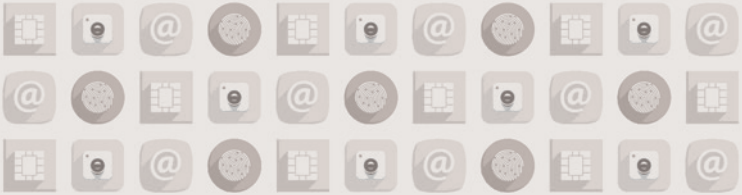
GOVERNMENT DATA
COLLECTION

Are people at risk?



Ligue des **droits de l'Homme**
FONDÉE EN 1898

EDUCATION
HEALTH
POLICE
JUSTICE

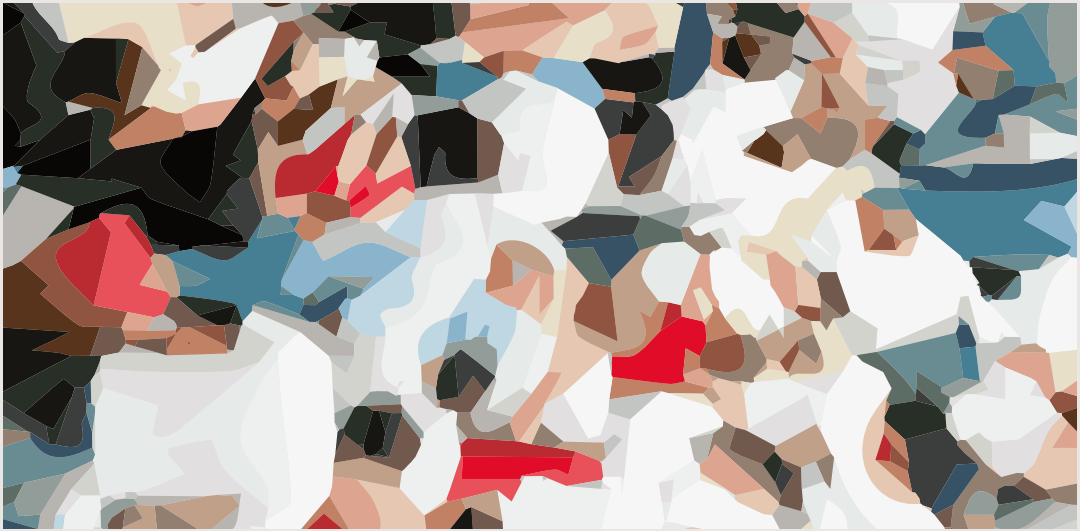
aedh

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



GOVERNMENT DATA COLLECTION

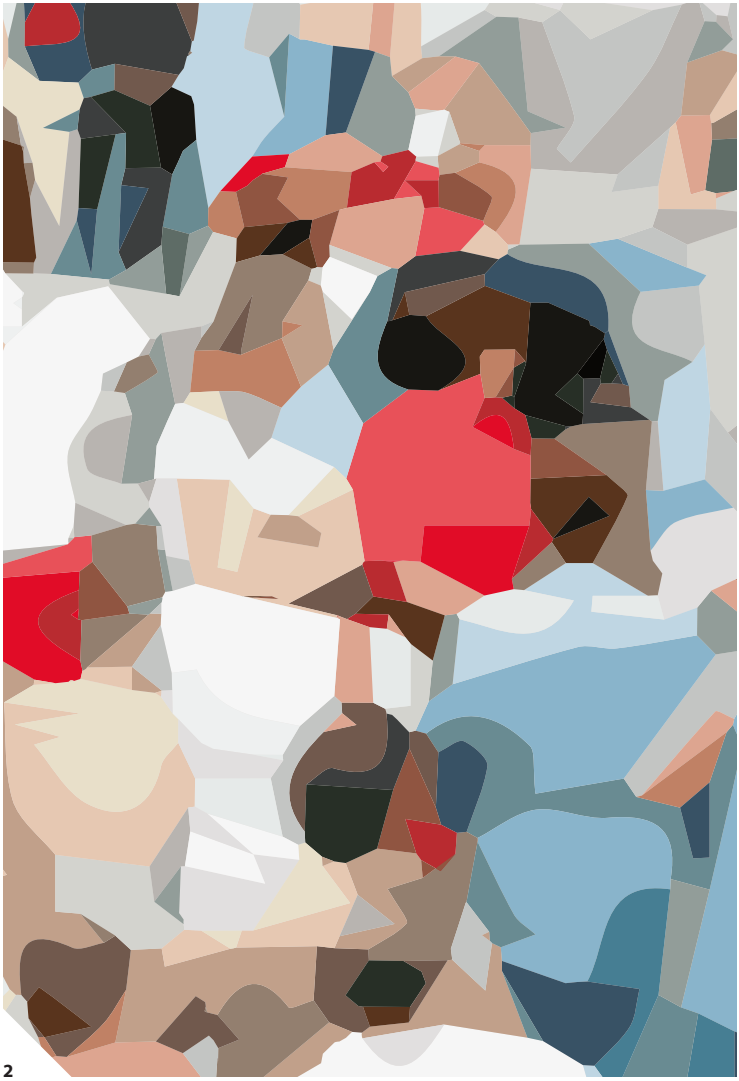
Are people at risk?

Citizens (including you!) are often unaware of the extent of records held by State institutions and agencies containing their personal data and that of people close to them. Are you aware that this data storage may be a violation of your rights, even if there are rules governing such a practice?

Every citizen should know their rights and legal remedies and should not rely on public authorities to decide how their personal data will be used.

Every citizen should exercise vigilance, not only for themselves and their own data, but also for their relatives and society in general.

This passport gives you key information to exercise your vigilance and rights. Once you are aware of your rights, you can then seek further information and take the steps that are necessary (further information is available on the listed websites on the back cover).



GOVERNMENT DATA COLLECTION

Are people at risk?

Purpose and dangers of the files

PURPOSE

The databases used in the education sector are generally intended to facilitate the management and administration of the education system, including organizing enrollment in an educational establishment or in classes, activities and services. They also allow statistics to be put together from the data collected.

These aims are in some way legitimate because they contribute to effective management: defining the number of classes, the number of teachers by discipline, etc.

DANGERS AND NECESSARY PRECAUTIONS

The school databases reviewed contain a considerable amount of data available to schools and authorities. Often, proportionality with the pursued objective is not respected.

Only data that is strictly necessary for management should be collected. Some files contain sensitive data such as the health, mental state, religious views or origins of the pupils. Of course, the more "sensitive" the data, the greater the security measures should be, which is not necessarily the case. Otherwise, children and families may fall victim to discrimination, or even be in danger (discrimination based on religion, origin, etc.).

Such sensitive data in a file related to education should not be recorded without the consent of parents or guardians. Aside from college students and secondary school students in their final years, the people involved are minors. It is therefore primordial to be fully aware of the consequences of such consent and consent should not be given without checking collected data.
A mistake made or a difficult school year might, if recorded, have consequences and cause discrimination for a pupil throughout their educational life and even beyond.

PERIOD OF DATA RETENTION OF EDUCATIONAL RECORDS IN EACH COUNTRY STUDIED

Country	storage life in the studied Education files
United Kingdom	unlimited
France	5 years after leaving the last school attended
Italy	December of the year of graduation
Luxembourg	up to 7 years after leaving secondary education, except data on suspensions, specific linguistic regime and non-attendance (deleted once secondary education is over)

WHAT THE LAW SAYS

The collection of students' and their parents' personal data requires their consent even when this data is collected for statistical or research purposes.

Conducting research and statistics does not require the collection of all individual student data at the national level; a representative sample is sufficient.

NGO initiatives to promote greater respect of the principle of proportionality and the protection of personal data

In 2010 in France, any references to nationality, date of arrival in France and the language spoken by parents were removed from the national education records by the Council of State following the NGOs' initiative.

In Germany, in 2006, the proposition for use of the "Student ID Number" was dropped after a strong mobilization of NGOs.

OUR RECOMMENDATIONS

AS A CITIZEN, YOU SHOULD MAKE SURE THAT:

- Data collected in order to manage schools is not saved at a national level but at relevant local levels. Knowing the "school difficulties" or disabilities of a pupil is useful only to the school or possibly the local administration. The identity of pupils is not needed on a national level.
- Collected data processed at national level is saved only as aggregate data, especially if sensitive data (e.g. health or religion) is involved. Aggregate data is found from a statistical calculation based on a group of individuals' raw data that is grouped according to common characteristics. The anonymisation of data alone is not sufficient to guarantee your personal data protection.

IF YOU AND YOUR CHILD ARE CONCERNED BY AN EDUCATIONAL RECORD:

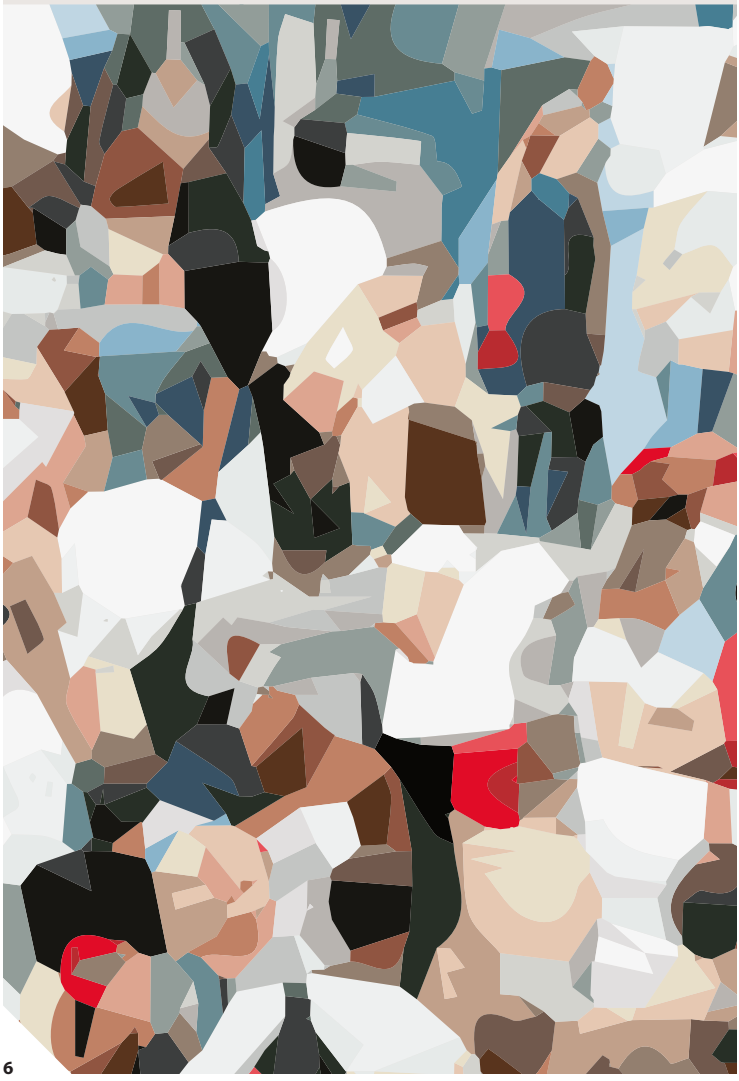
YOU SHOULD REQUEST:

To be informed on how your data will be used (transparency) and the nature of its use, so that you may exercise your right to object and your right to request a deletion or modification.

YOU SHOULD CHECK THAT:

School data is not a basis for discrimination and is not used, for instance, to profile the pupils. Some databases can provide a profile of pupils so as to advise them on schooling or future professional activity.

You must check the nature of data collected and its use before giving your consent to being registered in an education file.



GOVERNMENT DATA COLLECTION

Are people at risk?

Purpose and dangers of the files

PURPOSE

Files concerning health data are used to ensure the effectiveness of public health departments, a personalized follow-up of patients and policyholders, including the coordination between different healthcare professionals, or to monitor the health status of the population through statistical data.

HIGHLY SENSITIVE DATA AND PROVEN RISKS

Health data is by definition "sensitive", particularly because on the one hand, it reveals the health of the patient, and on the other hand, it can reveal social status and other personal information. This data should be particularly protected, which is impossible when a large number of people can access the data relatively easily. The respect for medical confidentiality, a necessary guarantee of the relationship of trust between doctor and patient, is thus jeopardized.

Centralized databases do not always ensure the segmentation of data, which would allow personalized access for each healthcare professional.

Patient anonymity is not always guaranteed and this may encourage other actors, such as employers, insurers and credit agencies, to try accessing this data for economic profit. This constitutes a breach of privacy and risks of discrimination linked to health status: refusal from a bank to grant a loan, access to a job or refusal of complementary health insurance, for example in the event of serious illness.

An example where electronic files become unavoidable

Finland is about to switch to a system of completely paperless medical prescriptions, which means the end of paper prescriptions and archiving of all medical data in computerized health records. It will be impossible to escape from this information system. This is a violation of the right of every person to keep their medical records private.

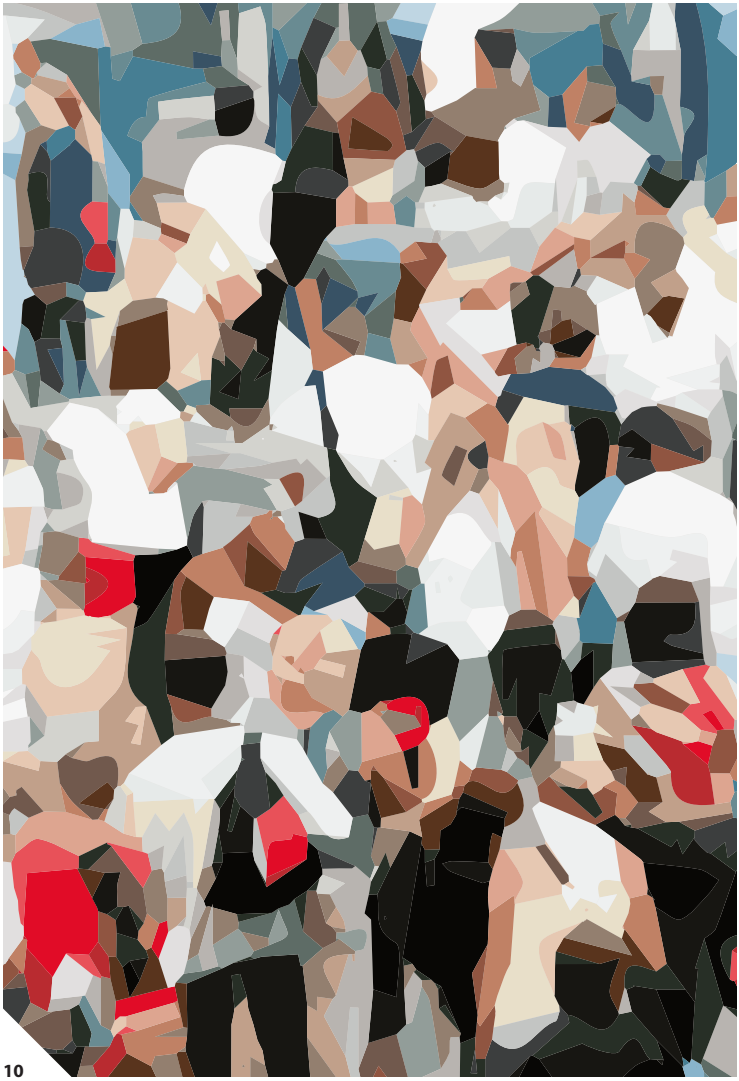
PERIOD OF DATA RETENTION OF HEALTH RECORDS PER COUNTRY

Country	Storage life in files
Hungary	30 to 50 years
Greece	up to 20 years
Czech Republic	5 years (50 years in some cases)
Italy	Lifetime, possibility of removal at the patient's request
Germany	Lifetime, possibility of removal of certain elements of data at the patient's request
UK	Lifetime
Finland	30 months in the "Prescription Centre" system, then up to 10 years in an archive centre
France	10 years from the closure of the file by the patient

OUR RECOMMENDATIONS

AS A CITIZEN, MAKE SURE THAT:

- Electronic medical records are reserved for patients who require expensive, extensive and long-term treatments.
- Patients are informed when their health data is recorded and their consent must be given. They must be able to decide whether to open an electronic health file or not and define which third parties can access their data and which elements of this data. They must also be able to exercise their rights to access and modify data and to deny access to third parties.
- A study on the advantages and disadvantages of the different possible data carriers is carried out by a special independent committee.
- Archived data in health records is in line with specific protective measures, including data encryption for data leak prevention. When data is used for statistical purposes, it must be anonymised.
- An alternative system, such as paper prescriptions, is used at the patient's request.
- The personal data stored in health records is the choice of the patient.



GOVERNMENT DATA COLLECTION

Are people at risk?

Purpose and dangers of police files

Police files are an essential tool for the police to protect citizens and conduct investigations. They improve the possibilities of solving investigations and identifying the alleged perpetrators of criminal offences so that they can then be brought to trial.

However, these files are based on uncertain criteria of suspicion of guilt and dangerousness. They are therefore likely to violate the presumption of innocence, the right to privacy and the right to data protection.

The introduction of biometric data in police files is now widespread, the security issue being a crucial element to enforce this practice. The significant expansion of this practice bears no reasonable relation to the ultimate aim. This is already worrying in a State grounded by the rule of law, so the idea that this state could drift into a less democratic form should be a cause for reflection on the actual relevance of this data processing.

FROM PROTECTION TO DISCRIMINATION: THE SENSITIVE ISSUE OF POLICE FILES

There are a number of situations, aside from conviction, that lead to a person's details being recorded in police files: these may be details of a suspect, a victim, a witness, etc. Depending on how these files are used and the people with access to those files, the recording of personal data in some police files can result in discrimination, have an impact on a person's professional life, etc.

Furthermore, any records filed, with or without a charge, may be kept for an unreasonable period due to non-compliance with the principle of proportionality and poor application of file-handling regulation.

The delicate issue of transparency

To avoid jeopardizing the effectiveness of an investigation, personal data can be legitimately collected without the person concerned being aware. However, such opacity can only be justified for a limited period and never beyond the duration of the investigation. A person who is no longer a suspect should be informed of the details of the data recorded (nature of data collected, file name and use). In addition, all data stored should be deleted at the end of the investigation.

The proliferation of police files and their expansion

Police files have multiplied in volume over the years, with the collection of DNA, fingerprints, information on immigrants, foreign residents and individuals involved in a police investigation, etc. In addition, we leave traces everywhere, including on the sites concerned by an investigation: hair, fingerprints, etc. Mere presence can be recorded by video surveillance cameras. There is therefore a significant possibility of being temporarily suspected, as well as being recorded in a police file.

The vast possibilities of error

These errors are due to several factors: files not being updated during or after the investigation (person exonerated but still recorded as "dangerous" in a police file), data recorded incorrectly (e.g "author" instead of "victim "or "witness" of the offense!).

These errors become difficult to correct as they propagate throughout the different overlapping between police files, or with justice files and also with European files. For instance, the national files that contain the fingerprints of foreigners supply the European Eurodac system and some databases of suspected terrorists supply the Schengen Information System (SIS II); therefore, errors are passed on automatically.

The impact of centralization at European level

European systems, founded on increasingly advanced and intrusive technology, lead to increasingly widespread surveillance. The centralization of these systems presents an additional risk caused by discrepancy between the reason for the data collection and the actual use made of it.

PERIOD OF DNA DATA RETENTION BY THE POLICE:

Country	storage life in files
Hungary	20 years for suspects of serious crime and their connections
France	25 years for suspects, 40 years for persons convicted
United Kingdom	indefinitely for DNA data collected before 2012. Since 2012, from 2 to 5 years

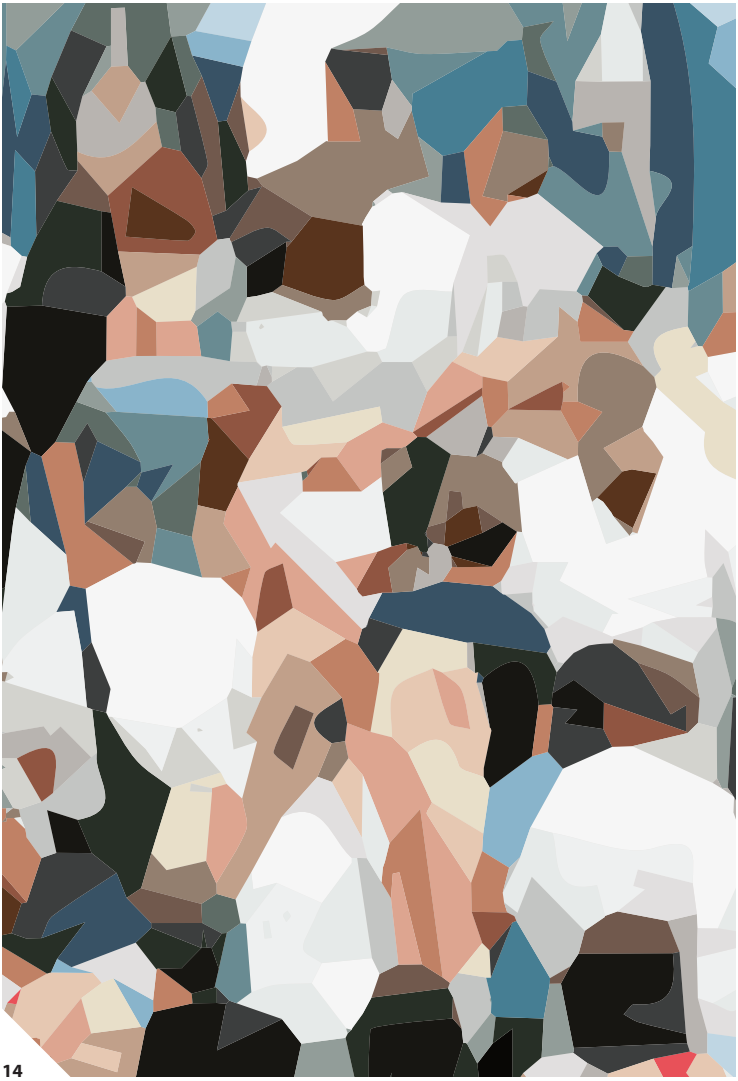
OUR RECOMMENDATIONS

AS A CITIZEN, MAKE SURE THAT:

- Citizens are adequately informed of the collection and storing of their data. This is necessary given the complexity of police files, the expanding scope of their collection and their wide dissemination;
- Citizens have the possibility of appealing to the authorities in charge of the files, appealing to the judicial authorities or bringing a complaint to the data protection authority, so that their data can be corrected or deleted;
- The data is compartmented so that anyone who consults the files only has access to the data they are seeking (compliance with the principles of proportionality and specified lawful purpose);

  DNA data of protesters and political activists are not collected and archived in the same manner as those of criminals;
- The data protection authorities review the criteria fields in the police files before they are created, and also regularly verify the practices and compliance with rules of operation, specifically in terms of updates and secure access;
- The collection of biometric data for secure ID documents is distinguished from the data collected during police investigations. Although the cross-referencing of this information does increase police effectiveness, it also increases the risk of miscarriages of justice.

If you believe your personal data has been recorded in a police file for any reason whatsoever, as a suspect, victim, simple witness of an offense, protester, etc. Inquire about the collection of your personal data in police files. Make sure the data recorded is accurate and also if it is legitimate that this data is still recorded in a police file!



GOVERNMENT DATA COLLECTION

Are people at risk?

Purpose and dangers of the files

PURPOSE

The protection of society, which is the basis for legitimate justice files, must not, under any circumstances, infringe on fundamental rights such as the right to work, the right to free choice of a professional activity, the right to the protection of personal data and the right to privacy.

Files administered by the courts are various. Criminal records, which contain the definitive convictions of a citizen, are the most common in European countries. There are also files classed by offense, ranging from homicide to traffic offenses, as well as files related to genetic and biometric information which, when shared with the police, facilitate collaboration between the police and the judicial system.

DANGERS

Offenders are not the only ones affected by these files. Being a witness or suspect during the time of the procedure is sufficient to be registered in these databases without being clearly informed. It is then difficult to take action.

In addition, these files are not free from errors that may result from the entering, filing or transmission of this data.

It is possible, however, to exercise the right to verify the information contained in these files. It is then necessary to make a request to the competent authority to correct data or to check that the data that can be removed has been.

Furthermore, these files can be used for other purposes than those

required for justice. For example, we are requested to provide criminal record information to access some jobs: this is a source of danger to the person, though in many cases it is neither useful, necessary nor required!

Exchanges between countries:

ECRIS - European Criminal Records Information System

ECRIS is a European system for exchange between the Member States of information on the convictions of their nationals. However, national laws differ: a punishable act in one country will not be in another country, or not in the same way. Moreover, information on convictions is subject to different processing and different archiving periods between states. Therefore, exchanges can lead to discrimination, distortion, and increased inaccuracies caused by automated translations.

How does ECRIS work?

The rules that apply are those of the Member State where the conviction is delivered (for the definition of the offense and the retention period). If the convicted person is a non-national in the State in which the conviction takes place, this State must transmit the information on the sentence to the State of origin. The latter will be responsible for recording information in the criminal record of the person and sending this data to any Member State requesting it.

Lastly, when you apply for a job, your criminal record may be requested by the employer. This request may be systematic irrespective of the position sought, or limited to specific professions. However, the terms of the request and the information provided vary from one State to another. The criminal records office may disclose the entire record or just an excerpt containing the most severe offenses or those likely to have an impact on the position sought. Again, these exchanges, which are not always necessary, can cause discrimination due to the different rules and practices between Member States.

WORTH KNOWING:

If you request someone's criminal record (if you are an employer, for example), you should be aware that the information received should not be a barrier to reinsertion, nor a monitoring or discrimination tool.

As a resident in a European country, you have rights:

- The right to information about the content of the criminal record
- The right to privacy: files and data recorded therein must comply with the principles of necessity and proportionality to the objectives
- In the event of errors, the right to appeal to the judicial authorities or the possibility of bringing a complaint

In some countries, the employer may request criminal records within a framework provided by law. France and Luxembourg are exceptions because no legislative framework governs the request for a criminal record.

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

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

HU, 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.

SCAN TO CHALLENGE YOUR KNOWLEDGE

NO DATA WILL BE STORED

QUARTR -Design CRÉATONE - Paris