes or obliges an employer to enquire about a candidate's convictions, as is the case for certain jobs (e.g. in contact with children, security positions) and when an authority must know a person's history before allowing him or her to practice certain professions (e.g. doctors, lawyers). Depending on the country, the information may come as a certificate of good conduct, which does not contain any conviction information, or an extract from a criminal record. If this approach is not tightly regulated (e.g. established list of jobs concerned) and error-free, it may undermine reintegration of an individual who has served his or her sentence or integration of that person in another country, negatively affecting his or her right to freely choose a job.

5.2.4. Future possibilities

At present, ECRIS only affects EU nationals, but the EU intends to eventually include all persons living within its borders. Member States are exploring the idea of supplementing ECRIS with a "European index of convicted third-country nationals" for foreign nationals living in a Member State, with a view to exchanging information on their prior criminal convictions[51].

5.3. Questionable laws

5.3.1. ECRIS texts: open to interpretation

ECRIS was created by the Council Framework Decision 2009/315/JHA of 26 February 2009, and implemented by Council Decision 2009/316/JHA of 6 April 2009. In each Member State, the national laws and regulations governing criminal records as well as those implementing European and international laws are also applicable to ECRIS.

The texts implementing ECRIS are highly questionable. To begin with, they lack clarity and even have deficiencies, leaving too much room for interpretation. For example, they do not explain how a State should transpose a conviction that does not exist under its own laws. They also frequently refer to national laws. The 2010 manual of procedure[52] indicates that in certain States an individual's permission is not required to send information to an administrative authority for purposes other than criminal proceedings, or the individual concerned must explain why he or she is requesting an extract from his or her criminal record. With regard to identification, some States require additional personal information (e.g. parents' names, fingerprints) that the State which has been requested the information must provide if it has such information.

51. For more information, please see: http://www.publications.parliament.uk/pa/cm201213/cmselect/cmeuleg/86-xviii/8619.htm, http://ec.europa.eu/justice/criminal/european-e-justice/ecris/
52. Note from Council Secretariat to Delegations, Council Decision on the exchange of information extracted from criminal records – Manual of Procedure, 21 April 2010.

Furthermore, several basic data protection principles are flouted by the poor quality of the texts. As mentioned earlier, the purpose of ECRIS is too broad, owing especially to integration of the counter-terrorism policy. The idea of proportionality lacks precision, even if only concerning the personal information that must be sent to legal authorities, and has not been defined clearly enough to be practically implemented. As the scope depends on each national system, there is much to criticise in the resultant unequal treatment of citizens. In its Opinion of 16 September 2008, the EDPS recommends that only the person concerned be allowed to request information from his or her criminal record. It also points out that the circumstances in which criminal record information can be requested outside of criminal proceedings are not sufficiently defined. It is unfortunate that the majority of the EDPS's key proposals were not incorporated in the final ECRIS text.

In addition, the information exchanged is automatically translated using two coded reference tables (non-indictable offences and crimes). These tables do not standardise the definitions of the offences or the sentence lengths applied under the different national systems, they simply serve to give an understanding of the national systems.

The reliability of this method is highly questionable. In addition to increasing the risk of errors when encoding information, not knowing the national laws of the originating country leaves too much room for interpreting offences, which is highly prejudicial to the individuals concerned.

Finally, the lack of precision concerning the supervision of data processing raises the question of whether the principles of security, rights of individuals and transparency are indeed upheld.

5.3.2. Weak data protection, missing guarantees and the need for strong legislation

The European data protection laws applicable to ECRIS are the European Convention on Human Rights, the Council of Europe's 1981 Convention 108, and Council Framework Decision 2008/977/JHA of 27 November 2008, which was strongly criticized for not affording enough protection to individuals. This Framework Decision was integrated as a result of the EDPS's 2008 Opinion, which called for the Framework Decision to be adopted before adopting ECRIS to ensure there was a minimum structure in place for protection.

It is important to note that, contrary to the other systems examined in this monograph, Directive 95/46/EC (the 1995 Directive) does not apply to ECRIS as it is not applicable to police and judicial cooperation in criminal matters. Nonetheless, the revision of the 1995 Directive proposes a directive on the protection of personal data processed in connection with the prevention and detection of crime, criminal investigations and proceedings, and enforcement of sentences, which would repeal the current framework of Decision 2008/977/JHA.

Regulation (EC) 45/2001 on the responsibility of European institutions does not apply to ECRIS either. This means that no EU institution is responsible for ECRIS. Consequently, the EDPS does not have competency to supervise data processing, and there is no coordination between the EDPS and national data protection authorities for implementation or monitoring of the system. It should be noted that the EDPS did request such coordination in its 2008 Opinion, but in vain. This is dangerous for European citizens because there is no supranational supervision of exchanges between Member States, which leaves a large margin for error and weakens the protection of citizens in general. Furthermore, not updating an individual's criminal record can have serious consequences for that person, making strict monitoring of exchanges more than necessary.

The concern over monitoring is heightened by the lack of precision around the entities in charge of supervising data processing at the national level. Insofar as the 1995 Directive does not apply, national laws have effect, but certain national data protection authorities may not have competence over criminal

records. Among the countries examined for this project, for example, this is the case in Luxembourg, where police and judiciary files are the responsibility of a specific supervisory authority which is independent of the data protection authority and presided over by the State public prosecutor.

Additionally, the security measures identified in ECRIS legislation stipulate that no Member State's authority can access any other Member State's databases, and that Member States must guarantee the confidentiality and integrity of criminal record information transmitted to other Member States. However, these measures are only relevant if implementation of ECRIS is actually supervised.

Between a weak Framework Decision, obsolete texts and the absence of key texts, the protection of individuals subject to ECRIS seems quite feeble. Consequently, it is essential that the aforementioned proposed directive on police and legal cooperation be adopted and be strong enough to prevent this type of inconsistency and provide real protection for the individuals concerned.

As it currently stands, ECRIS legislation does not provide the minimum guarantees for protecting individuals.

5.3.3. National laws: plurality of systems and the ability to request criminal records for professional purposes

National laws and regulations on the structure of national criminal record systems and the definitions of crimes and cases in which such information can be used are applicable to information exchanged via ECRIS.

The 1959 European Convention on Mutual Assistance in Criminal Matters is also relevant for ECRIS. Specific clauses in other European texts also refer to the use of ECRIS.

• Article 10 of Directive 2011/93/EU authorizes employers to know of a candidate's prior convictions for offences involving children and of disqualification from exercising activities involving any contact with children. The candidate's consent is required.

• Article 50 of Directive 2005/36/EC on the recognition of professional qualifications authorizes competent national authorities to demand the criminal record – less than three months old – of a professional looking to reside in their Member State. This applies to "regulated" professions, which vary from one country to another. Such professionals may work, for example, in health care (e.g. doctors, nurses), security (e.g. security guards, firemen), law (e.g. lawyer, notary), airports and architecture[53].

Since criminal record systems and use are not standardised across Europe, implementation of ECRIS involves a multitude of national texts, and therefore several national procedures, which increases the risk of misuse and complicates the task of supervising ECRIS.

5.4. Data collection and retention period

For every conviction that appears on a criminal record, the State that convicted the person will transmit the following information to the State(s) of nationality of the individual concerned:

53. For more information, see the European Commission's regulated professions database: http://ec.europa.eu/internal_market/qualifications/regprof/index.cfm?fuseaction=regProf.index&lang=en

Mandatory information	**Optional information**	**Additional information**	**Secondary information**
	Information that must be transmitted if the convicting State usually enters it in criminal records	*Information that must be transmitted if the convicting State usually enters it in criminal records*	*Information that may be transmitted*
▪ **On the individual convicted:** last name, first name, date of birth, place of birth (town and State), sex, nationality and, if applicable, previous name(s) ▪ **On the nature of the conviction:** date of conviction, name of the court, date on which the judgement became final ▪ **On the offence giving rise to the conviction:** date of the offence and name or legal classification of the offence, as well as reference to the applicable legal provisions ▪ **On the contents of the conviction:** notably the sentence as well as any supplementary penalties, security measures and subsequent decisions modifying the enforcement of the sentence	▪ Convicted person's parents' names ▪ Reference number of the conviction ▪ Place of the offence ▪ Disqualifications arising from the conviction	▪ Convicted person's identity number or type and number of the person's identification document ▪ Convicted person's fingerprints ▪ Pseudonym and/or alias name(s)	Information on attenuating or aggravating circumstances related to the offence[54]

54. Art. 11(1)(c) of Framework Decision 2009/315/JHA says that the transmission of such supplementary information is not compulsory.

The differences between types of data do not appear in the form used to request information extracted from the criminal record[55], as the categories are not visible. Furthermore, the note on identification information, *"To facilitate the identification of the person as much information as possible is to be provided"*, creates confusion as to what can legally be included in the form.

As for **the retention period** of convictions entered in criminal records, the law is not clear. That being said, since the context of the conviction depends on each Member State, it can be assumed that the retention period will depend on the country that sentenced the person.

Take the example of a French citizen who committed a crime in the United Kingdom: When the United Kingdom sends information on the conviction to France, France will apply the United Kingdom's retention period rules. So, if the conviction would be kept on record for ten years in the United Kingdom but only two years in France, the conviction must remain on the French citizen's criminal record for ten years. The United Kingdom must inform France that it must remove the conviction at the end of the ten years.

This further complicates ECRIS, and means that each European citizen will be treated differently for the same offence.

5.5. Operational implementation

ECRIS is not a centralized system, it is actually decentralized. Consequently, in contrast to the other systems examined, ECRIS does not have a central database. All criminal records are maintained at the national level, and ECRIS relies on the direct exchange of information between competent national authorities. ECRIS can be described as a method that enables Member States to know what is in the criminal records of their citizens and other EU citizens they are prosecuting.

Each Member State must designate one or more authorities to handle requests related to its criminal record database. These authorities are called "competent authorities" or "central authorities". They are the only bodies with access to their citizens' criminal records.

Central authorities are responsible for:

• transmitting information on convictions to the State of nationality of individuals convicted on their territory, including sending any modification to the conviction such as a new entry, removal or amendment;

• receiving and storing information on their citizens transmitted by another State, which includes updating criminal records according to the modifications made by that State;

• transmitting information on their citizens' convictions upon request from the central authority of another State during criminal proceedings brought against their citizens or during non-criminal proceedings in the case of extracts from criminal records and certificates of good conduct. The information must be up to date.

The authorities may be:

• The Ministry of Justice (as in Italy) or a specific department thereof (as in Luxembourg)
• A specific administrative service responsible for criminal records (as in France)
• The national police or a department thereof (as in Denmark)
• The Ministry of the Interior (as in Lithuania)

The United Kingdom, because of its decentralised system, has one coordination authority and multiple regional authorities. The three jurisdictions of Scotland, Northern Ireland, and England and Wales, have separate criminal history systems, different offences and different penalties[56]. The coordination authority therefore forwards the requests from other Member States to the competent regional authority. It is also responsible for sending the responses to the States that requested information.

55. Annex of Framework Decision 2009/315/JHA.
56. Note from Council Secretariat to Delegations, Council Decision on the exchange of information extracted from criminal records – *Manual of Procedure*, p. 103, 21 April 2010.

5.6. Citizens' rights of information and correction

An individual's right to access information entered in his or her criminal records depends on the national law of his or her Member State of nationality. That being said, by virtue of the right to protection of personal data that exists in the countries examined for this project, individuals have the right to know of existing files and the personal data contained therein.

In Germany and in France, to avoid external pressure, individuals may consult their entire criminal record but they cannot obtain a copy. This does not apply to the Czech Republic or Portugal. Furthermore, some States guarantee unrestricted access, while others need to know why access is requested.

The right of correction also depends on national law. However, since information must always be updated before it is transmitted, it can be assumed that countries that allow individuals to access their criminal record also allow them to correct this information or offer the possibility of judicial appeal. In all cases, the competent institutions are national bodies.

LDH, Ligue des droits de l'Homme
www.ldh-france.org

AEDH, Association européenne
pour la défense des droits de l'Homme
www.aedh.eu

Humanistische Union
www.humanistische-union.de

HCLU, Hungarian Civil Liberties Union
www.tasz.hu/en

ALOS-LDH, Action Luxembourg Ouvert
et Solidaire - Ligue des droits de l'Homme
www.ldh.lu

MEDEL, Magistrats européens
pour la démocratie et les libertés
www.medelnet.eu

This publication is cofunded by the Fundamental Rights Program of the European Commission.