GOVERNMENT DATA
COLLECTION

Are people at risk?

Comparative overview

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

April 2014

SUMMARY

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

INFORMING CITIZENS ON DATA COLLECTION
PASSPORT FOR THE PROTECTION OF PERSONAL DATA

COMPARATIVE OVERVIEW OF LEGISLATION AND PRACTICES AS REGARDS INSTITUTIONAL FILING IN FOURTEEN EUROPEAN UNION STATES, IN THE CONTEXT OF THE EU LEGAL FRAMEWORK

INTRODUCTION - CONTEXT

Citizens are ignorant of the scope of the institutional filing that they and their relatives are subject to. Consequently, they are not aware that this filing might be abusive, even when it is permitted by law. Based on country assessments and a comparative overview (filing systems and relevant legislation, the powers of data protection authorities or DPAs, the appeals process, etc.), our project aimed to develop awareness-raising tools and an information campaign informing European citizens of how their personal data is used and the rights they have in this field.

In parallel, the project aimed at alerting decision-makers to the need for more protective legislation. This is especially true in the current context, where an increasing number of filing systems have been created for security reasons (the "anti-terrorism" argument often being used to justify data collection since the terrorist attacks that took place on 11 September 2001 in the United States).

Our project refers to the principles in the Convention for the Protection of Human Rights and Freedoms (Article 8: "Everyone has the right to respect for his private and family life") and the Charter of Fundamental Rights that has been binding since the 2009 Treaty of Lisbon (Article 7: "Everyone has the right to respect for his or her private and family life, home and communications" and Article 8: " Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority"). The project also refers to general or specific European Union (EU) texts, as well as texts from the Council of Europe on the protection of individuals as regards their personal data processing.

Given that the Directive 95/46/EC is currently being revised (in 2012, the European Commission proposed a replacement regulation on personal data protection and a new directive on personal data protection with respect to judicial and police cooperation in the penal field), an assessment of personal data protection on the national and European levels is more necessary than ever. This assessment deserves recognition from decision-makers and the public.

The following organisations participated in this project:

- Two European networks: **AEDH** (European Association for the Defence of Human Rights) and **MEDEL** (Magistrats européens pour la démocratie et les libertés);

- Four national NGOs[1]: **LDH** (Ligue des droits de l'Homme, in France), **HCLU** (Hungarian Civil Liberties Union, in Hungary), **HU** (Humanistische Union, in Germany) and **ALOS-LDH** (Action Luxembourg Ouvert et Solidaire - Ligue des droits de l'Homme, in Luxembourg).

Results of our work include:

- This comparative overview of filing systems, relevant legislation and practices as regards institutional filing in the fields we focused on: police, justice, education, and health. This overview allows us to underline the risks created by these filing systems on the national, European and international levels; to draw up a list of good and bad practices; and to identify differences.

- Fourteen national reports that provide an overview of the filing systems studied; the legislative framework in the country concerned, including the data protection authority (DPA); and any difficulties we encountered while studying the country.

- A summary of European information systems on personal data and the legal framework.

All these documents are published on each partner's website[2] in English and/or the national language.

- A quiz: this is a multiple-choice questionnaire aimed at raising awareness of personal data filing systems and protection.

- A passport: this booklet is available in printed or electronic form and informs European citizens, essentially those from the project's partner countries, of their rights as regards personal data protection and the means they have to enforce and exercise their rights.

- A "Hit Parade": a brief visual summary of filing systems to which we especially want to draw the public's attention.

1. Non-governmental organisation.
2. Websites are listed on the back cover.

METHODOLOGY – FILING SYSTEMS STUDIED

Methodology and fields of action covered

We chose to complete in-depth studies on the countries of the four partner organisations: **France**, **Germany**, **Hungary** and **Luxembourg**. Shorter studies completed by the four national partners and AEDH focused on **Austria**, the **Czech republic**, **Finland**, **Greece**, **Italy**, **Poland**, **Portugal**, **Slovenia**, **Spain**, and the **United Kingdom**.

We chose to study countries that are geographically, historically and culturally representative of diversity in the EU. This allowed us to obtain an overview of institutional filing situations in the EU for the comparative analysis.

At the project's launch seminar, we decided to focus our research on institutional filing systems in four fields: **justice**, **police**, **health** and **education**. This is because EU Member States constantly take action in these fields. Furthermore, filing systems in these fields, especially those of health and education, contain information on large numbers of people.

Countries have gradually centralized and computerized the filing systems studied. To make comparisons possible, we decided to focus on the following points: the purpose of the filing system and its use; registration criteria of data subjects; data collected; the regulatory framework and existing or planned data protection guarantees, especially data storage periods; the role of DPAs; legislative risks or hazards; risks due to non-respect of legislative guarantees; abuses; appeals regarding filing systems; the public's knowledge of filing systems; any protest movements seeking modifications to filing systems; and strengths and weaknesses.

Each partner completed a national report based on:

- In-house skills
- In-house discussions to select topics for each field
- Information collected (documentary research – Internet searches, reports, etc.)
- Interviews with selected experts, workshops bringing together experts, citizens and civil society organisations
- Questionnaires that were sent to selected institutions (Ministries, DPAs or supervisory authorities, trade unions, etc.).

AEDH worked on a presentation of the European legal framework and its developments with regards to the fields we studied. AEDH also produced reports on Greece and Finland

Using this information, the comparative analysis was finalised and recommendations were adopted at both transnational seminars (September 2013 in Berlin and December 2013 in Budapest). An external evaluator, who is an expert in personal data protection, monitored the whole project and completed in-depth evaluations at each stage.

The comparative overview focuses on the following four issues (identified at the second seminar):

• Rights and freedoms endangered by filing systems and their implementation

• The transparency of filing systems and rules governing their management; that is to say, citizens' knowledge of filing systems and information provided on these filing systems

• The appeals process and its navigation; reported use of this process

• The role played by supervisory authorities: their powers, means and actions

Our studies are based on extensive research. Local experts in the legal and technical fields verified the data collected. However, it is not impossible that our documents contain errors caused by the language barrier, the technical complexity of rules applying to these filing systems, practices that do not reflect rules and the difficulty in involving experts. This is despite all the precautions we have taken in order to deliver quality documents.

Filing systems studied

There were many obstacles when comparing national filing systems. In particular, some police filing systems contained data that was also relevant to the justice field. It was therefore difficult to decide which field to attribute the filing systems to. For the comparative analysis, filing systems were attributed to the field of the authority responsible for the database.

The language barrier was another obstacle when searching for information, especially with respect to each country's criminal records database. This contributed to the opacity of filing systems and rules jeopardizing the defence of individual rights.

Lastly, comparisons had to take into account different considerations. For example, when comparing data storage periods for two seemingly similar filing systems, we had to consider which kind of data was saved, how access to the data was controlled, whether practices were different from rules, whether the error rate was high or low, the impact of potential breaches on privacy, etc.

Furthermore, the population concerned also had to be taken into account. For instance, in **Germany**, education filing systems are not national, but exist at local levels (in the Bavaria and Berlin federal states). In **Luxembourg**, it is doubtful whether anonymising data for statistical purposes is an effective way of protecting data subjects considering the small size of the country.

Given the increasing interconnection of national filing systems on the European and even international levels, different management practices and file contents raise concerns for the protection of data subjects.

Filing systems studied in several countries

Justice field

- **Criminal records**: Austria, the Czech republic, Finland, France, Germany, Hungary, Luxembourg, Poland, Portugal, Spain and the United Kingdom

Police field

- **Biometric passports**: France, Germany and Spain
- **Central domicile declaration registers**: Austria and Germany
- **DNA databases**: Austria, the Czech republic, France, Germany, Greece, Italy, Luxembourg, Portugal and the United Kingdom
- **Fingerprint files** to identify offenders, persons involved in offences and/or asylum seekers and immigrants: FAED and AGDREF 2 in France, IDENT1 in the UK, PERPOL and ADEXTRA in Spain and AFIS in Germany
- **Police information files and systems for repressive purposes**: SIGO, INTPOL, PERPOL and Archivo GATI in Spain, RoboCop in Hungary, TAJ and STIC in France, INPOL in Germany, the Integrated System of Police Information in Portugal

Education field

- **Pupil databases**: databases in two German federal states and national databases in Austria, France, Greece, Italy, Luxembourg and Poland.
- The collection of data on **religion, health** and sometimes ethnic origin in education filing systems: Greece, Hungary and Italy.

Health field

- **Health filing systems**: Austria, the Czech republic, Finland, France, Germany, Greece, Hungary, Italy, Poland and the United Kingdom.
- Health filing systems functioning with an **electronic health card**: Austria and Germany.

Filing systems that were studied in one country

These are topics to which one or more partners wanted to draw public attention due to a specific context or risk.

Justice field

- The **Vehicular and Driver Data Register** in Finland
- The **Cassiopée** filing system that collects information on ongoing legal proceedings and the FIJAISV (judicial filing system on perpetrators of sexual or violent offences) in France
- The **Register of Measures Involving Deprivation of Liberty, Requisitions and Non-Final Judgments** and the criminal investigation filing system **INTCF-ADNIC**, which aims to identify and compare biological samples, in Spain.

Police field

- The **anti-terrorism database** in Germany
- The **wanted persons website** in Greece[3]

3. This filing system is described in the justice section of the Greek report. Here, the judiciary decides which data in the filing system will be processed. The Police acts as the data processor.

- The **Managing of Information of Criminal Interest Linked to Minors** (GRUMEN) and the **File for Social Security Frauds** (Archivo SISS) in Spain

- **Video surveillance at the Luxembourg-Findel detention centre** in Luxembourg

- The **Statistical and Monitoring Tool for Assistance to Returning Refugees** (OSCAR), which collects fingerprints, and the **Automated DNA Database** (FNAEG), which originally collected the genetic fingerprints of sexual offenders then those of other persons, in France.

Education field

- **Student databases at universities** in Slovenia

It should be noted that some "pupil" databases are used up to university level: for example, the National Student Register (Italy) and the RNIE database (France).

- The **Personal Skills Booklet** in France

- The **National Library Users' Data File** in Luxembourg

Health field

- The **Newly Diagnosed HIV-Infected Individuals Information System** (SINIVIH) in Spain

- The **file listing Persons Hospitalized Without Their Consent** (HOPSY), the **Collection of Medical Psychiatric Information** (RIM-Psy), the **pharmaceutical filing system**, and the **National Directory for Social Welfare / National Management System of Identifiers** (RNCPS/SGNI) in France

- **Video surveillance at Luxembourg Hospital.**

Institutional filing on the European level

Following the opening of internal borders, the European Union (EU) has created institutional databases and interconnection systems between national databases for security purposes. These systems are governed by personal data protection rules. We studied the following European systems:

Schengen Information System II (SIS II)

The Schengen Information Systems, SIS and SIS II, gather the biometric information of missing persons, wanted persons (so they can be arrested for extradition or for legal proceedings, for instance), and persons under covert surveillance or specific controls. They also gather information on missing objects to make it easier to find them. The issue is whether it is appropriate to collect so much information on people who are simply "suspects" or witnesses in legal proceedings.

EURODAC System

EURODAC makes it possible to identify and carry out checks on asylum seekers on EU territory. The fingerprints of all asylum applicants and unsuccessful asylum applicants are recorded and compared with fingerprints already in the database. This system is supposed to "efficiently" implement the regulation that determines which State processes an international protection application (the Dublin III Regulation[4], which replaced the Dublin II Regulation[5], which in turn replaced the Dublin Convention[6]). This raises questions as to the disproportionate number of prints collected and saved.

4. Regulation (EU) No. 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person (recast)
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:180:0031:0059:EN:PDF
5. Council Regulation (EC) No 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32003R0343:EN:HTML
6. Convention determining the State responsible for examining applications for asylum lodged in one of the Member States of the European Communities - Dublin Convention
http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&numdoc=41997A0819(01)&model=guichett&lg=EN

Visa Information System (VIS, soon to be VIS II

The Visa Information System, VIS, aims at standardising entrance formalities for foreigners who require visas to enter the Schengen area and finding foreigners who "forget" to leave the territory once their short-stay visa has expired. In particular, it aims to prevent foreigners from "consulate shopping" (applying for visas in several European consulates). This system compares biometric data, primarily the ten fingerprints. This raises questions as to the disproportionate number of fingerprints collected and saved after visas are granted or refused on non-criminal grounds.

ECRIS System

ECRIS was implemented in order to facilitate information exchanges between the judicial authorities of Member States with respect to criminal investigations and legal proceedings. ECRIS is not a centralised database on the European level. It organises the electronic consultation of criminal records between one country and another. However, European countries have different definitions of crimes and offences, different procedures for recording convictions and different methods of accessing filing systems. These data exchanges may therefore lead to discriminations.

THE EUROPEAN LEGAL FRAMEWORK

Two founding texts were adopted within the Council of Europe framework. These texts are the Convention for the Protection of Human Rights and Fundamental Freedoms of 1950 (in particular Article 8 on the right to privacy) and the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), which expressly provides for the protection of fundamental rights and freedoms when processing personal data.

Although in the 1980s preparations were being made to abolish internal borders so people could move freely within the EU, very few Member States ratified Convention 108.

Consequently, the Schengen agreements were adopted at the EU level. These agreements made provisions for sharing files on wanted persons, but also created the obligations to ratify Convention 108 as regards data protection and respect the Council of Europe's 1987 Recommendation on data protection in the police sector.

For existing DPAs, these agreements, as well as major advances in the telecommunication fields, meant that the creation of the common market in 1990 would have repercussions on all European personal data transfers. Furthermore, legislation was very different from country to country, which led to different levels of protection. This applied to all aspects of protection systems: the concepts used, principles established, personal rights accorded, and powers of existing DPAs (the existence of which was not recognised in the Convention).

For this reason, national supervisory authorities called on the European Commission to set up a binding legal instrument with a general scope at the annual international meeting in Berlin in 1989. Consequently, as the EU developed, so did an ambitious but complex policy for the protection of individuals with regard to personal data processing, starting in the 1990s.

After the creation of a single goods and services market, a horizontal directive was adopted in 1995 harmonising national legislation on the protection of individuals with regard to personal data processing and the free movement of such data. However, its scope in both the private and public sectors is limited to areas governed by EU law.

To ensure people could move about freely within the EU, a series of shared information systems on individuals were set up, together with specific data protection frameworks. A single DPA, composed of representatives from national DPAs, was set up for all of these systems. In addition to the file on wanted persons mentioned above, filing systems on asylum seekers and visa applicants were also created. Lastly, the Prüm Convention made it possible for police services to transfer data from their databases (genetic data, fingerprints, etc.).

More recently, the Treaty of Lisbon, which came into force on 1 December 2009, made the Charter on Fundamental Rights binding. This Charter creates the right to the protection of privacy (Article 7) and the right to the protection of personal data (Article 8). These rights may be invoked before an independent court[7] in case of a suspected breach by a Member State, an EU institution or an EU body[8]. The treaty also provides for the existence of DPAs.

The Council of Europe's Convention 108, sectoral recommendations and the European Union

The 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, also known as Convention 108, is based on Article 8 of the European Convention on Human Rights concerning the right to privacy. It is the first binding international legal instrument that can be universally applied to the field of protecting individuals' fundamental rights and freedoms with regard to personal data processing. It aims to ensure all parties receive an equivalent level of protection so cross border data movements can continue to be protected. It requires States to adopt legislation complying with the Convention before ratification. However, it does not make provisions for mechanisms checking compliance.

With respect to public security, the Council of Europe adopted a Recommendation on the use of personal data in the police field in 1987 (Recommendation R 87)15 of 17 September 1987. EU agreements and conventions make it compulsory to take this Recommendation into account (this is the case for the Schengen agreements, the Europol convention, etc.). National police filing systems, but also police data processing on the EU level, must therefore be created and/or modified in compliance with Recommendation R (87) 15.

The text of the Convention is currently being modernised to take into account new global challenges with regard to personal data protection. The measures that the advisory committee have suggested incorporating into the Convention include "privacy by design". In other words, the right to personal data protection is taken into account when designing data processing tools and services.

The Convention 108 advisory committee has also suggested that no public or private field of activity should escape data protection measures. National legislation would be checked for compliance with the Convention once before ratification, and then periodically.

7. Article 47 of the EU Charter of Fundamental Rights
8. Under the conditions set out in Article 51 of the EU Charter of Fundamental Rights

There is a lot at stake in this modernisation process. The aim is to confirm the Convention's international scope (in the absence of any binding initiative by the United Nations in the field of personal data protection), to ensure supervisory authorities cooperate when dealing with cross-border complaints and to provide for the joint development of recommendations covering new practical and technical innovations.

Directive 95/46/EC of the European Parliament and of the Council

This directive, adopted on 24 October 1995, deals with the protection of individuals with regard to personal data processing and the free movement of personal data. It develops the principles of Convention 108. The directive aims at ensuring a high level of personal data protection throughout the EU by harmonising national laws to respect this fundamental right and freedom. It confirms the Convention's principles (personal data processing must be implemented for explicit and legitimate purposes, be proportionate to these purposes as far as content and data storage periods are concerned, be accompanied by appropriate security measures) and accords further rights to the data subject, no matter their nationality. This includes the right to be informed when personal data is collected; the right to access personal data; the right to request corrections to erroneous data; the right to oppose a data processing operation on legitimate grounds; and the right not to be subject to a decision which produces legal effects concerning them or significantly affects them and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to them.

Furthermore, this directive precisely defines the circumstances in which personal data processing is deemed legitimate. Data processing is permitted when the data subject gives their explicit consent, or when processing is necessary in order to execute a contract or respect a legal obligation applying to the controller. It establishes reinforced protection principles for sensitive data (ethnic origin, political opinions, etc.) and data transfers to third countries.

Lastly, it creates national supervisory authorities that can carry out interventions before filing systems are implemented (based on obligations to declare filing systems before their implementation) and after filing systems are implemented (investigations, complaints handling, etc.).

Directive 95/46/EC applies to both the public and private sectors. However, it should be underlined that it does not apply, in the case of the public sector, to data processing linked to public security, defence, state security and state activities in areas of criminal law for which the European Union has shared competence or no competence at all.

The European legal framework on personal data protection is currently being revised. It is thought that its scope will be extended to the fields of police and justice. The 1995 Directive would be replaced by a regulation on the general data protection framework (that applies directly to Member states) and a directive on personal data protection with respect to judicial and police cooperation in the criminal field[9]. At a later date, a certification process for personal data processing would also be implemented and specific texts applying to some European data processing operations would be revised. The issues at stake include modern technological challenges and the more uniform application of personal data protection rules in the EU. It is expected that key measures will be implemented, such as the right to digital oblivion, the right to data portability (the data subject's right to get back their data from a service provider so as to be able to transfer it to another service provider of their choice), the power for DPAs to impose financial penalties and the implementation of a standardising mechanism by a European Data Protection Board (to replace the Article 29 Working Party – see below).

9. www.eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:EN:PDF

Specific legal instruments and public filing systems on the EU level

Following the opening of internal borders, the European Union (EU) has created institutional databases, interconnection systems between national databases and information exchange systems for security purposes. In line with the policy initially established in the Schengen agreements mentioned above, the EU adopted specific instruments incorporating data protection requirements (in particular, the Council of Europe's Recommendation R (87) 15 mentioned above).

These specific instruments concern the filing systems on wanted persons (SIS), asylum seekers (EURODAC), short-term visa applicants (VIS), exchanges with Europol and its filing systems, data exchanges with Eurojust and the Council framework decision 2008/977/JHA that applies to data exchanges as part of cross-border operations under the Prüm Convention (this framework decision will be replaced by a directive put forward by the European Commission in 2012, that extends its field of application to all national police filing systems in Member States).

The four European systems studied here are: the Schengen Information System II (SIS II) on wanted persons, the Eurodac system on asylum seekers, the Visa Information System (VIS) and the European Criminal Records Information System (ECRIS).

Data protection bodies in the European Union

The **European Data Protection Supervisor**[10] (EDPS), the EU equivalent to national supervisory bodies, supervises EU institutions and organisations. This position was created in 2001. The Supervisor makes sure that all EU institutions and organisations respect individuals' rights and freedoms when processing their personal data. The EDPS also has an advisory role and cooperates with national supervisory authorities and with the Article 29 Working Party.

***Article 29 Working Party**[11] (Art. 29 WP) is an independent advisory body created by the Directive 95/46/EC and is composed of representatives of national DPAs, the EDPS and the Commission (Commission representatives do not vote). The Art. 29 WP delivers opinions, especially on new proposals by the Commission, and on the level of protection in third countries to which European data might be transferred. It publishes recommendations and reports promoting respect for and the standardization of personal data protection measures in Member States.

***Joint supervisory authorities**

Depending on the context, the supervision of European institutional filing systems may be carried out by national supervisory authorities alone (e.g. for ECRIS), joint supervisory authorities, or national supervisory authorities in cooperation with the EDPS.

10. www.secure.edps.europa.eu/EDPSWEB/edps/EDPS?lang=en
11. www.ec.europa.eu/justice/data-protection/article-29/index_en.htm

GLOSSARY

: « considered to be good practice »
: « considered to be risky practice »

Personal data: “Any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity” (Directive 95/46/EC, Article 2).

Processing of personal data (processing): “Any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction” (Directive 95/46/EC, Article 2).

Personal data filing system (filing system): “Any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis” (Directive 95/46/EC, Article 2).

Controller: “The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law” (Directive 95/46/EC, Article 2).

Third party: “Any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data” (Directive 95/46/EC, Article 2).

Recipient: “A natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not” (Directive 95/46/EC, Article 2).

The data subject’s consent: “any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed” (Directive 95/46/EC, Article 2).

Sensitive data: data listed under “special categories of data” in the 1995 Directive or Convention 108.

- Convention 108, Article 6 (Special categories of data): “Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.”
- Directive 1995, Article 8 (The processing of special categories of data): “Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.”

Interconnection: “Automated linkage of data from filing systems or processing that were previously distinct” (CNIL: http://www.cnil.fr/documentation/fiches-pratiques/fiche/article/comment-determiner-la-notion-dinterconnexion/).

Anonymous data: “Any information relating to a natural person where the person cannot be identified, whether by the data controller or by any other person, taking account of all the means likely reasonably to be used either by the controller or by any other person to identify that individual.

«Anonymised data” are therefore anonymous data that previously referred to an identifiable person, but where that identification is no longer possible” (Article 29 Working Party, Opinion 4/2007 on the concept of personal data, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf).

Pseudonymised data: “data relating to an identifiable individual, as the connection between the pseudonym and the identifying data (e.g. first and last names, address etc.) is available, either to the collecting organisation or to a third party. Even if the pseudonym and its correlation with the identity are exclusively known to one given party (whether the controller or a trusted third party) and are not shared with anyone, pseudonymised data remains personal data” (Press release, EDPS/2013/03, http://europa.eu/rapid/press-release_EDPS-13-3_en.htm).

Note: The concepts of reversible anonymisation and irreversible anonymisation are also used. Irreversible anonymisation is equivalent to anonymisation and reversible anonymisation is equivalent to pseudonymisation.

Irreversible anonymisation: The technique of deleting all identifying elements in a group of data. Practically speaking, this means deleting all direct or indirect identifying data. Re-identifying the person is therefore impossible. (CNIL, http://www.cnil.fr/fileadmin/documents/Guides_pratiques/Livrets/securite/files/assets/seo/page40.html).

Reversible anonymisation: The technique of replacing an identifier (or more generally personal data) with a pseudonym. This technique makes it possible to lift anonymity or study correlations if needed. (CNIL, http://www.cnil.fr/fileadmin/documents/Guides_pratiques/Livrets/securite/files/assets/seo/page40.html).

DPA: Data Protection Authority. In this document, the term is used to refer to a supervisory authority (in the sense of Directive 95/46/EC). DPAs are public authorities set up by Member States so as to ensure that provisions on personal data protection are implemented. To that purpose, DPAs are supposed to fulfil their functions independently.

DPAs in each country studied (national language / English)

Austria: Österreichische Datenschutzbehörde / **Austria**n Data Protection Authority
www.dsb.gv.at

Czech republic: Úřad pro ochranu osobních údajů / Office for Personal Data Protection
www.uoou.cz

Finland: Tietosuojavaltuutetun Toimisto / Office of the Data Protection Ombudsman
www.tietosuoja.fi

France: Commission Nationale de l’Informatique et des Libertés (CNIL) / National Commission on Information Technology and Freedom
www.cnil.fr

Germany: Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) / Federal Commissioner for Data Protection and Freedom of Information; Datenschutzbeauftragte der Länder / Data Protection Commissioners of the Federal States
www.bfdi.bund.de

Greece: Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα / Hellenic Data Protection Authority
www.dpa.gr/portal/page?_pageid=33,40911&_dad=portal&_schema=PORTAL

Hungary: Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) / Hungarian National Authority for Data Protection and Freedom of Information
www.naih.hu

Italy: Garante per la Protezione dei Dati Personali (GPDP) / Italian Data Protection Authority
www.garanteprivacy.it

Luxembourg: Commission nationale pour la protection des données (CNPD) / National Commission for data protection
+ Supervisory authority for police, customs, intelligence service, armed forces and justice filing systems (known as the "supervisory authority", Law of 2 August 2002, Art. 17(2)).
www.cnpd.public.lu/fr/index.html

Poland: Generalny Inspektor Ochrony Danych Osobowych (GIODO) / Inspector General for Personal Data Protection
www.giodo.gov.pl

Portugal: Comissão nacional de protecção de dados (CNPD) / National Data Protection Commission
www.cnpd.pt

Slovenia: Informacijske pooblaščenke / Information commissioner
www.ip-rs.si

Spain: Agencia Española de Protección de Datos (AGPD) / Spanish data protection office
www.agpd.es/portalwebAGPD/index-ides-idphp.php

United Kingdom: Information Commissioner's Office (ICO)
ico.org.uk/

JUSTICE

The European Criminal Records Information System (ECRIS[12]) was set up in 2012, pursuant to the decision of the Council of the European Union of 6 April 2009[13]. This system provides, through the electronic interconnection of criminal records databases in various Member States, direct access to information on the convictions of any EU national, regardless of the Member State that convicted him/her. Data is stored in national filing systems on the basis of the person's nationality. If a person is convicted in a country they are not a citizen of, their sentence is automatically communicated to authorities in their country of citizenship. Each Member State updates the records of its own nationals, no matter where in the EU the case was judged. Upon request, judicial authorities from another Member State may access criminal records.

In principle, this system is supposed to allow a court to take into account previous convictions (or absence of previous convictions) from authorities in the country in which the person is being judged and in other Member States. In practice, however, the system has other repercussions. Someone applying for a job might, for instance, be requested to supply a copy of his/her criminal record.

It should be mentioned that technical mistakes can arise as a result of data collection, storage or transmission. This could be caused by the electronic interconnection of decentralized filing systems on the national level, the use of reference tables for transmitting data in a standard European form, the codification of infringements, sentences and convictions, the automatic translation system used, etc.

Several issues must be raised, in particular:
- Infringements are not standardised from one country to another. Consequently, a person might be convicted in one Member State for an action but not be punishable in another.
- Criminal records systems vary from one country to another. There is no standardised approach to access by judicial and police authorities, by convicted persons themselves, by third parties, etc.

The first issue is differences in infringements from one country to another. This constitutes a threat for data subjects. Data gathered in one country's criminal records is not equivalent to data gathered in other countries' criminal records, even if this information appears to be of the same nature. There are many examples illustrating this problem (see below page 28): infringements are classified differently, infringements are described differently and data storage periods vary from one country to another.

The implementation of the ECRIS system in the EU has highlighted the importance of differences between national criminal records.

12. European Criminal Records Information System.
13. COUNCIL DECISION 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:093:0033:0048:EN:PDF

A. FREEDOMS AT RISK

Criminal records consist of data on someone's legal history. Disclosing this data without restrictions would be a violation of the following fundamental rights: the right to privacy, the right to personal data protection, the right to work, the right to the free choice of employment, the right to equality, the right not to be discriminated against, the right to social rehabilitation, etc.

In all the countries studied, criminal records are held for very similar purposes: to protect society, to prevent reoffending and to ensure that court decisions were properly executed.

Allowing an employer to view an applicant's criminal record enables them to check that a previous conviction does not present a risk as regards the job the data subject is applying for. This aims at preventing reoffending and protecting society. For instance, the head of a retirement home would check that the applicant never committed infringements against vulnerable adults.

Criminal records also ensure that court decisions are executed properly as viewing them makes it possible to check whether a person is prohibited from a professional activity (e.g. managing a commercial company after being convicted of misuse of company assets). Lastly, criminal records contribute to enforcing the law, as the judge can check if the person is a repeat offender (if so, the type or severity of the sentence changes).

While criminal records are held for very similar reasons from country to country, they operate quite differently. In some countries, for instance, criminal records include the names of the data subject's parents and/or spouse to prevent civil status errors (**Hungary**, **Austria**, **Luxembourg**, **Spain** and **France**). This could put these relatives at risk of discrimination.

Criminal records checked for employment purposes

In **France**, criminal records are divided into three bulletins. The data subject can easily get a copy of the third bulletin by ordering it for free from the Ministry of Justice. He/she is then free to give it to anyone who requests it (in practice, this is usually a future employer). This bulletin, named "bulletin n°3" or "criminal record extract" includes only the most serious offences (it is blank if there are no serious convictions). The content of bulletin n°3 is filtered so offenders are not prevented from reintegrating society. The data subject can even ask for some convictions to be deleted from the bulletin if they can provide sufficient guarantees they will not reoffend. It should be underlined that only the data subject can request this bulletin. All other people who wish to access this information, whether individuals or organisations, must request it directly from the data subject. Bulletin n°1 contains information on all convictions[14] and is only communicable to judicial authorities. Bulletin n°2 does not include less serious offences and is communicable to administrative and military authorities for specific purposes.

In **Luxembourg**, there is a similar system. However, since the Law of 29 March 2013 relative to criminal records and the exchange of information taken from criminal records between EU Member States[15], there are no longer three bulletins but two. The first contains information on all convictions and can be viewed by judicial authorities (like the bulletin n°1 in **France**). The second is filtered and can only be issued to the data subject (like bulletin n°3 in **France**). In both countries, it is easy, quick and free for the data subject to obtain a criminal record extract. The request can be made on the government's website.

14. Bulletin n°1 contains all convictions except commercial penalties or disciplinary penalties and convictions for which the data subject has received amnesty or judicial rehabilitation including deletion from the criminal record. Some convictions are deleted from the criminal record after a certain length of time (around 5 years).
www.vos-droits.justice.gouv.fr/casier-judiciaire-11942/casier-judiciaire-contenu-de-casier-20250.html
15. www.legilux.public.lu/leg/a/archives/2013/0085/a085.pdf#page=2

The fact that only the data subject can request a criminal record extract, and that they have the choice to communicate it to third parties, could be considered a guarantee strong enough to protect fundamental rights. However, it is not an absolute guarantee: even if the person is free to disclose their bulletin as they wish, it is obvious that refusing to provide it for a job interview would seem suspicious to the employer. Moreover, a data subject may find it difficult to refuse when they consider they are in a position of weakness (under financial pressure, etc.). Therefore, there is a risk the data subject may be discriminated against in the employment field. Despite this, neither **France** nor **Luxembourg** has implemented measures limiting third parties' rights to ask a data subject for a criminal record extract. Furthermore, in **Luxembourg**, the new law stipulates that the employer may request a data subject's criminal record not only for the purpose of recruitment but also to "manage staff" – that is to say at any time during the employment relationship.

There are therefore two risks associated with legislation and practices:

- The lack of measures restricting criminal record requests in the employment context.

This is the case in the **UK**: any employer may request "basic disclosure"[16] of the candidate's criminal record.

- The lack of any system classifying infringements by type and/or the employment sector concerned, even if the extract provided is filtered.

In **France**, only the most serious offences and custodial sentences are recorded in bulletin n°3, but this bulletin is always the same no matter who the recipient is. The same is true in **Luxembourg**, where this is all the more alarming given that bulletin n°2 is almost the same as bulletin n°1. Only suspended prison terms of 6 months or less are excluded from bulletin n°2 (while in **France**, bulletin n°3 only mentions: non-suspended prison sentences of two or more years, non-suspended prison sentences of less than two years the court has requested to be recorded in criminal records, ongoing disqualifications and incapacities, social and judicial supervision measures and prohibitions on practising professional or volunteer activities that involve ordinary contact with minors[17]). Similarly, in **Germany** and **Austria**, it should be underlined that the most "filtered" record always contains the same data, no matter why it is being issued.

In **Finland** and **Portugal**, however, there are some positive practices. In **Finland**, information contained in the criminal record issued is filtered depending on the recipient. This ensures interests are successfully balanced (taking into account security on the one hand, and privacy and professional integration on the other). Only employers offering jobs involving contact with children may request such files, and only infringements indicating the data subject's incompatibility for working with children are disclosed. In this way, third parties authorised to access data are filtered, as are the infringements and convictions the recipient is provided information on (infringements are not sorted by seriousness, but by type, taking into account the recipient's legitimate interest in the information, which is required to protect "contact" persons in the job concerned).

Portugal provides interesting guarantees. When a criminal record is requested for an employment background check, the extract provided only contains information on prohibitions to perform specific jobs or functions. In this way, the information on a data subject's legal history that is provided to "private" third parties is filtered in a way that reflects the purpose of their request.

Similarly, in **Poland**, only some employers are authorised (in theory) to access criminal records. In **Hungary**, criminal records are not issued directly: the data subject is issued with a certificate stating they have a clean criminal record. This document is legally required when applying for some types of jobs. However, employers are not prohibited from requesting such certificates for jobs that are not specifically covered by this provision. Consequently, in practice, this document is requested in cases where it is not legally required.

16. Extract of criminal records that records unspent convictions.
17. www.vosdroits.service-public.fr/particuliers/F14710.xhtml#N1018D

Some countries have also implemented measures to minimise the risk of the data in criminal records being disclosed by third parties who access it legally. In **Finland**, for instance, the employer must not keep any information on a data subject's legal history that is listed in the criminal record. They may only record whose criminal record they consulted and the date they consulted it[18].

Other good practices must also be mentioned. In **Germany**, suspended sentences of less than 2 years are not recorded if the person convicted was a drug addict. In **Spain**, suspended sentences are not recorded in criminal records, and rules for minors (which are more favourable) may apply to young people between 18 and 21, depending on their maturity. In **France**, sentences in bulletin n°1 are recorded the same way for minors and adults, but infringements in bulletins n°2 and 3 are not. This is in order to avoid jeopardizing their professional integration. In **Luxembourg**, infringements committed by minors are not listed in criminal records, but there is a "special register" of decisions by the youth court and juvenile judge. This register is updated by the criminal records officer (Law of 10 August 1992 on Youth Protection, Article 15).

In **Luxembourg**, there are two bulletins, but the filter applying to suspended sentences and sentences visible to third parties provides very little protection (almost all convictions are recorded in both bulletins). There is therefore an important risk that data subjects will be discriminated against during the recruitment process. This is especially true given that foreigners applying for the same job as **Luxembourg** citizens provide criminal records that are not comparable as regards data recorded (and there are many cross-border workers). This is despite the fact that the law reducing the number of bulletins to two was intended to provide citizens with better transparency and clarity[19]. It should be noted that the law sets a two-year storage period for employers keeping criminal records data.

It is also interesting to consider how the rules on criminal records are applied in practice: respect for legislative intent, potential abuses, etc.

In **Hungary**, though a certificate attesting a data subject has a clean criminal record must be provided when applying for some jobs, an increasing number of employers are requesting this certificate for jobs that are not listed by the law. This is also true in **Finland**, where employers sometimes try to access the legal histories of employees/future employees when they are not supposed to (for instance, when the job does not involve working with children). In the **UK**, all employers may request applicants to provide criminal record extracts (this is called "basic disclosure"). This extract contains information on all unspent convictions, given that rehabilitation periods depend on the nature and length of convictions[20]. The law also designates employers and other organisations that may directly obtain "standard disclosure" from the authority holding the file. "Standard disclosure" is information on all convictions, spent and unspent, including cautions. This concerns jobs that involve working with children or vulnerable adults, but also medical professions, military positions, etc. "Enhanced disclosure" also exists: the recipient obtains information of all convictions plus any other information considered relevant by the police or the government (arrests, third-party allegations, etc.). Enhanced disclosure may be legally requested for some jobs. Generally, it concerns jobs involving contact with children or vulnerable adults. Therefore, the employer may be informed that a data subject was arrested, was a suspect in a police investigation, or said to be violent by a neighbour. In essence, this means that, even if the person was never found guilty, they could be "socially convicted" because an employer accessed their full criminal record and freely interpreted police data.

18. Law on checking the criminal background of persons working with children (504/2002) and Law on the amendment of sections 6 and 7 of the criminal records act (505/2002)
http://www.tem.fi/files/36811/TEMesite_Lasten_kanssa_tyoskentelevien_rikostausta_EN.pdf
19. Bill n°6418 relating to the organization and content of the exchange of information extracted from the criminal record between Member States of the European Union
http://www.chd.lu/wps/PA_RoleEtendu/FTSByteServingServletImpl/?path=/export/exped/sexpdata/Mag/198/081/109870.pdf
20. Rehabilitation periods are between 6 months and 10 years, and imprisonment or detention that exceeds 30 months is never cleared.
www.justice.gov.uk/downloads/offenders/rehabilitation/rehabilitation-offenders.pdf

Storage period of convictions in criminal records

Storage periods for convictions in criminal records are often longer than the offence's limitation period. So the State agrees to prosecute offences within a specific period, but if a person is prosecuted and convicted for an offence within the time limit, the State records this conviction for periods that exceed the offence's limitation period. These storage periods could be considered additional risks to the right to oblivion.

Data storage periods are necessarily limited and determined by law. They take into account the right to oblivion but also the right to privacy. In most countries studied, there are legal storage periods for convictions data in criminal records. The countries studied had implemented similar periods:

- Regardless of the seriousness or type of infringement committed, the file or data is deleted when the person dies or reaches a certain age, between 90 and 100 (**France**, **Germany**, **Czech republic**, **Finland** and **Italy**).

- Shorter deletion periods apply depending on the seriousness of the infringement. In **France**, crimes against humanity are never removed from the file and all other infringements are removed after 40 years maximum (when they are automatically deleted). Less serious infringements are subject to shorter data storage periods. They are deleted after 3, 5 or 10 years, and automatically deleted when the prison term is less than 10 years. These periods run from the start of the sentence's enforcement period or the sentence's limitation date if it is not enforced. Limitation is after 3, 5 or 20 years, depending on whether it concerns a contravention (minor offence), délit (offence) or crime (crime). In **Germany**, data storage periods are between 6 and 21 years (shorter than storage periods in **France**), depending on the seriousness of the infringement, the type of sentence handed down and the nature of the infringement. In the **Czech republic**, infringements are stored in criminal records for between 1 and 15 years, depending on their seriousness. In **Portugal**, the storage period is 5 or 10 years after the sentence has been purged. In **Spain**, the storage period is 6 months for the least serious infringements and 5 years for the most serious infringements, on the condition that penal liabilities no longer exist and civil interests are satisfied. In **Hungary**, the period varies from 8 to 12 years for "intentional" infringements. This period is always reduced by 2 years when the infringement was not intentional. In **Austria**, storage periods are 7, 12 or 17 years depending on the seriousness of the sentence, but they can be doubled for sexual offences (sexual offences are never deleted if the offender is imprisoned for more than 5 years). Furthermore, if more than one conviction is recorded in a criminal record, the longest storage period applies to all convictions. In **Luxembourg**, storage periods vary from 5 to 20 years, depending on the seriousness of the conviction, starting from the date the sentence is purged (automatic redemption). In **Finland**, depending on the seriousness of the offence, the storage period is for 5, 10 or 20 years starting from the judgement date (which is much shorter than storage periods that run from the enforcement date, as is the case in most of the other countries studied). The storage period can be extended if the offender commits a second crime while a previous offence still appears on their criminal record.

Comparing data storage periods makes it possible to highlight excessively long periods in some countries. **France**'s 40-year storage period is double that of the maximum period usually applied in other countries. Any breach of the right to privacy, to professional integration and to the mobility of people within the EU must be justified. Given these different storage periods, which depend on many factors (type of sentence, sentence length, type of infringement, seriousness of the infringement, intention, suspended sentences, compensation paid to victims, etc.), questions should be asked as to what is really necessary, especially given that ECRIS makes all sorts of data exchanges possible. A similar approach should be adopted in all EU countries.

With respect to amnesties, it should be pointed out that some countries delete amnestied convictions from the criminal record (**France**[21]) while other states keep records of amnestied convictions (although records note that the data subject received an amnesty – **Luxembourg**[22] and the **Czech republic**).

B. TRANSPARENCY AND CONTROL BY DATA SUBJECT

Informing citizens

In most of the countries studied, there is little information provided on criminal records and the effect these records could have on the professional integration or discrimination of data subjects.

In the **UK**, the first link visible on the Home Office website is "Get a DBS (criminal record) check". Then, users can choose to click on the link "DBS eligibility guidance". This redirects them to a page listing most of the jobs for which a criminal record check is necessary. The guide explains the procedure and invites the reader to contact DBS if they have any doubts as to the legality of the request. The fact that the procedure is described and that citizens are alerted to risks of abuses is positive. However, it is disappointing that the person responsible for signalling these abuses is the data subject, who can only make such statements if they are fully aware of the dangers and not under financial or any other kind of pressure.

In **France**, there is no handbook to explain which jobs may require criminal record checks. Authorities updating criminal records can only give bulletin n°3 to the person concerned and not third parties. The data subject, once they have the bulletin, may give it to whomever they wish. They are given no information on the kinds of job or function that give rise to legitimate checks of bulletin n°3, since this is entirely at the employer's discretion. The French Ministry of Justice website provides an unsatisfactory response to this question[23]. However, the official website for the Information and Documentation Centre for Young People provides appropriate advice[24] .

It should be mentioned that in **Luxembourg**, **France** and **Germany** (among others), employers who access criminal records data, even if this is in filtered form, are largely unaware of legal data storage periods. It is disappointing that private sector employers are given very little or no information on how to ethically handle the criminal record of a job applicant or employee.

In **Finland**, the Ministry of Employment and the Economy provides detailed information on the employers' obligations to request and check criminal records. A 2013 handbook is even available in English[25].

21. www.vos-droits.justice.gouv.fr/casier-judiciaire-11942/casier-judiciaire-contenu-de-casier-20250.html
22. Article 2 of the Law of 29 March 2013 on the organization of criminal records and the exchange of criminal record information amongst member states of the European Union
23. www.faq.cjn.justice.gouv.fr/selfservice/template.do?id=47
"It is not forbidden for a private employer to request a job applicant to provide a copy of their bulletin n°3, but only the job applicant can obtain the document and decide whether or not to produce it given its contents."
24. www.jcomjeune.com/le-casier-judiciaire/le-casier-judiciaire-national-un-acces-difficile-a-certains-metiers
25. www.tem.fi/files/36811/TEMesite_Lasten_kanssa_tyoskentelevien_rikostausta_EN.pdf

Data subjects' right of access

Based on existing personal data protection rights in all countries concerned, data subjects have the right to be informed of existing filing systems and the personal data contained therein. However, although this right exists, most people are unfamiliar with the law. For instance, in countries where criminal record extracts (**Luxembourg**, **France**, etc.) or certificates stating data subjects have clean criminal records (**Hungary**) are delivered to the data subject, citizens may believe this filtered version is the only part of their criminal records they are allowed to view. In principle, they have the right to access all data saved in criminal records.

For instance, in **France**, the law strictly regulates the accessing of criminal records. Bulletin n°1, which contains all criminal record data, is viewable only by judicial authorities and prison administrations. Bulletin n° 2 can be obtained by administrative and military authorities (prefects, public administrations, military authorities, presidents of departmental councils, heads of public or private firms that work with minors, etc.) for specific reasons (job offers, awards, etc.). However, while only bulletin n°3 can be issued to the data subject, he/she can ask to check all data stored on the three bulletins that make up his/her criminal record[26]. Many citizens may not be aware of this right to view their entire criminal record. The right to check convictions saved in the various bulletins is important, because it allows data subjects to ensure that there are no errors and/or that legal rehabilitations have been taken into account. It also allows data subjects to note that convictions may appear on both bulletins 1 and 2 and request their deletion from bulletin 2[27].

One good practice exists in **Germany** and **France** that does not exist in the **Czech republic** and **Portugal**, for instance. A data subject's right to check his/her complete criminal record is restricted to "viewing" – no copies are supplied. This provision is very important and was implemented in order to protect the data subject from third-party pressure to obtain his/her data.

Controlling access to the filing system and its uses

In **Germany**, the Federal Office of Justice prepares a protocol for every piece of information transmitted to third parties. Each protocol lists the name of the person requesting the data, the provision allowing them to consult the data, the purpose of the consultation, which data consulted was, the name of the person at the Federal Office of Justice who gave access to the data, the date of consultation, etc. These protocols are saved for one year (or longer in exceptional circumstances). In **Austria**, a protocol is also prepared each time someone accesses data, and the content of the protocol is saved for three years. Lastly, in **Finland**, anyone can find out which third parties accessed their criminal record data over the previous year, as well as their reasons for consulting.

The guarantees created in various countries would lead to better security if implemented jointly. These include restricting who is authorized to access criminal records, recording the date of consultation, recording the type of data consulted, recording the name and position of the person, recording the reasons they consulted the data, etc.

In addition to regular internal checks, supervisory authorities (DPAs) must also carry out regular checks to ensure that access to data filing systems is lawful.

26. www.faq.cjn.justice.gouv.fr/selfservice/template.do?id=38 Article 777-2 Of the Criminal Procedure Code /www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=535DC5517A910480A2B3F3A34A6BEC5D.tpdjo14v_2?idArticle=LEGIARTI000006578332&cidTexte=LEGITEXT000006071154&dateTexte=20140204&categorieLien=id&oldAction=rechCodeArticle

27. Article 775-1 of the Criminal Procedure Code /www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=535DC5517A910480A2B3F3A34A6BEC5D.tpdjo14v_2?idArticle=LEGIARTI000025585884&cidTexte=LEGITEXT000006071154&dateTexte=20140204&categorieLien=id&oldAction=rechCodeArticle

C. APPEALS

There are substantial differences in the appeals process from country to country. European data protection rights state that cases can be brought before the DPA (Principle 6 of Recommendation R87 (15) of the Council of Europe's Committee of Ministers to Member States). The nature of the competent court determines the sentences that can be handed down.

In countries such as **France**, the **UK**, **Hungary** and **Austria**, appeals may include requests for remedies or financial compensation for the infringement. In **Austria**, if the Vienna Police Department refuses to communicate data stored in criminal records, an appeal can be brought before the administrative courts. In **France**, the case can also be brought before criminal courts, and sentences such as fines and imprisonments may be handed down.

One good practice must be mentioned for **Germany**. When a data subject has made a complaint as to the recording of data, the data is "blocked" while the complaint is being dealt with. In other words, the data is still stored in the file and its communication to third parties is still possible. However, people viewing the data are informed it may be stored illegally or incorrectly.

D. ROLE OF NATIONAL DATA PROTECTION AUTHORITIES

Data Protection Authorities have an important role as regards criminal records: when files are centralised, computerized and/or modified, DPAs have the power to publish opinions on new rules and make sure they conform to the right to personal data protection. For instance, the French DPA CNIL, in its opinion on the bill on criminal record centralisation, recommended that the right to access full criminal records was restricted to viewing the data.

National Data Protection Authorities also have the power to handle appeals regarding violations of the right to personal data protection; for instance, when the decision of the authority holding the file is deemed unsatisfactory (Principle 6.6 of Recommendation R87 (15) of the Committee of Ministers to Member States[28]). This appeal does not prejudice any appeal to a court. In **Germany**, an appeal can first be lodged with the authority holding the file (the Federal Office of Justice). If its decision is unsatisfactory, a lawsuit may be filed with the administrative courts.

Data Protection Authorities may carry out and report on checks by way of an annual report (in the case of the French DPA) or a report published every 2 years (in the case of the German DPA), which also sets out recommendations for improvements as regards personal data protection. As far as checks are concerned, DPAs generally have the power to impose sanctions if they observe violations, even if no complaint is filed beforehand. In **France**, for some sensitive state files such as criminal records, CNIL must inform the Prime Minister of any violations of rights or freedoms it has noted, so he/she can decide on appropriate measures to rectify the situation[29]. Meanwhile, in **Hungary**, the DPA made no comment on the law applying to criminal records. Furthermore, in practice, the Hungarian DPA only carries out checks on criminal records when complaints are filed. The Hungarian DPA's annual report contains no information on general or regular inspections of criminal record management. Nevertheless, it should be noted that the Hungarian DPA played an active role in drafting modifications to the law on recording minor offences by publishing several opinions.

28. www.privacycommission.be/sites/privacycommission/files/documents/recommendation_87_15.pdf
29. www.cnil.fr/linstitution/missions/sanctionner/

In **France**, the DPA has issued several opinions on criminal records since its creation. For example, CNIL has criticised the excessive length of time required to update and transfer information from courts to the central database. In **Luxembourg**, a specific supervisory authority independent of the National Commission for Data Protection (CNPD) oversees police and justice filing systems. The composition of this authority is problematic, as it is headed by the Chief Public Prosecutor or his/her delegate, whose duties include managing some of the filing systems they have to oversee.

Our recommendations to improve personal data protection in the justice field are as follows:

The law must specify all situations where someone's criminal records can be requested or accessed, even when the data subject can choose whether to provide their criminal record to a third party. Consent is not freely given when a data subject feels that refusing access to third parties such as an employer, bank or insurer would prejudice their own interests.

- The law should list the different kinds of third parties authorised to request a data subject's criminal record. It should also state which categories of convictions these third parties can view.
- The law should specify the conditions under which a data subject's criminal record can be consulted. Even if the extract supplied only contains information on the most serious convictions, a third party should not be allowed to note down information on these convictions.
- In addition to regular internal checks, DPAs must regularly check the legality of criminal record consultations.

To prevent any danger to society, an efficient system listing prohibited occupations (e.g. prohibitions on creating a company, working with children, etc. depending on the convictions) should be considered sufficient.

It must be possible to take both automatic rehabilitation and judicial rehabilitation into account:

- Automatic deletion: Data must be automatically deleted from criminal records after a period determined by law, provided that there is no repeat offending.
- Judicial rehabilitation: The data subject must be able to request rehabilitation reducing the automatic deletion period.

When data is deleted from criminal records, it must be deleted completely. In other words, it is insufficient to state next to the conviction itself that the conviction was rehabilitated. Such statements do not adequately prevent unfair discrimination.

The right to access a data subject's criminal record should include:

- The right to check whether access to the criminal record was granted in a lawful manner, including when access was granted to courts and public bodies-

The right to check whether out-dated entries have been deleted

This right implies that all consultations of a data subject's criminal record must be recorded.

When a data subject's data is being checked because he/she made a complaint, the inspected data shall be "blocked" during the verification period. This means that third parties accessing this data must be informed that it may be illegally or incorrectly stored.

Note:

The following examples show how ECRIS clearly creates risks of discrimination and inequalities:

- Abortion is viewed and regulated differently from country to country in the EU. In some countries, abortion is a right; in others, it is prohibited. However, there are also different periods during which abortion is allowed, and different reasons why a woman can get an abortion (emotional distress, no specific motive, etc.). In the countries where abortion is forbidden, exceptions to this rule can vary (risks to the child's life or health, risks to the mother's life, etc.).

Let us consider two women in the same situation: each has an undesired pregnancy followed by an abortion after the same amount of days. One of these women has her abortion recorded on her criminal record because it was unlawful in her country. The other has nothing recorded on her criminal record. These women then apply for the same job, in the same country, and have the same skills. If administrative authorities in the country check future employees' full criminal records, the employer will learn of one candidate's abortion and not the other's. Even if the employer is not supposed to discriminate on this basis, there is always the risk that the employer (even in the public sector) judges people with their own conscience. It should be borne in mind that the more personal data is disclosed, especially when they are not needed as regards the purpose, the higher the risk of discrimination.

The example above was for an abortion recorded on a person's criminal record that was checked as part of the recruitment process. However, let us consider a situation where both these women move to a third country where repeat abortions are punished with a criminal sentence. If they both had second abortions, one would be legally considered a reoffender and sentenced, and the other would not (because the country would have no record of her first abortion).

In addition, the range of different offences varies considerably from country to country.

- In **Hungary**, the foetus is considered a human being from conception. Let us consider a driver who involuntarily causes a car crash that leads a passenger in the other car to have a miscarriage. If this crash occurs in **Hungary**, it could be considered an involuntary homicide. In **France**, the child becomes a human being once born. Consequently, the accident would not be considered a homicide (however, the mother can claim physical and moral damages caused by the loss of the unborn child). If the crash occurred in **Hungary**, it would be recorded in the driver's criminal record. If the same accident occurred in **France**, it would not be recorded in the driver's criminal record. However, both these files can be consulted throughout the EU.

POLICE

A. FREEDOMS AT RISK

Filing systems are necessary tools to ensure police are able to effectively carry out different activities (ensuring citizen security, managing complaints, apprehending criminals and offenders, etc.). However, these filing systems must not impinge upon the rights to privacy and protection of personal data. The right to be presumed innocent must not be threatened.

Some of the police filing systems studied pose particularly serious threats for privacy and freedom.

1. Freedoms at risk because of the kind of data processing

Wanted persons website in **Greece**[30]: Information on wanted persons – their names, photographs, and the reason they are wanted (terrorism, paedophilia, etc.) – is published on a website[31]. Insofar as these persons are presumed innocent unless they are definitively proven guilty (in which case the database would concern escaped prisoners and persons convicted in absentia), the automated publication of this information on the Internet is a serious blow to the presumption of innocence.

- Central domicile declaration registers in **Austria** and **Germany**: Declarations of domicile are mandatory in these countries. These registers allow anyone to obtain another person's name and address for any reason. Address information is accurate given that all changes of address must be declared. Not declaring a change of address can lead to a fine of between €500 and €1000 in **Germany**. Any third party may request to access this data via the Internet, bypassing police services. The data subject may oppose the online disclosure of their address to third parties by posting a written statement to this effect. However, by default, the information can be accessed via the Internet and the data subject must take active steps if he/she wishes to prevent it being divulged. Moreover, the data subject cannot refuse written requests to police services for his/her address to be disclosed. In addition, if it is established that the request is for a legitimate reason[32], other data contained in this file can also be passed on (qualifications, gender, religion, nationality, marital status, etc.). There are many complaints concerning this filing system, but it is by and large accepted by the general public. A similar filing system was considered in the **United Kingdom**, but because of the mobilisation of British opponents, the plan was abandoned.

- The national register of individuals in **Luxembourg**: This register was created by the Law of 19 June 2013. Its three purposes are to identify individuals; to provide data on individuals to persons in charge of public filing systems, for the purposes of their legal or regulatory duties, or in anonymised form for statistical purposes; and to maintain a historical record of this data for administrative purposes or, after anonymisation, statistical purposes[33].

30. This filing system is controlled by a judicial authority (the prosecutor) but is for police purposes. That is why, in this comparative overview, it is included in the police field.
31. www.astynomia.gr/index.php?option=ozo_content&lang=%27..%27&perform=view&id=36029&Itemid=1237&lang=
32. www.gesetze-im-internet.de/mrrg/__21.html
33. Law of 19 June 2013 on identifying individuals, on the national register of individuals, on the identity card, on the joint register of individuals, Section 3 "The National Register", art. 4.

- Video surveillance at the Findel retention centre in **Luxembourg**: A retention centre is not a detention centre. Retention centres are where asylum seekers and undocumented persons are held while waiting for decisions on their cases (administrative rather than legal decisions – for example, decisions organising their return to another country). They are kept in retention centres so they do not escape authorities. Video surveillance is a major infringement of the privacy of people held in retention centres and others who visit the centre, including the car park (visitors or lawyers, for instance). It is not known how long these videos are kept and who has the power to delete them[34]. Images recorded in corridors must not extend to inside rooms, toilets, changing rooms, showers, etc., but this is the bare minimum in terms of the right to privacy.

- The STIC filing system (Recorded Offences Processing System) in **France** and the INPOL filing system (Informationssystem der Polizei[35]) in **Germany**: In both systems, people recording data may add notes on the data subject's physical or psychological characteristics. Consequently, **France**'s STIC filing system can contain personal data making it possible to directly or indirectly obtain information on the person's racial origins; political, philosophical and religious opinions; membership in a trade union and health or sexual life, if this data was relevant to circumstances surrounding the offence or was useful when describing the person for identification or search purposes[36]. This leads to the inclusion of the following details: "autistic", "transvestite", "homosexual" etc. Similarly, an individual's characteristics can be recorded in **Germany**'s INPOL filing system. The aim is to protect the police and the data subject: "armed", "violent", "drug user", etc. Nevertheless, several German DPAs have raised awareness of practices that do not respect the filing system's purposes. For example, depending on the context, the following details may not be relevant: "crazy" and "danger: infection risk". These details can lead to stigmatisation[37] .

The risk of discrimination may also affect the workplace. In **France**, the STIC filing system may be consulted for administrative purposes when recruiting, authorizing or approving staff in security-related professions[38] (for example, for supervisory staff, security guards or people wanting to work at airports)[39] in addition to criminal records (see the justice chapter). However, this filing system is still not up-to-date, despite CNIL's repeated observations to this effect (a person might be referred to as the perpetrator of a crime during an investigation and exonerated once judged, and a suspect may become a simple witness during a judicial investigation). The STIC filing system can also be consulted during naturalisation procedures.

- The anti-terrorism database in **Germany**: This database contains personal information on people who are members or supporters of terrorist organisations or organisations supporting terrorist organizations; people who have committed illegal or violent acts during international political or religious protests; people who support the use of such violence; and the contacts of these people. Depending on the persons concerned, data gathering is more or less intrusive. It can even include a specific person's religion, the places he/she has visited, telephone contacts and e-mails, the vehicles he/she has used, etc. However, there is no proof as to the effectiveness of this database. This is extremely serious given that the database makes it possible to transfer information gathered by secret services to police filing systems and vice versa, despite the fact that secret services have much wider and more opaque investigative powers than the police. Moreover, some of the records in this database concern persons who may be in contact with suspected terrorists or who may be members of associations suspected of supporting terrorist organizations. The database is therefore based on debatable risk criteria, which make the intricacy

34. ALOS-LDH contacted the Detention Centre, which claimed they could not provide this information to third parties, but that they follow the criteria established by the CNPD and that their video surveillance was authorised by the CNPD in 2011.
35. Police information system.
36. Decree n° 2001-583 July 5th 2001, Article 1, § 2.
37. Parliament of Berlin, printed matter 17/103 – Statement of the government of Berlin to the Data protection Commissioner of Berlin p55 f
38. Consultations of the STIC filing system for administrative enquiries may today concern more than 1 million jobs.
39. Law of 5 November 2001 dealing with daily security.

and opacity of rules even more open to criticism. In addition, the Federal Constitutional Court declared the database partially unconstitutional (see the appeals section below).

Finally, in its 24th Activity Report, the **German** federal DPA (the Federal Commissioner for Data Protection and Freedom of Information) reported the case of someone that had been registered as a contact person in the counter-terrorism database after their private-sector employer submitted a request to the Federal Intelligence Service to find out if they were in the database, which was not the case at the time[40]. According to the Commissioner, the Federal Intelligence Service should also have informed the data subject that their private-sector employer submitted the request.

- DNA databases: Every country studied has a DNA database used by the police. The target population, data collection conditions, data type and data uses are different from one country to another. There seems to be a trend extending the scope of DNA databases.

Of all the databases studied, the one that presented the most risks to human rights was that of the **UK**. Much data is saved for indefinite periods (primarily because the 2012 law on the protection of freedoms, which states how long data can be kept, cannot be enforced retroactively). The use of DNA data has been considered for the health sector. This is a blow to fundamental freedoms because files cannot be collected for one purpose and used for another without the agreement of the data subject or, in exceptional circumstances, without law changes[41]. Furthermore, there are press reports of unregulated counter-terrorism DNA databases[42]. Meanwhile, in **France**, the FNAEG (automated DNA database), which was initially only supposed to contain the DNA of sex offenders, has been extended over the years to include perpetrators of other infringements, such as thefts and threats to property. Consequently, many demonstrators have been forced to submit DNA samples on the grounds they damaged property.

In addition to primary data collection practices and data types, good and bad practices also represent risks for freedoms, in particular:

- Consenting to biological sampling
- Interconnection risks
- Data storage periods
- Biometric identification (for passports and other identity documents)

2. Freedoms at risk because of data processing conditions

Consenting to biological sampling

Biological sampling affects a person's right to physical integrity. The right to privacy as defined in the fundamental texts includes a person's physical integrity.

Regardless of whether collecting biological data is proportionate to the objectives pursued, bypassing a person's right to physical integrity first requires their consent. There are many different examples overriding this principle on security grounds and for the purposes of criminal trials. Some countries require consent for every biological sample, while others only request consent from a category of persons or depending on the seriousness of the offence the individual is suspected of. Other countries are not concerned about obtaining the individual's consent.

40. 24th Activity Report of the Federal Commissioner for Data Protection and Freedom of Information (BfDI) covering the years 2011 and 2012, page 118 www.bfdi.bund.de/SharedDocs/Publikationen/EN/AnnualReport/2011-2012.pdf?__blob=publicationFile
41. Principle in Article 5 of Convention 108, also referred to in the S and Marper v. UK ECtHR case of 4 December 2008. www.hudoc.echr.coe.int/sites/fra/pages/search.aspx?i=001-90052#{«itemid»:[«001-90052»]}
42.www.independent.co.uk/news/uk/home-news/police-told-to-explain-use-of-unregulated-dna-database-8651380.html

- **Portugal** has a unique DNA database (Base de dados de perfis de ADN para fins de identificação civil e criminal) that aims to make the identification of criminals and civilians easier. In other words, it not only seeks to identify people for police purposes, it also seeks to identify civilians or dead bodies (the DNA of the data subject/dead body is compared with DNA data stored in the central file). Nevertheless, the idea of recording the entire population's biological information met with sharp criticisms. Consequently, any citizen's biological data that is used for civilian purposes is collected and stored on a voluntary basis. Their consent is therefore required. However, it should be noted that data kept with the person's consent is kept forever, (unless this person decides to revoke their consent). The fact that the person must take active steps to revoke the indefinite storage of their data is reprehensible. In addition, data subjects whose data is collected for non-civilian purposes have no right to object .

- In the **United Kingdom** so-called "non-intimate" biological samples (for example, saliva samples) can be collected from anyone kept in custody for an offence registered by the police, without the person's consent or authorization. In this situation, the data subject may only be a suspect, and therefore innocent until proven guilty. By 2012, data on nearly 7 million people, that is to say more than 10% of the British population, had been recorded in the DNA database. According to the press, 77% of young black men aged between 15 and 34 living in England and Wales appear in this database[43].

- In **France**, the person must give their consent before providing a biological sample that is recorded in FNAEG (the Automated DNA Database). However, if the person refuses the police officer's request for a sample, he/she is punishable by one year's imprisonment and a €15,000 fine. This penalty is doubled for people who are convicted of crimes. According to the Penal Procedure Code (Article 706-56), when a person is convicted of a crime or an offence punishable by ten years' imprisonment, the sample can be taken without the person's consent if the Public Prosecutor submits a written request to this effect.

- In **Luxembourg**, prior consent is compulsory except if the offence is considered serious (as in **France**). Nevertheless, the threshold considered "serious" is well below that which applies in **France**. When a person is suspected of an offence punishable by two years' imprisonment, a biological sample can be obtained through physical coercion. This is despite the fact that the **Luxembourg** DPA expressed an unfavourable opinion on this threshold, noting that it was too low compared with the ten years' imprisonment threshold in **France**.

- In **Germany**, except in cases of immediate danger, sampling must be approved by a judge. Since 2005, however, the suspect's prior written consent is sufficient to obtain a biological sample. This provision has been criticised because of the pressure police can put on suspects during custody and the imprecise criteria concerning the seriousness of the crime or offence.

In these countries, consent is far from being free and informed.

43. www.telegraph.co.uk/news/uknews/1533295/Three-in-four-young-black-men-on-the-DNA-database.html

Interconnection risks

In **Hungary**, a new law makes it possible to record the ethnicity of any person taking part in public interest work programmes. The rules governing this database must be closely supervised so as to avoid interconnections with police filing systems. Moreover, the RoboCop record system contains much obsolete data, because of excessively long storage periods. This is all the more dangerous given that information in the RoboCop system is transferred to criminal record systems, which are likely to interconnect at the European level through the ECRIS exchange system (see the justice section). A person could be arrested at the Schengen border because of obsolete data in the RoboCop record system.

Another problem resulting from interconnections is the transmission of errors from file to file at the national, European and even international levels. The STIC filing system in **France**, for instance, contains 80% errors (caused by reversing the names of victims and perpetrators of offences, for example). Furthermore, data in this filing system, which is used to register offences, will be used in the new "Processing of Prior Judicial Records" (TAJ) database, which combines STIC and JUDEX, its equivalent for the gendarmerie (constabulary).

Errors can also be transferred to the European level. The French filing system FNAEG is one example. This filing system originally recorded sex offenders' DNA profiles, but was extended to cover all sorts of crimes and offences, such as threats of damage to persons, drug trafficking, offences against individuals' freedoms, exploitation of begging, endangerment of minors, theft, extortion, fraud, destruction, damage, damage to property, etc. In the FNAEG database, 80% of data deals with non-convicted persons who are presumed innocent. This is mostly because policemen overuse the term "suspect: reliable and consistent evidence." This allows them to record the DNA profiles of people in custody and not just use this data for simple comparisons (before destroying it). This data is kept for 25 to 40 years. Under the Prüm Convention, this data filing system can be subject to transmission requests from authorities in the 27 other European countries. It can also be consulted by Interpol. In 2012, according to the French DPA (CNIL), FNAEG contained the DNA profiles of more than 2 million individuals (1,640,000 defendants and 400,000 convicted persons).

Lastly, some interconnections may not have a legal grounding. The security of filing systems must be ensured. To limit the risks of illegal access to data, people handling such data must be alerted to this problem. In **Portugal**, the authority responsible for the database (the National Institute of Forensic Medicine) has developed a procedural manual on databases' technical operating rules to guarantee quality, security and confidentiality. In **Spain**, a set of rules[44] applying to all filing systems establishes classification criteria for necessary security levels (basic/medium/high) according to the filing system's content and use. This set of rules establishes the measures applicable depending on the security level concerned.

Data storage periods

In **Hungary**, the personal data of people suspected of committing serious crimes, as well as the data of their contacts (who are presumed innocent in both cases) are kept for 20 years in the RoboCop record system.

In **France**, defendants' DNA profiles can be kept for 25 years in the FNAEG filing system, and 40 years if the person is definitively convicted. Data in the automated fingerprint database (FAED) can be kept for 25 years (see the appeals section).

44. Real Decreto 1720/2007 de 21 de Diciembre por el que se aprueba Reglamento de desarrollo de la Ley Organica 15/ 1999, de 13 de Diciembre, de Proteccion de datos de caracter personal

In **Luxembourg**, a person's DNA profile is not kept if he/she is cleared of suspicion.

In the **United Kingdom**, DNA data was kept indefinitely under the 1984 Police and Criminal Evidence Act (PACE). Under the new Protection of Freedoms Act 2012, data is stored between 2 and 5 years. As this law is not retroactive, all data gathered before 2012 will be kept indefinitely.

While the law does state that data in some filing systems cannot be kept for longer than the offence's limitation period, this is not always the case. In **France**, data can be kept 40 years. In the **United Kingdom**, for persons on record before 2012, there is no time limit. This is a violation of the right to oblivion.

Biometric identification

On the European level, the Schengen information systems (SIS and SIS 2) contain biometric data identifying missing or wanted persons (suspected of having committed an offence and/or convicted of crimes). The Visa Information System (VIS) compares biometric data through fingerprints. EURODAC, which is used to process asylum applications, also records fingerprints. Data processing aims to detect multiple visa or asylum applications by one person as well as identity fraud. In this context, the collection and storage of individuals' fingerprints once their file is closed deserves special attention. Saving all ten fingerprints could be considered excessive.

The TES (secure electronic documents) database in **France** manages procedures related to the issuing, renewal and delivery of passports. Interconnections are possible between TES and the national version of the SIS II wanted persons database. TES contains scanned images of faces and fingerprints, as well as other information. The number of fingerprints collected and stored has given rise to considerable discussion in recent years. Following the Decree of 30 April 2008[45], it was decided that eight fingerprints would be collected and stored in the TES database when a French citizen applied for a passport, even though the passport's electronic data component only included two fingerprints. The Council of State cancelled Article 5 of this Decree in a decision dated 25 October 2011, because collecting and storing more prints than those recorded in the passport's data chip was considered excessive "for the purposes of the data processing"[46]. In 2012, the French Constitutional Court censured the provisions of a law that would have made it possible to group biometric data contained in French citizens' passports and identity cards in the TES database[47]. The law would also have allowed the police to consult biometric data in order to identify suspects in judicial inquiries. The Constitutional Court considered that privacy risks outweighed the benefits put forward. Prior to this decision, an excessive number of fingerprints were collected over a period of several years. Comparisons with other European countries indicate the practice was not strictly necessary to attain the stated goal (increasing the security of identity documents). Indeed, in **Germany**, only two fingerprints are collected for biometric passport applications. These fingerprints are collected for the sole purpose of being recorded in the passport's data chip. In other words, fingerprint data is only kept in a national filing system for the time it takes to deliver the passport to its rightful holder. After this point, fingerprint data is only recorded in the passport, which is held exclusively by the data subject.

On 17 October 2013, the European Court of Justice delivered a judgment[48] that deserves to be mentioned. A German citizen considered that recording his fingerprints on his passport's data chip was a breach of his privacy. The Court acknowledged that collecting and storing fingerprint data in the pass-

45. Décret n° 2008-426 du 30 avril 2008 modifiant le décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports électroniques. http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000018743961
46. www.conseil-etat.fr/fr/communiques-de-presse/passeport-biom.html
47. Décision n° 2012-652 DC du 22 mars 2012, Loi relative à la protection de l'identité
www.conseil-constitutionnel.fr/decision/2012/2012-652-dc/decision-n-2012-652-dc-du-22-mars-2012.105165.html
www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/2012652DCccc_652dc.pdf
48. ECJ Judgment of 17 October 2013, Case C-291/12, Schwarz v. Stadt Bochum

port was indeed an infringement of these rights, but considered this infringement was justified to prevent the fraudulent use of passports. The Court stated that there were sufficient guarantees ensuring fingerprint data was not used for other purposes than those officially justifying its collection ("verifying the authenticity of a passport and the identity of its holder", and "preventing illegal entry into the EU"). The Court mentioned that one of these guarantees was the fact that the prints were only recorded in the passport's data chip, "which belongs to the holder alone". This guarantee does not apply to the French TES database, because two fingerprints are kept in a centralized database. This is despite the fact that the purposes of the data collection are the same in **France** and **Germany**.

In **Spain**, the National Identity Card is electronic (DNIE: Documento Nacional de Identidad electrónico) and is managed by ADDNIFIL. The chip contains the index fingerprints of both hands. In **Spain**, the identity card is compulsory from the age of fourteen and has many purposes: not only is it used for border controls, it also provides access to private services. In particular, it is required before making a credit card payment. However, the fact that this filing system exists is widely accepted.

B. TRANSPARENCY AND CONTROL BY DATA SUBJECT

People must be aware of these filing systems, the rules that govern them and the data collected. There are many factors that can be considered to lead to better awareness. One example is laws or regulations creating and describing filing systems (purposes, content, origin of data, recipients, storage period, exercising of rights, etc.). This information must be provided to data subjects when data is collected.

The right to access to one's personal data

In all the countries studied, the right to access personal data recorded in a filing system exists. However, some legal exceptions or restrictions are not defined clearly enough to allow data subjects to access their information in practice. In **Hungary**, for instance, people can ask to access personal data collected in the RoboCop filing system. However, the police can refuse access on the grounds of "ongoing criminal investigations". This exception means that competent authorities can refuse access to data whenever inquiries, proceedings, investigations, etc. have been opened. The authorities are not required to indicate when the data subject or their lawyer can access this data. Moreover, the nature of some databases and confidentiality rules are obstacles to this principle. This is the case for **Germany**'s anti terrorism database. In its 2011-2012 annual report[49], the German DPA (BfDI[50]) revealed it had discovered that data was being illegally gathered on people cleared of suspicion. They deplored the fact that they could not really act or provide specifics on these errors because of confidentiality clauses. Obviously, the data subjects concerned cannot assert their right to access and correct data, even through the DPA. In April 2013, the Constitutional Court also reported this lack of transparency and called for the DPA to be given effective powers of control[51].

In **France**, the right to access police filing systems is qualified as "indirect". The data subject must send a request to CNIL to find out whether he/she appears in a police filing system. A CNIL representative (a magistrate) then contacts the person in charge of the filing system to check whether there is any information on the data subject and its accuracy. The representative also asks for data to be corrected if necessary and provides the data subject with information on the results of this investigation. Nevertheless, CNIL must obtain the agreement of the filing system manager. In 2012, CNIL received more than

49. www.bfdi.bund.de/SharedDocs/Publikationen/EN/AnnualReport/2011-2012.pdf?__blob=publicationFile
50. Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
51. www.bverfg.de/entscheidungen/rs20130424_1bvr121507.html

3,600 requests for indirect access (a 75% increase compared with 2011). Half of the checks carried out were made on STIC and JUDEX files[52]. The large number of requests, their complexity and the many checks required (the managing service must collect all required documents) explain the length of time it takes to deal with requests. This is especially true for filing systems such as STIC (which may lead to an investigation lasting several years). This can prejudice people whose data is erroneous when they apply for certain jobs.

For individuals, the rights to access, correct, and/or delete personal data contained in a file must not be overly difficult to implement. For **Spain**'s INTPOL filing system, which lists previous offences, a form is made available to Internet users on the Department of Internal Affairs web site, to make exercising these rights easier. In **France**, CNIL publishes model letters on its website for those who wish to access their personal data. These templates include a letter specifically requesting indirect access to STIC and JUDEX police files[53].

Textual inaccuracies and changes to the purposes of filing systems

Generally speaking, the stated purposes of police filing systems lack accuracy, which can lead to misuse. For example, in **Germany**, anyone suspected of a "sufficiently serious" or sexual offence may have their DNA collected and stored in the criminal police's DNA database. But a "sufficiently serious" offence is no longer defined, because the list of offences referred to was cancelled in 2005. Consequently, a wide range of offences now give rise to DNA data profiling, in particular offences such as theft, drug offences, damage to property, and even defamation. In **Austria**, this concerns people suspected of "dangerous aggressions". The **Austria**n Constitutional Court has determined that the phrase "dangerous aggression" is too broad and the law must be amended accordingly by 2014.

In **France**, the FNAEG filing system initially aimed at centralising sexual offenders' DNA profiles only. Six successive laws have since widened the range of offences covered: theft, defacement, deterioration, damage to property[54], etc[55]. A data subject is required to provide a DNA sample after merely being suspected of one of these offences (no conviction is required). FNAEG's wider scope is still being contested (by citizens, NGOs, members of parliament, etc.).

The law should specify what data must be collected, under which conditions and, if data is saved, when it will be deleted or destroyed. When an individual agrees to provide a DNA sample, he/she should be informed of what will be done with it. The individual must be told if the biological sample will be kept or destroyed after DNA sequencing, analysing and recording (and if so, for how long). Individuals must also be aware of their rights. Security measures are no longer suitable. This should lead to requests for more protective security measures. For instance, once the DNA required for identifying suspects has been sequenced, keeping biological samples is useless.

Moreover, DNA fragments were originally chosen because they were "non-coding". In other words, they were thought to contain no medical or other information than that necessary to identify individuals (sex, filiation, etc.). However, advances in genetic research have found that DNA fragments do in fact carry information about geographical origin and possible illnesses[56]. In **France**, **Spain**, and **Germany** in particular, these supposedly "non-coding" DNA sequences are kept. This situation is an example of how protective measures can lose effectiveness.

52. Rapport d'activité 2012 de la CNIL, page 49
www.cnil.fr/fileadmin/documents/La_CNIL/publications/CNIL_RA2012_web.pdf
53. Guide Droit d'accès de la CNIL, page 21
www.cnil.fr/fileadmin/documents/Guides_pratiques/Livrets/droit_d-acces/files/assets/downloads/publication.pdf
54. This incrimination makes it possible to repress numerous demonstrators.
55. Article 706-55 du Code de procédure pénale http://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006071154&idArticle=LEGIARTI000006577732&dateTexte=&categorieLien=cid
56. www.bastamag.net/Fichage-ADN-tout-ce-que-la-police

Finally, rules must be transparent enough to allow citizens to check they are respected in practice. In **Hungary**, for example, the law appears to respect the principles of data protection. However, data protection practices – in particular, the way the RoboCop records system is used – are considered abusive.

C. APPEALS

1. DNA databases

In most of the countries studied, data subjects can file appeals requesting modifications or deletions when they have been refused access to data, or if their right to privacy has been breached. In **Italy** and **Austria**, appeals are lodged with the DPA. In the **United Kingdom**, it is impossible to appeal if a request for deletion has been refused[57]. This is deplorable, especially given that data deletion is at the discretion of the Chief Police Officer. However, following judgments by the European Court of Human Rights (especially S and Marper v. **UK** dated 4 December 2008) and claims by NGOs, the Protection of Freedoms Act 2012 reformed the DNA database by introducing several measures including limited data storage periods.

2. Other filing systems

Greece's wanted person filing system is a good example of how serious abuses can be. In 2012, the Police published photos of 29 HIV-positive prostitutes on the Astynomia website[58] for public health reasons[59]. This is a major blow to privacy, which is clearly out of proportion to any possible benefits. More suitable measures would have been providing information on places these women worked or a campaign to increase awareness of HIV protection and testing. Many NGOs launched campaigns following this publication and appeals were lodged with several institutions, including the European Commission and European Parliament. Fortunately, these photos are no longer on the site today.

Appeals lodged by vigilant associations have made it possible to denounce many rights violations (generally justified for security purposes) and correct legislation accordingly. In **France**, Decree 2008-426 of 30 April 2008 originally stipulated that eight fingerprints would be collected from biometric passport applicants and stored in the TES database. Many associations – including the French Human Rights League – requested this Decree be cancelled for abuse of power. Following the Council of State's decision of 26 November 2011, the eight fingerprints were reduced to two. A further decision by the Constitutional Council on 22 March 2012 censored the text permitting the use of the TES database for inquiries by the judicial police (see the biometric information section).

57. However, once the statutory deletion period is over, there is the possibility to appeal
58. www.astynomia.gr/index.php?option=ozo_content&lang=%27..%27&perform=view&id=36029&Itemid=1237&lang=
59. www.huffingtonpost.com/2012/05/03/greece-prostitutes-hiv-arrests_n_1473864.html

Decisions on appeals to the European Court of Human Rights (ECHR) also help restore rights. In the case of M K v. **France**, the ECHR published a decision on 18 April 2013 stating that storing the fingerprints of a person who had never been convicted in the Automated Fingerprint Filing system (FAED) was a disproportionate blow to his/her privacy as guaranteed by Article 8 of the European Convention on Human Rights. The Court referred to its own judgment of 4 December 2008 (in S and Marper v. **United Kingdom**), which established that storing the data of non-convicted persons for an unlimited period of time was a violation of privacy.

Lastly, it should be noted that the Federal Constitutional Court declared the German counter-terrorism database partially unconstitutional on 24 March 2013. The Court ruled that recording the personal data of members of organizations that carry out terrorist activities in this database is disproportionate if the members concerned are unaware of these activities. It also ruled that it was disproportionate to record the data of persons who merely advocate violence without taking any action. Finally, it considered the provision on "contact persons" was not precisely enough worded and was therefore a disproportionate measure.

D. THE ROLE OF DATA PROTECTION AUTHORITY

Data Protection Authorities contribute to draft laws and/or regulations on implementing police filing systems by submitting non-binding opinions. National DPAs also generally hear appeals in cases of suspected privacy violations and/or when access to data is refused. For example, for DNA databases in **Austria** and **Italy**, appeals against refusals to delete data are referred to the DPA. However, in **Greece**, no case has ever been brought before the Greek DPA (HDPA) because the DPA has no legal authority to check DNA data processing. This is despite the fact that, pursuant to the personal data protection law, the DPA should have jurisdiction to hear appeals on DNA databases.

In principle, lodging a complaint with a DPA does not exclude any other judicial remedy, according to EU personal data protection rights as transposed in national law. For the INPOL filing system in **Germany**, all individuals have the right to be informed of the collection and storage of their personal data, the reason this filing took place, the origins of the data and its destination. If this information is not forthcoming, the individual can lodge a complaint with the German Federal Commissioner for personal data protection, but an action before the courts is also possible.

In addition to acting on behalf of individuals, DPAs can and should regularly conduct audits and publish reports. The Greek DPA, for example, publishes many recommendations on the country's DNA database. The French DPA (CNIL) checked that unnecessary fingerprint data really had been deleted from the TES database (although apparently CNIL did not object to the fact that authorities responsible for issuing identity documents still collect eight fingerprints, despite only processing two of them). CNIL also carried out checks on STIC data in 2007-2008 and, in a report published in 2009, criticised the fact that 80% of records contained errors (caused by confusing victims/perpetrators, amendments to facts not being recorded, etc.). A further check carried out at the end of 2012 led CNIL to conclude that the same mistakes were present as in 2009. To remedy this, CNIL has submitted ten proposals to the Interior and Justice ministries, including a recommendation to make it a priority to update "the most sensitive records" such as those dealing with minors; and a request to public prosecutors to inform the Ministry of the Interior of measures clearing people who were initially suspected of crimes, as this update may lead to the deletion of the file.

In **Germany**, the Federal Commissioner for Data Protection (BfDI) has issued a complaint with regard to the difficulty of carrying out checks on the anti terrorism database. These difficulties arise from the database's technical complexity (there are confidentiality clauses, as well as a large number of authorities involved), but also because the DPA does not have jurisdiction to carry out checks on databases at the Länder (federal state) level, where federal DPAs have jurisdiction.

Our recommendations to improve personal data protection in the police field are as follows:

Data subjects must be informed when their data is collected and stored in police filing systems. This is necessary given the complexity of police filing systems, the widening scope of police data collection and the extensive use of police data.

Any exceptions to this rule must be strictly monitored and justified on a case-by-case basis (for example, during an investigation, a suspect's identity may need to be kept secret, this should be limited to the investigation period).

Data subjects must be guaranteed access to their personal data and this right should not be too difficult for the data subject to enforce. The fact that personal data is often collected without consent must not prejudice the right to access, modify and delete data.

Data subjects must have the right to lodge a complaint with both the data protection authority and judicial authorities. This right must be effective.

It must always be possible to appeal to judicial authorities, no matter where the first complaint was lodged (supervisory authority, controller or judicial authorities).

For data subjects, providing fingerprints for identity documents does not have the same repercussions as providing fingerprints for police investigations. The conditions for collecting fingerprint data must be different in each case: the records should not appear in the same filing systems, and the storage period must be different. These filing systems must not be interconnected.

Data shall be divided into sections so that each person viewing the police file only has access to the data he/she is allowed to consult in order to comply with the principles of proportionality and purpose.

The DNA data of demonstrators and political activists must not be collected and stored in the same way as the DNA data of criminals.

DPAs must be able to verify the characteristics of police filing systems before they are created, carry out regular checks on practices and operational rules, in particular with respect to updates and security of access.

HEALTH

A. FREEDOMS AT RISK

In most of the countries studied, health filing systems aim to ensure the efficiency of public health care services through improved cooperation between health practitioners and to follow-up on patients and insured parties, especially with respect to social security payments. However, in the **Czech republic**, the aim of health filing systems is to improve knowledge of the country's general health situation, and not any personalised health follow-up. In **France**, there is a kind of disassociation between, on the one hand, repayments and medical practices and, on the other hand, the medical file.

Those objectives are understandable but they must not give rise to violations of fundamental rights and freedoms, such as the right to privacy and the right to not be discriminated against. Medical secrecy really must be guaranteed because, since Hippocrates, it has been a means of ensuring the patient can talk freely to doctors and be correctly diagnosed. Indeed, personal health data is considered sensitive (Article 6 of Convention 108 and Article 8 of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data). The principle of enhanced protection for sensitive data means that their processing is forbidden except in exceptional circumstances. For instance, special categories of data may be processed when the data subject has given his/her explicit consent, or when the law creating the exemptions is subject to suitable safeguards and is of substantial public interest[60]. This principle is also guaranteed by Article 8 of the European Convention on Human Rights .

Citizens and their representatives must be aware of the possible risks and benefits of these filing systems. They must also be aware of the difference between law and practice, and adopt a critical approach towards communication campaigns promoting these databases. For instance, the slogan for the Dossier Médical Personnel (personal medical file or DMP) in **France** is: "DMP, the more they know, the better you feel"[62]. This totally ignores privacy risks.

In the **UK**, journalists[63] revealed that the National Health Service (NHS) had convinced people to sign up to the Summary Care Record (SCR) by claiming that those refusing it ran the risk of receiving wrong diagnoses or inappropriate drugs. The NHS also tried to convince people to remain in the database by claiming they could suffer delays in their medical treatment, or lack opportunities to obtain the most appropriate treatment.

The existence of medical filing systems, the more or less accurate laws they are governed by, and the potential abuses they may lead to, may pose risks for freedoms, especially the right to not disclose personal health data in given situations (the right to medical secrecy). These risks are all the more important given that data can accumulate over the years and become sought after information (for the health information industry, insurance companies, etc.). This is despite the fact that data is defined more or less loosely depending on the country (even outside the medical field), and that filing systems are subject to varying degrees of protection.

60. Article 8 of Directive 95/46/EC
61. Article 8 of the European Convention on Human Rights
"Right to respect for private and family life
1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.
62. "DMP, plus on en sait, mieux on se porte" www.dmp.gouv.fr
63. Daily Mail, May 2010

- In **France**, DMPs contain general medical data, data on care, medical imagery and data on prevention (antecedents, allergies, drugs prescribed and delivered, etc.). The HOPSY filing system, which lists persons hospitalised for mental health reasons without their consent, may contain, among other things, justice information (the facts that led to the person being hospitalised without their consent and the judge's actions).

- In **Hungary**, health care data includes information on the person's physical, psychological and mental state and any addictions. Medical documentation may also include any other data that comes to the healthcare provider's notice, irrespective of form or medium.

- In **Austria**, compulsory data stored in the ELGA system includes the insured party's income (the insured party does not pay healthcare expenses exceeding 2% of their annual income). Optional data includes medication prescribed by doctors and medication supplied by pharmacists.

- In the **UK**, the SCR contains information on prescription medication, allergies and any previous reactions to medication.

In addition to "medical" data, each filing system contains identifying data, which poses different kinds of privacy risks. Some filing systems contain professional information, in addition to the data subject's surname, first names, date of birth and address (for example, the HOPSY filing system in **France**). Most of this information is collected under a social security number, which is often used when processing other data. Health filing systems that work with an electronic card belonging to the patient/insured party may contain data useful to first aid services (blood group, allergies, diseases such as HIV, hepatitis B, hepatitis C, etc.).

In **Spain**, there is an ad hoc filing system for people who have been diagnosed with HIV in national health centres. This filing system is called SINIVIH, and is managed by the National Centre for Epidemiology. On the national level, this filing system is anonymous but the initials of the HIV-positive person are still linked to health data. On the local level, the SINIVIH database for each autonomous community records the person's first and last name. Appeals to stop the creation of this filing system failed. The Supreme Court ruled in 2007 that the filing system respected the law[64].

B. TRANSPARENCY AND CONTROL BY DATA SUBJECT

Objectives and purposes of the filing systems

In **France**, the DMP aims to ensure better coordination between health practitioners, better follow-up of care and more efficient monitoring of social security expenditure[65]. These same objectives are targeted in other countries, including **Austria** and **Italy**. In **Austria**, the ELGA system aims to improve the quality of medical treatment by making data available and transparent. It also aims to reinforce the patient's rights and create health care savings. In **Italy**, the Fascicolo sanitario elettronico (electronic health filing system or FSE) aims to make it easier to diagnose patients, prevent illnesses, monitor health expenditure and carry out scientific research. In the **UK**, the aim of the SCR filing system is to improve medical follow-up by making patients' data available no matter where the patient goes for treatment. In **Hungary**, data gathered in health filing systems may be used for statistical purposes and scientific research, in order to improve the country's general health situation. Personal medical data is also used for crime prevention, solving police investigations, aptitude tests, training programmes, etc. In the **Czech**

64. Decision of the supreme Court of July 9th, 2007, on the SINIVIH filing system
65. www.legifrance.gouv.fr/affichTexte.do;jsessionid=E15AF53AF9F2E13C72613CFAC3BA6ECC.tpdjo07v_2?cidTexte=JORFTEXT000000625158&categorieLien=id

republic, the purpose of the National Health Register is not to provide personalized follow-up to patients but to study the causes and consequences of some diseases, to collate statistics and to develop a public health policy that meets the population's needs. In this situation, there is absolutely no reason for storing nominative data. Although this data can only be transmitted once it is anonymous, health practitioners can access data they entered into the database and Ministry of Health employees may unlawfully disclose data. NGOs are currently battling this system.

In **Finland**, the public health register[66] has the same aims but identifying data is saved and can be used during epidemics. The Finnish system has not been challenged because security measures appear sufficiently robust (access is limited to persons working on the data, there are different levels of access, employees given access to the filing system receive training, checks are carried out, etc.). However, data subjects cannot access, modify or delete their data. Nevertheless, if the data controller[67] suspects there is a mistake, it can communicate the data to the person concerned in order to modify it if necessary. These mistakes do not affect privacy since the data is not supposed to make it possible to make conclusions about individuals. Technically speaking, mistakes would only impact statistics and the results of scientific research.

In **Greece**, the filing system's main aim is to better manage the national social security system. In **Poland**, the medical information filing system System Informacji Medyczne (SIM) aims to cut the costs of public health services by modernising the system.

In **France** and **Greece**, doctors have expressed their concerns and even opposition to such filing systems because they fear abuses with respect to the access to and use of sensitive data. This opposition raises the question of whether the filing systems are actually efficient when it comes to improving healthcare.

Consent to data collection/transmission

In **Finland**, the Prescription Centre filing system gathers prescription and consultation records in electronic format so they can be consulted by chemists. Patients can prevent their prescription from being recorded by asking for a paper version that is given to them directly or sent by phone or fax. However, plans are underway to modify the law in 2014 with the effect that paper prescriptions will no longer be issued. Data subjects may no longer be able to oppose data collection by the Prescription Centre.

In **France**, the patient decides whether to create a DMP. Some data can be omitted or "blocked" at the patient's request, and data is saved up to 10 years following the file's closure. However, according to a 2012 survey[68], 45% of the persons surveyed had their DMP opened without being asked for their consent.

In **Greece**, the patient must provide explicit and specific consent every time doctors want to access data entered by other doctors in the e-Prescription database.

In **Italy**, the patient must provide their free, express, clear and unequivocal consent before their electronic health record is created. However, once a file is created, the data collected is saved for the patient's entire lifetime, unless they request its deletion.

66. HILMO
67. National Institute for Health and Welfare.
68.LH2 carried out for the Comité interassociatif sur la santé (Ciss) www.ticsante.com/story.hp?story=1202#ixzz2jzksQ4SM

In many of the countries studied, lawmakers are implementing data collection systems on a "default" basis – patients can only express their disapproval after the fact. This process does not make it possible to obtain the patient's prior approval, in that the patient must take active steps to refuse filing after the file has been created. For instance, in **Hungary**'s new electronic public health filing system that contains data on prescriptions, diseases, etc., doctors can access data (whether they are general practitioners or specialists) without obtaining the patient's prior consent. However, the patient can opt-out by sending a written letter to the National Health Insurance Fund. In **Austria**'s ELGA system, the patient's consent is not necessary when collecting optional data (optional data is data the law does not require to appear on a patient's card). However, the patient may ask that the collecting of optional data stop (this is an "opt-out" system).

This concept of "optional data" should be further discussed. In **Germany**, **Austria** and the **UK**, recording some types of data is optional (often medical data) and other types of data are compulsory. Administrative data required for each of these three databases is mandatory, which means the patient/assured party cannot oppose its collection. This is also the case for some health data: reactions to medications or allergies in the **UK** and medical prescriptions in **Germany**. The following are examples of optional data: information on blood group and allergies on the electronic health card in **Germany**; and medical certificates and laboratory tests in the ELGA filing system in **Austria**. It should also be noted that, in **Austria**, optional data is collected "by default", while in **Germany** the patient must consent before this data is saved in the filing system.

Content and access: who can access medical data?

In **France**, only practitioners who hold secure electronic health professional cards can access their patient's DMP. Data is sorted by "field of consultation" (a chemist cannot read a consultation report, for example). A patient's identification number is a random national health identifier . It was the French DPA that requested this number be random: the government wanted it to be the patient's social security number which is a number also used by other parties, including employers). Data recorded under this identifier includes health status, consultations, hospital and x-ray records, etc. Risks mainly arise as a result of bad practices and breaches of the law. When a non-authorised third party accesses the DMP by fraud or hacking, this amounts to a major violation of privacy. To avoid such problems, unique software is used and DMP files are hosted by an accredited provider. A record is made of every time the DMP file is accessed and viewed. Anyone found guilty of illegally disclosing data runs the risk of a one-year prison sentence and a €15,000 fine. The HOPSY filing system contains data on the identity of the person hospitalised without his/her consent but also the person who requested hospitalisation and legal information.

In **Germany**, data is stored on a centralised server, which means that persons who are not the data subject (such as employees doing maintenance) may access content if it is not coded. The database contains sought-after information (for businesses, clinical researchers and insurance companies), which increases the risk of abuses and creates increased pressure to legally entitle more groups of people to access the filing system. The advantage of the German electronic health card is that it is possible to access files anytime and modify or delete optional data. In order to be as transparent as possible, the Ministry of Health plans to give the insured person access to their electronic medical file, the ability to modify or delete optional data and to print the file. However, this creates the risk that third parties, especially employers or insurers, ask insured parties for copies of their medical records. In addition, the patient cannot prevent the storage of compulsory data. It should also be noted that it is possible to consult the last 50 times the electronic medical record was accessed. This means the data subject can check who viewed their personal medical data.

In the **UK**, patients can ask their doctor to print them a copy of the data collected in the summary care record (SCR)[69]. According to the NHS website, health practitioners only have access to data required for their functions.

In **Hungary** and **Austria**, there is an electronic health card, as in **Germany**. In **Austria**, however, there is no central database storing all personal data. Some basic administrative information is printed directly on the e-Card, other information is stored on the e-Card's chip and medical data is stored in the information systems of health care professionals. The e-card is key to accessing data in the e-card system and the information systems of the various health care professionals.

In **Greece**, authorised users of the e-Prescription system only have access to data they entered themselves into the database. In exceptional circumstances, and with the patient's consent, a doctor may access to their patient's full medical record.

According to the Polish Ombudsman, the law creating the data filing system is insufficiently precise with respect to the categories of data that can be saved in the medical information system and who has access to this information. The Ombudsman also criticised the fact that the system was created by ministerial decree, given that the Constitution states that personal data processing must be founded in law (in the strict sense of the law; in other words, a law voted in Parliament). In **Hungary**, similar criticisms have targeted acts creating some databases and data collection rules on specific issues such as contagious diseases. In these examples, Hungarian health filing systems are based on ministerial decrees, while personal data processing should be permitted and regulated by law.

Data storage periods

In **Austria**, data is viewable by chemists for up to two hours after the patient's visit, and by doctors, hospitals, etc. for 28 days. A record is made of each time the data is accessed. This record is saved for 3 years in order to ensure those who accessed the data were legally entitled to do so.

In **Hungary**, data may be saved for 30 years (50 years in some cases). In **Greece**, data is not kept in the filing system for more than 20 years after the last medical consultation. This data storage period seems very long considering that, in practice, legal and security measures are not strong enough to prevent non-authorised access to data in the long term. In the **Czech republic**, most data is saved for up to 5 years, but some may be saved for up to 50 years, depending on the register concerned. In **Italy** and **Germany**, personal health data is saved for the data subject's lifetime in the electronic health filing system, unless the patient requests the deletion of saved data. Nevertheless, in **Germany**, some data cannot be deleted from the filing system. In the **UK**, data is also collected for the data subject's lifetime. Furthermore, once the patient has agreed to open a SCR, they cannot prevent data from being collected and stored, unless the SCR has not yet been used for health care. If the patient decides to close their SCR, data is not deleted, but remains saved in the filing system. Consequently, opting out only makes data non-consultable by health practitioners.

In **Finland**, data collected in the Prescription Centre filing system is stored 30 months before being transferred to an archive filing system (Prescription Archive" where it is kept for 10 years. Data in the Prescription Archive is no longer accessible to chemists but can still be used for research or drug safety measures, for instance. In **France**, data is stored 10 years in the DMP starting from its closure (as requested by the patient). During this period, the patient can ask for the DMP to be reactivated. They can also request the definitive deletion of some or all data. As regards **France**'s HOPSY filing system, data is stored up to the end of the civil year during which the hospital stay took place.

69. www.nhscarerecords.nhs.uk/faqs

Security of access

Too many people can access the HOPSY filing system in **France**. Even the Ministry of Health seems unable to manage the situation, as it sent out a survey in 2011 asking who had access to the filing system. We have little information on how the HOPSY filing system is used. The filing system is always checked when someone asks for permission to bear a firearm. Security seems extremely weak given the seriousness of the discrimination that may result from accessing the filing system (a psychiatric hospitalisation may lead to social stigmatisation, damage to a person's career, etc.).

The rules governing access to the German electronic health card are not yet definitive as the health card is relatively new. However, most data is saved on a server (the card is the "key" to access the system), and the card contains only some administrative data, some prescriptions (up to eight) and medical data required for first aid.

In **Hungary**, the system is unclear with respect to several points. For instance, a doctor can transfer a patient's medical record to their general practitioner except if the patient objects to the transfer. But how can this right to object be effective if there is no duty for the doctor to inform the patient? The patient's consent is not needed for collecting medical data. The patient can only prevent access to their personal data by actively sending a written request to the National Health Insurance Fund. Also, in **Austria**, data is stored by default, and the insured party has to opt-out if they do not want this to be the case. Opting out can be done by submitting an online request, which is easy enough to do – but only if the person knows their rights. In **Hungary**, access to data is supposedly dependent on the reasons for consulting the file, but this guarantee appears weak given that security measures can be modified by ministerial decree and that the national DPA is no longer independent.

In **Greece**, data accuracy is relative, because a doctor cannot delete or correct any data he/she entered. National and regional doctors' associations have raised concerns as to the lack of appropriate security measures, including those ensuring the protection of health secrecy. The risk is all the more serious given that non-authorized accesses may lead to the disclosure of almost all of a person's health data.

Measures aiming to protect the right to privacy include the rule that data collection and storage periods must be proportionate to the purposes of the data collection. Consequently:

- A person must have a legitimate purpose in accessing or receiving data: this is the case in **France**, the **Czech republic** and **Greece**. A similar measure is planned in **Hungary**.
- Data storage periods must vary depending on the objectives or recipients. See, for example, **Austria**.
- Making data anonymous must depend on the purposes and recipients. See, for example, bad practices in the **Czech republic**, where data is not anonymous even though it is collected for statistical purposes and identifying data is unnecessary.

Registering an ID number for non-medical purposes and interconnection risks

Personal health data is often recorded under a number that is, in most cases studied, the social security number or an identification number attributed to the individual for several administrative filing systems. For instance, in **Italy**, **Poland**, and the **UK**, individuals are allocated an identification number from birth, and this number is used in health and other filing systems (for instance, in the social security system in **Poland**). In each of these countries, the number has meaning. The Italian number is composed of letters and numbers that indicate the person' gender and month, day and place of birth.

In most countries, the social security number is used. This is the case in **Germany**, **Hungary**, **Austria**, the **Czech republic** and **Greece**. In **France**, CNIL has ensured that the number used in DMPs is random, to avoid risks associated with uncontrollable interconnections. Consequently, the Identifiant National de Santé (National Health Number or INS) is unique, permanent, meaningless and cannot be guessed.

Concerns have been raised in some countries where ID numbers are used in several filing systems. In **Greece**, for example, NGOs are worried that professional users may abuse their right to access the system, which could lead to non-authorised people accessing all data saved. In **Finland**, a Personal Identity Code or Personal Identity Number[70] is used in the HILMO filing system (Care Register for Social Welfare and Health Care). This number has meaning and is used in other fields, such as justice[71]. However, according to the Ombudsman dealing with data protection issues, the security of health filing systems is sufficiently robust.

Centralised systems lead to increased interconnection risks

Some countries have non-centralised systems. In **Austria**, there is no central database for ELGA files. Data is stored in the information systems of health care professionals, and some data is recorded directly on the insured party's e-Card (some data is printed on the card, other data is recorded on the chip). It is through the patient's e-Card and the indexes of healthcare professionals and patients included in the ELGA system that authorized persons (with a health professional e-Card) can access data, wherever it is stored. In **Germany**, some data is stored on the e-Card, but most is stored on a server.

C. APPEALS

The right to personal data protection means it is possible to file appeals. Appeals lodged by individuals, who often have had to overcome many obstacles, have improved data protection. Appeals have helped deal with gaps in legislation and draw attention to abuses.

- In **France**, issues raised by associations of patients and physicians have led to several modifications to DMPs. Individuals have also lodged appeals with the administrative courts with respect to the HOPSY filing system after being refused access to their medical files. In one case, the administrative court ordered the Paris Prefecture to communicate the contents of a file to the data subject, as well as the official order that led to his/her forced hospitalization.

- In **Germany**, appeals have attempted to challenge the existence of the electronic health card, but all have failed. One lawsuit filed with the Federal Constitutional Court challenged the law establishing the electronic health card. The Court decided that the lawsuit was inadmissible, because insured parties cannot bring claims against the law. In another lawsuit filed with the Social Court in Düsseldorf, the Court decided that the general interest prevailed over the right to informational self-determination.

- In **Hungary**, it was judged unconstitutional to put data subjects' insurance numbers on prescriptions for non-refunded pharmaceutical products in 2009. The problem appeared to be resolved until a new ministerial decree required a bar code containing the insured party's identifier to appear on prescriptions.

70. www.thl.fi/en_US/web/en/statistics/information/register_descriptions/careregister_healthcare
71. For other examples of the uses of Personal Identity Codes: see www.vrk.fi/default.aspx?id=45

A complaint to stop unlawful data processing was submitted to the Hungarian DPA but the DPA refused on the grounds that the infringement was minor. However, this “minor” infringement concerns hundreds of millions of prescriptions per year. In addition, the National Health Insurance Fund makes the database (or data) accessible to multinational companies and researchers without providing any data protection guarantees (such as prior consent or even the right to opt out).

- In **Greece**, most actions against this filing system, including appeals, have been by NGOs working in the health sector or doctors’ associations. However, some courts have judged that the system’s benefits outweigh any risks for citizens.

D. THE ROLE OF THE DATA PROTECTION AUTHORITIES

Data Protection Authorities in each country must have the power to comment on health data bills and practices before these enter into effect, and to carry out regular checks after they have been implemented.

- In **France**, the DPA (CNIL) has delivered opinions on laws before they are passed and carried out regular checks now the system has been implemented (for example, on-the-spot checks). CNIL has ensured that social security numbers are not used as DMP identifiers, making interconnections impossible. CNIL has also ensured that patients are given clear information on DMPs and what it means to consent to these files being created (patients must sign written consent forms containing information on DMPs). CNIL also ensures that all access to and consultation of DMPs are tracked and that data stored in DMPs or transferred to other sources is coded. CNIL succeeded in ensuring a random national health identifier was used. In addition, CNIL has published a guide for health professionals. CNIL issued a favourable opinion on the creation of the HOPSY filing system, highlighting good practices laid down in the law. These include informing the patient that a file is created upon entering the hospital, providing the patient with information when he/she requests information on his/her legal position and rights, and modifying access to data in line with recipients’ roles and data content, etc.

- In **Greece**, the DPA regularly carries out checks and issues recommendations. Checks carried out in 2013 raised awareness of the fact that past recommendations had not been followed.

- In **Hungary**, the Ombudsman was replaced by a national DPA in January 2012. Since then, two cases have been reported. Both involved appeals filed by patients against doctors who refused to provide them with their medical records. In the first case, the doctor was fined, but in the second case, no breach of law was found.

- In **Austria**, the DPA recommended that personal data be transmitted in the following way. Rather than creating “automated” access to data in databases, the patient or doctor should be able to choose whether to disclose their data to other professionals when they deem it necessary.

Our recommendations to improve personal data protection in the health field are as follows:

The use of electronic medical filing systems must be reserved for patients undergoing heavy, expensive and long-term treatments.

The patient must provide prior explicit consent before any personal data is collected for storage in a health filing system. The patient must be able to choose whether or not to open a personal health file. The patient must also determine which third parties can access his/her data and which data in each case.

Stored data must be protected by specific data security measures, such as encryption.

Private third parties such as banks, insurers, employers and pharmaceutical industries or information companies must not have access to central health databases. Regardless of their aim, including predictive medicine, personal data must not be transmitted to private bodies.

Data used for statistical purposes must be anonymous. Anonymisation means that persons to whom data is provided for statistical purposes must not be able to identify data subjects by employing reasonable means. What “reasonable means” entail must be assessed in line with the type and number of anonymous data files transmitted, as well as the information they contain.

If requested by the patient, paper prescriptions must be used as an alternative to electronic prescriptions.

Independent studies must be carried out on different kinds of data storage media including electronic cards, flash drives, etc. before any database is implemented.

DPAs must have strong powers to intervene early on in countries where the law regulating health filing systems is vague.

EDUCATION

A. FREEDOMS AT RISK

In all the countries studied, data is recorded in the education field to improve management of the educational system by simplifying administrative formalities, providing better advice to pupils, publishing educational statistics, etc.

Given these objectives, considerable amounts of data presenting privacy risks is collected and saved for long periods. However, children and teenagers should have the "right to oblivion". This information should not allow educational institutions to establish profiles predicting a young person's future. Processing data on children's religious views and ethnic origins can lead to discrimination or stigmatisation risks. This should be of central importance to parents and teachers.

In the **United Kingdom**, a 1996 law allowed the government to collect anonymous data directly from schools for the National Pupil Database (NPD)[72]. A series of amendments (in 2000 and 2009) made it possible to compile a list of all pupils. More than 40 individual-level data items are collected without the consent of pupils or their parents. Data items include exam results, first language, attendance, eligibility for free school meals, special educational needs, ethnicity, etc. These targets are even more ambitious than those in **Luxembourg**. Indeed, the NPD aims to identify pupils' strengths and weaknesses so as to choose suitable educational support, publish statistics, target funding for local authorities, etc.[73] Such ambitious aims may lead to uncontrolled data transfers. It should be noted that data is held in four different categories (with different levels of access depending on the privacy risk). Anyone requesting access to data must indicate the category of data they want to access and explain why the information in the least sensitive category is insufficient for their purpose. Balancing risks and benefits is a good thing; however the system is a little too "all-or-nothing" in each category. For instance, to obtain statistics on ethnic origins and school results, someone may be given access to the third category of information (identifiable and sensitive individual pupil level data). In addition to ethnic origins and school results, the person has access to information on "eligibility for free school meals", which does not seem useful or necessary for their study.

In **Austria**, data on the pupil's language, religion, educational needs, school, school type, attendance, examinations, financial support, etc. are saved in the Education Database (Bildungsevidenz), together with their name, birth date, social security number, gender, nationality and address. Data is not anonymised before being transferred to the federal **Austria**n statistics department. Data must be anonymised 20 years after the pupil has left school. This period seems excessively long. Although the law states that conclusions cannot be drawn on pupils' individual situations, there is a high risk of discrimination. Some NGOs have criticised this filing system and the **Austria**n Ministry for Education won a "Big Brother Award" (award targeting the worst privacy violations) for setting up the database.

In **Luxembourg**, the law passed in March 2013 states that the Pupil Database, which groups two earlier databases in this field (separate databases for primary school and secondary school), contains the following information: courses taken, grades, comments from teachers, extracurricular activities, suspensions, justified and unjustified absences, socio-cultural background, mother tongue, number of siblings, country of origin, and the educational level, job and income level of the student's parents or legal guardians, etc.

72. The National Pupil Database only covers educational institutions in England. Similar systems apply to schools in the rest of the UK.
73. Deloitte stated this database was a "set of data on schools potentially the world's richest".

While data is anonymised before being used for research and statistics, this is insufficient to avoid privacy breaches, since **Luxembourg** is a small country. Given the many types of data collected, deleting the pupil's name is insufficient to prevent them being identified. This is especially true when the person has a unique profile. There is a high risk of discrimination.

In addition to this issue, some administrative bodies may access personal data (before it is anonymised). These institutions include the Ministry of the Family, local administration, educational advisors, the State Secretary in charge of higher education, the national employment agency (which uses data to advise students in professional training programmes), counsellors (which uses data to provide advice to students on vocational training), etc. It should be noted that, in **Luxembourg**, refusing to provide compulsory information can lead to a fine of €250. Of the data recorded in this filing system, only phone numbers and emails are optional.

The **Luxembourg** Pupil Database is a good illustration of how deleting first names and surnames does not always mean data is anonymous for the purposes of personal data protection. According to WP29, anonymous data is a data on an individual who cannot be identified using reasonable means. Small country sizes make it difficult to anonymise data (as is the case in **Luxembourg**), but this is not the only factor compromising anonymisation. Questions should be asked as to the guarantees provided whenever a country's data is said to be anonymous (for instance, if a large country has a central filing system that excludes names but includes a pupil's town, school attended, country of origin, age, number of siblings, etc., it is possible to identify the pupil using "reasonable means"). The difference between anonymous data and non-anonymous data is fundamental because it determines whether data is personal or not, which then leads to different protection rules.

The recording of sensitive data: the example of religious views

Data on religion is one of the special categories of data listed in the Directive 95/46/EC. In principle, processing of this data is forbidden[74]. This data is generally referred to as "sensitive", because this is the term used in several national laws transposing the Directive (see glossary).

Some of the countries studied collect data on religious views in education filing systems. This is the case in **Greece**, **Hungary**, **Italy**, and **Austria**.

In **Greece**, where the e-School database was implemented in 2006, there are optional lessons on the Orthodox Christian religion. To manage enrolments in these lessons, the religious views of pupils are collected in the database. If the religious view registered is "Orthodox Christian", the pupil is enrolled in religious lessons.

There are no other classes on religion or ethics in Greek public schools. It is worrying that, for a lesson on a given religion, data is collected on other religious views and even the lack of religious views. Collecting and storing information on religious views, no matter what they are, is excessive given the purpose of the database (improving the management of enrolments).

In **Hungary**, religious education and ethics lessons will take place in school for children between 6 and 10 starting in the 2013-2014 school year. Parents must register their child in one of these lessons. Lessons on different religions are organised (depending on the resources of local religious authorities). A new school-level database was implemented to manage enrolments. If parents do not want to provide

74. Directive 95/46/EC, Article 8(1): "Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life."
www.eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

religious data, they can choose not to make a declaration. Their child is then automatically enrolled in ethics lessons. It should be noted that the filing system containing pupils' names and classes can be viewed by the religious authorities concerned, since they are in charge of organising lessons. Information is only collected on the child's first name and surname, class and religious views (address and date of birth are not collected). Nevertheless, it is easy to identify someone using this data alone. The legality of this filing system is set out in a law adopted by the Parliament, but the main rules are contained in a ministerial decree. Consequently, this new school policy lacks the basic guarantee that fundamental rights be protected using laws.

In **Austria**, NGOs have criticised the fact that data saved is not anonymous (it is only anonymised 20 years following its collection). Since sensitive personal data is collected, including religious views, this filing system may create grounds for discrimination.

Other sensitive data may also be collected in education databases. Data on pupils' health is collected in databases in **Greece** and in **Italy**. In **France**, this information can be inferred from the kind of school attended by the pupil (e.g. medico-educational institutes).

Storage periods of personal data

In some countries studied, data storage periods are not legally limited. This is the case in the **UK**, where data may be saved for an unlimited period, without even being made anonymous.

In **Austria**, the law imposes time limits on data storage. The most sensitive data (address, social security number, etc.) is deleted two years after the child has left school. Other data used for matriculation can be saved for 99 years. Data must be anonymised 20 years after the pupil has left school.

In **France**, data is deleted from the RNIE database 5 years after the pupil left the last school attended. The Ministry of Education sought a 40-year storage period for a former version of the database (BNIE). Following a query by CNIL as to the purpose of keeping data for such a long period, the Ministry reduced it to 35 years[75]. However, this was still excessive, even for a pupil leaving school at the age of 16 (attending school after 16 is no longer an obligation).

In **Italy**, data in the national pupil and student database (Anagrafe Nazionale degli Studenti) is saved up until the end of the calendar year following the end of each level of schooling. Data collection starts in the first year of primary school and ends until after university studies have been completed.

In **Luxembourg**, data may be saved for up to seven years after the student has finished their secondary education. Nevertheless, all data on suspensions, non-attendance and linguistic regime are deleted once the pupil leaves secondary school.

In **Germany**, there is no centralised national database in the field of education. Only some federal states, such as Berlin and Bavaria, have education databases. Storage periods are very short compared to those in other countries studied. In Berlin, all data is deleted one year after the pupil leaves school. In Bavaria, school-year-related data (special educational needs, full-day-care, participation in exchanges, etc.) is deleted one year after collection while other data (name, address, nationality, etc.) is deleted six years after the pupil leaves school.

75. Letter from the French DPA to the Ministry for National Education, on 12 June 2006: "I observe that the storage period for data in nominative form is 40 years. I would question the relevance of such a period since the purpose of data collection is the monitoring of pupils' schooling. Please explain the reasons for such a period".
Letter from the Ministry for National Education to the French DPA, on 8 February 2007: "The storage period for data in nominative form, initially planned as 40 years, will now be limited to 35 years. This length is the addition of the data storage period of Information System for pupils of the 1st degree (15 years), second degree (10 years) and higher education (10 years). It aims to make it possible to monitor all pupils' schooling until they leave the education system and higher education training programmes, including any breaks followed by a return to university for instance."
www.ldh-toulon.net/spip.php?article2877

B. TRANSPARENCY AND CONTROL BY DATA SUBJECT

Some countries have difficulties conforming to privacy requirements. In **Greece**, the e-School system was not implemented by a law. Instead, it was implemented by the Ministry of Education, which contracted with a private firm to do so. The Ministry never informed the Greek DPA (HDPA[76]) that the filing system existed (even though the law on the protection of personal data states that databases must be reported to the DPA before implementation). In addition, the database records sensitive data such as religious views without HDPA's approval.

In **France**, the Pupil Database was launched in 2004 but was never subject to regulations published in the Official Journal. It is only after criticism by parents and principals, as well as appeals to the Council of State (which delivered a judgment on 19 July 2010), that the Ministry of Education made the BNIE legal in 2012.

In order to limit invasions of privacy when processing data, it is possible to limit data disclosure depending on recipients (by sorting anonymised / non-anonymised data for instance). In **Hungary**, the law states that national database managers only have access to anonymised data, while identifying data can only be accessed by the following recipients at schools: teachers, principals and Church representatives. However, principals are now appointed by the State Secretary for Education, who is the leader of the majority party currently in government. In 2013, there were many controversial principal appointments. In too many cases, candidates supported by professional organisations and teachers' organisations were rejected for no real reason in favour of people loyal to the political party. Given this context, limiting who can access personalised data is useless. To protest at this state of affairs and improve security, some teachers anonymise rolls for ethics or religious education classes themselves. This shows a lack of trust in legislative guarantees.

Even if the law states what the aims of data collection are, in many countries there are fears that files will be used for other purposes. For instance, in **France**, though data is only collected for administrative purposes, people fear the education database will be used to identify undocumented migrants or verify absenteeism. This also applies to **France**'s Livret Personnel de Compétences (Personal Skills Booklet or LPC), which is a kind of CV that is theoretically only accessible by the Ministry of Education. Parents' organisations have raised concerns as to the lack of transparency with respect to how data collected in the LPC will be used. For instance, will a future employer be able to access it?

In many of the countries studied, citizens do not appear to be taking action against these databases. This shows how they lack information on and awareness of these filing systems. In the **UK**, citizens are more aware of the National ID Register or the DNA database, although parents have criticised the fact that confidential information on their children has been transmitted to private companies[77]. However, in **Germany**, civil society organisations and DPAs are very concerned with education filing systems. It is therefore very unlikely that a national pupil database will be implemented in the near future. Furthermore, the filing systems studied in Bavaria and Berlin have very narrow aims, and the rules for deleting data are very strict (see the storage periods section).

Despite the lack of public interest in data collection on pupils, the **UK** Department for Education seems to be making an effort regarding transparency. On its website, a considerable amount of information is provided on the National Pupil Database (NPD). One of the first links is a "NPD user guide". This guide explains which data is sensitive, how data is securely recorded, etc. Two practices deserve to be mentioned:

76. Hellenic Data Protection Authority.
77. www.mikesivier.wordpress.com/tag/national-pupil-database

- The “NPD data request application form” stresses that caution must be exercised when using the data obtained. The person requesting data must answer questions to ensure his/her request is legitimate. These questions ensure the person is aware of the seriousness of their request. Examples include: “What are the aims of your project or research?”, “Is there a specific question you are seeking to answer?”, “Who is the intended audience?”, “Are you proposing to match the data you have requested with any other data?”, etc.[78]

- The Department’s website discloses all requests made during the previous calendar year.

It is disappointing that, in **Hungary**, the DPA has provided little information on appeals brought before it (the database may be recent but has also been widely criticised). In addition, the DPA’s legitimacy has been contested given the circumstances surrounding its creation. Indeed, the new DPA replaced the old one before the previous DPA had completed its mandate. It is possible that **Hungary** has violated the DPA’s independence. For this reason, the European Commission has referred **Hungary** to the European Court of Justice with respect to this issue[79]. The European Court of Justice ruled against **Hungary** on 8 April 2014[80].

C. APPEALS

Checks must be carried out before and after databases are created in order to avoid privacy violations and discrimination. DPAs have the power to complete regular checks of filing systems once they have been created. In addition, it is recommended that legislative and/or executive bodies submit bills creating or modifying data processing procedures to the DPA (one example is the exchange of letters between the French Ministry of Education and the French DPA before the BNIE filing system was created). Over and above these checks, appeals lodged with the administrative body responsible for the filing system, the DPA or the courts (administrative, criminal or civil courts) help regulate filing systems. Appeals by individuals, supported by associations and trade unions for instance (parents of pupils, teachers, etc.) have meant that rules governing some practices have been modified and databases updated in order to better protect fundamental rights and freedoms.

In **France**, in 2010, the Council of State deemed that data storage periods and the amount of data in the pupil database was excessive[81]. Following this decision, the RNIE[82] filing system was created to replace the BNIE[83] filing system. Excess data such as nationality, year of arrival in **France** and the teaching of native languages and cultures have been removed. Also in **France**, parents have laid complaints with the courts because they considered their right to object had not been respected[84]. On 14 June 2012, the administrative court of Bastia ruled in favour of parents, based on Article 38 of Law 78-17 of 6 January 1978 on information technology, data filing systems and civil liberties (loi informatique et libertés), which states that “Any individual is entitled, on legitimate grounds, to object to the processing of any data relating to him/her”.

78. NPD Data Request Application Form: www.gov.uk/government/publications/national-pupil-database-application-form-declaration-and-agreement
79. www.europa.eu/rapid/press-release_IP-12-395_en.htm
80. www.europaforum.public.lu/fr/actualites/2014/04/cjue-hongrie-protecteur-donnees/index.html
81. Conseil d’État, 10ème et 9ème sous-sections réunies, 19/07/2010, 334014 http://www.legifrance.gouv.fr/affichJuriAdmin.do?oldAction=rechJuriAdmin&idTexte=CETATEXT000022513055&fastReqId=32778958&fastPos=1
82. Répertoire national des identifiants élèves.
82. Base nationale des identifiants élèves.
84. Some parents requested the deletion of data saved on their children. Their request was refused on the ground that schooling the child led to the impossibility to object to the “collection of data necessary to manage the pupil’s file, since these files do not gather sensitive data and they are used for a public service mission”. www.retraitbaseeleves.files.wordpress.com/2012/06/ta-bastia-decision-14juin2012.pdf

Lastly, even if this does not concern appeals, it should be noted that when DPAs and civil society organizations work together and publish reports, this may have an influence on plans to create or modify education filing systems. For instance, in **Germany**, there were discussions on introducing a pupil identification number in 2006. The project was abolished following strong opposition from NGOs and DPAs. Meanwhile, in the **UK**, the lack of citizen action against this kind of database has led to the scope of filing systems being constantly widened. Today, there are plans to further widen the scope of the education database, making it possible for the police and education stakeholders (amongst others) to access data for "social and economic" purposes (see the Deloitte report mentioned above).

In **Greece**, there is also a lack of interest in the e-school filing systems. Very few parents disagree to the collection and storage of their children's religious views.

D. THE ROLE OF THE DATA PROTECTION AUTHORITIES

In **France**, we consider that CNIL failed when the Ministry of Education implemented the BNIE pupil database (since renamed RNIE). Following appeals to the Council of State, CNIL regularly audits the system and has requested to be kept informed on file uses. In **Luxembourg**, the DPA is currently monitoring how the new filing system containing pupils' personal data is being developed. Online access to the system is controlled via an electronic "Luxtrust certificate" that is managed by a private firm. In 2011, the **Luxembourg** DPA intervened in order to obtain the removal of some school results published online (this data could be accessed with a student's first name and surname).

In **Greece**, the Ministry of Education set up the e-School system after signing a contract with an external company. The DPA was not informed of this step. Following its audit in 2012, the DPA made several recommendations to the Ministry of Justice (responsible for the filing system's technical management). The Ministry was supposed to make changes within six months of the recommendations being issued. As at the end of 2013, the Greek DPA had not been informed of any changes based on its recommendations, and it has not yet carried out an audit to check they have been implemented.

In **Hungary**, the DPA chairman considers saving data on religious views is legitimate because only the names and classes of pupils are communicated to religious authorities. In his opinion, pupils cannot be identified based on this information; therefore, data processing by the central government agency responsible for school maintenance does not breach privacy because the database is anonymous. It is also important that the ministerial decree states that parents can refuse to sign the written declaration form choosing whether their child attends religious or ethics classes. The DPA considers that the automatic enrolment in ethics classes of pupils who fail to make declarations is a sufficient guarantee for privacy.

In **Italy**, the DPA[85] delivered a favourable opinion on the filing system's creation. However, it would like to see a code of conduct and professional practices implemented for personal data processing on the institutional level. In **Italy**, the data subject has the right to object, in whole or in part, to data processing, provided that their reasons are legitimate (or if data is used for commercial purposes).

85. Garante per la Protezione dei Dati Personali.

Our recommendations to improve personal data protection in the education field are as follows:

Personal data must only be collected at the school level, or on a local or regional level, depending on why the data is collected and the responsibility owed to the child or student. Data used nationally for statistical purposes must be aggregate data collected on the local level, especially for sensitive data such as religion and health information. Aggregate data result from statistical calculations on individuals' raw data grouped because of common characteristics.

The data storage period must be short. This period must be established after taking into account the fact that data mostly concerns minors. Records of any educational "missteps" must not be kept in filing systems for their entire school career or longer.

Education databases must not contain sensitive data if it is not strictly necessary and proportionate to the legitimate purpose of the filing system. Consequently, when organising religious, classes a pupil's religious data must not be stored with any other identifying data except at the school itself. This means that one religion lesson is not grounds for setting up a database collecting pupils' religious data.

Institutions must expressly inform pupils (or students) and their parents what their data is used for. They must also provide training on data protection and databases. This is about more than simply providing information; it is also about educating people on these issues, starting from childhood.

Education on data protection in the education field is all the more important given that the general public appears less concerned about education databases than police and justice databases, including DNA databases and criminal records.

DPAs must have strong powers to act pre-emptively in countries where the law regulating educational filing systems is vague.

Filing systems studied by field

POLICE

France

FAED: Fingerprints File: This file is shared among police, gendarmerie and customs. It is used for the identification of criminals.

FNAEG: National File of DNA Profiles: centralises the DNA profile of the persons responsible, prosecuted or suspected for a crime. Its purpose is to facilitate the identification and the search of criminals.

ADGREF 2: Application for the management of the foreign nationals, created to guarantee the rights of the holders of a residence permits and to fight against illegal immigration in France.

STIC: Constitued Offences Record: contains information from the police about persons involved in a criminal procedure to facilitate the investigations.

TAJ: It contains information from the police and the gendarmerie about persons involved in a criminal procedure to facilitate the investigations (new STIC)

PASP: Prevention of Public Security Threats: contains information about people whose individual or collective activities could represent a threat for public security (in particular for the persons involved in acts of violence in urban area or during sports events).

TES: Secure electronic titles (Titres Electroniques Sécurisés): Data base created for the passports issue and control.

Germany

AFIS Automatic Fingerprint Identification System: File containing all fingerprints collected by the police.

Anti-Terrorism-File (Antiterrordatei (ATD)): fight against terrorism, therefore it is designed to include information (or references where to request information) on individuals either involved in terrorist activity, supporting terrorism or supporting violence.

DNA-Analysis-File: File containing DNA-data of (certain) convicted criminals, suspects, volunteers and crime scene traces.

Resident registration: File containing personal information about all citizens, e.g. current and former addresses, date and place of birth, children, religion etc. Currently organized at the local level but the legal possibility to set up a federal file exists.

Right-wing extremism: A joint file containing right-wing extremists.

Hungary

RoboCop: for administrative and crime analyzation purposes, criminal statistics and to make investigations more effective.

Luxembourg

DNA personal data

Spain

ADN-VERITAS: ensure a better cooperation between Police and Justice for the elucidation of criminal offenses, thanks to the genetic identification of biological traces.

ADEXTRA: This file contains reports and decisions taken during immigration procedures.

SIGO: Integral System of Operative Gestion: police database with all the information about offenses, offenders, automobiles and police investigations.

PERPOL: This file contains police antecedents about people in order to facilitate police investigations.

INTPOL: This file permits to ensure public safety through the control of people and facts of police interest, for to the prevention and the investigations of criminal offenses.

GATI: Objective: prevention of infringement to public safety and criminal law enforcement through the recovery, evaluation, treatment, coordination and analysis of all the information obtained by the police.

GRUMEN: This file contains police information about minors.

Italy

BANCA DATI DEL DNA (DNA Database): to facilitate the identification of criminal offenders, especially with the comparison of DNA profiles
CENTRO ELABORAZIONE DATI (CED): contains information and data for the protection of public order, public security and prevention/repression of criminal offenses.

Portugal

Base de dados de perfis de ADN para fins de identificação civil e criminal: DNA Database: for civil and criminal identification

Sistema Integrado de Informaçoes Operacionais Policiais (SIIOP): Police Database

Greece

Police DNA database

Police Website for wanted persons (also applies for Justice): Protection of the society and facilitation of the work of Police to sanction crimes

UK

National DNA Database: for crime prevention, criminal prosecution

Austria

Nationale DNA-Datenbank: National DNA Database

Finland

The national Vehicular and Driver Data Register: Improving road safety, reducing environmental nuisances caused by road traffic and managing tasks related to road traffic taxation and to motor vehicle mortgages

Europe

EURODAC

JUSTICE

France

Casier judiciaire national – National Criminal Record

FIJAIS: Judicial File of Sexual Offenders: This file lists the persons who have committed a sexual offence or a serious crime, to prevent repeat offenders and to facilitate their identification.

Cassiopée: Information System for the Criminal Procedure: Data base containing all the information about each judicial record.

Germany

Zentralregister – Central Register: contains information on criminal convictions (criminal record) and certain decisions of administrative authorities and courts.

ZstV: contains information on all preliminary investigations by public prosecution.

Luxembourg

Casiers judiciaires – Criminal Record

Vidéosurveillance - Centre de rétention de Luxembourg-Findel.

Spain

INTCF ADNIC: DNA Database: identification and genetic comparison of biological evidence for investigations requested by the judiciary and the public prosecutor.

Registro Central de Penados: This file lists the final sentences for the commission of a criminal offense. Registro de medidas cautelares, requisitorias y sentencias no firmes: The file lists the non-definitive penalties and measures security imposed after a crime or an offense in order to improve the good-working of criminal proceedings.

Portugal

Registo Criminal: Criminal Record

Austria

Strafregister (Criminal Record)

Finland

National Criminal Record

Europa

SIS II
ECRIS

HEALTH

France

DMP – Personal Health Record: contains health information about the patients in order to assure a better coordination between health professionals, better quality of care, better information to the patient, and the control of the national health expenditures.

DP Pharmaceutical file: to facilitate the coordination, quality, continuity of care and the safety of the delivery of medicines, products and objects.

HOPSY: records all the persons with psychiatric disorders hospitalised without their consent for a better health records' management, and harmonisation of the practices, and statistics.

RIMPSY: Psychiatric Information Records: records the patients of all the psychiatric structures for the improvement of the psychiatric activity and the optimization of care.

RNCPS SGNI- National Index of the Social Protection: It contains datas of all the persons with social benefits, to fight against frauds and to make easier the administrative procedure.es administratives.

Germany

KIS – Hospital Information System

Databanken über Infektionskrankheiten – Infection Diseases Database
eGK - Electronic Helth Card: contains information about every medical insured person.The purpose is the improvement of the economics, quality and transparency.

Luxembourg

Centre Hospitalier du Luxembourg Videosurveillance.

Spain

SINVIH: provides information to the health administration on the impact and evolution of new diagnosis of HIV infection in order to understand the factors and to determine preventive strategies.

Archivo SISS: contains information related to persons involved in Social Security frauds.

Italy

Fassicolo Sanitario elettronico – Electronic Health Record: to improve prevention, diagnosis and treatment of patients.

Greece

National System e-prescription

Poland

SIM (System Informacji Medycznej: Medical Information System

Finland

Care Register for Health Care: to collect information on the operation of hospitals, medical centres and other health care institutions and their patients/clients and those who receive medical treatment at home, for statistical, research and planning purposes.

The Prescription Centre: to enable collecting and storing electronic prescriptions.

EDUCATION

France

BNIE RNIE – National Index of pupils, students and apprentices: This index assigns a national number to each pupil, student or apprentice to facilitate the education system management and the statistical monitoring.

LPC – Personal Competences Book: This book should permit to each pupil, student or apprentice to highlight his competences developed at school but also out of school. It will be use for study options and admission.

Hungary

Educational files: religious views: to organise the classes of ethics or religious views.

Luxembourg

Base de données relative aux élèves: Student Database
Bibliothèque nationale de Luxembourg – Fichier des lecteurs (Users data file).

Italy

Anagrafe Nazionale degli Stdudenti: database created to facilitate the realization of the right/duty of education and schooling and to supervise the progress made in the areas of education, training and learning.

Greece

National File on Pupils of primary and secondary school.

UK

National Pupil Database

Austria

Bildungsevidenz: Education Database

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.