GOVERNMENT DATA
INS COLLECTION

Are people at risk?

GOVERNMENT FILING IN 14 EUROPEAN STATES

Do you know in which files you are likely to be registered?

EDUCATION

Pupils and students are likely to be registered in national files for which the claimed purpose is the management of schools and services that are provided: management of subscriptions and services… The objectives claimed do not always justify the saving of data on health, origin, tongue of parents, and even religion. These kinds of data are however saved in some of the countries we studied. Thus, the principles of proportionality and necessity are breached. Often, the consent of parents or pupil is not requested. Lastly, the retention of data often lasts well beyond what is necessary. Thus, a misstep can pursue a pupil during their whole life.

HEALTH

Most of the studied countries implement medical files for the good management of health systems. The different systems of access to medical data (rather the patient can choose whether to create or not a personal medical file; or the patient can hide or not some data; or the patient can allow access or not to different professionals) jeopardize medical secrecy. The centralized management and the inadequate anonymization in case of statistical use make us fear breaches of privacy and personal data protection.

POLICE

The number of police files is huge in all the studied states: files of wanted persons for infringements or because they are suspected to support or to be part of terrorist organizations, DNA databases… All these files may contain mistakes. The lack of regular updating may have serious consequences, like discrimination, when they are consulted by different players, essentially potential employers. Furthermore, it is often difficult, even impossible, for citizens that have been unfairly filed to obtain the correction or deletion of their data.

JUSTICE

In all studied files, there are criminal records. If their use seems necessary for the good functioning of justice, the fact that employers and different players have access to many of the data they gather implies a risk of being discriminated in employment.
Other justice files exist and they also present risks of breach of privacy (files of offences, files of sentences, etc.).
.

Ligue des droits de l'Homme
FONDÉE EN 1898

aedh FIDH

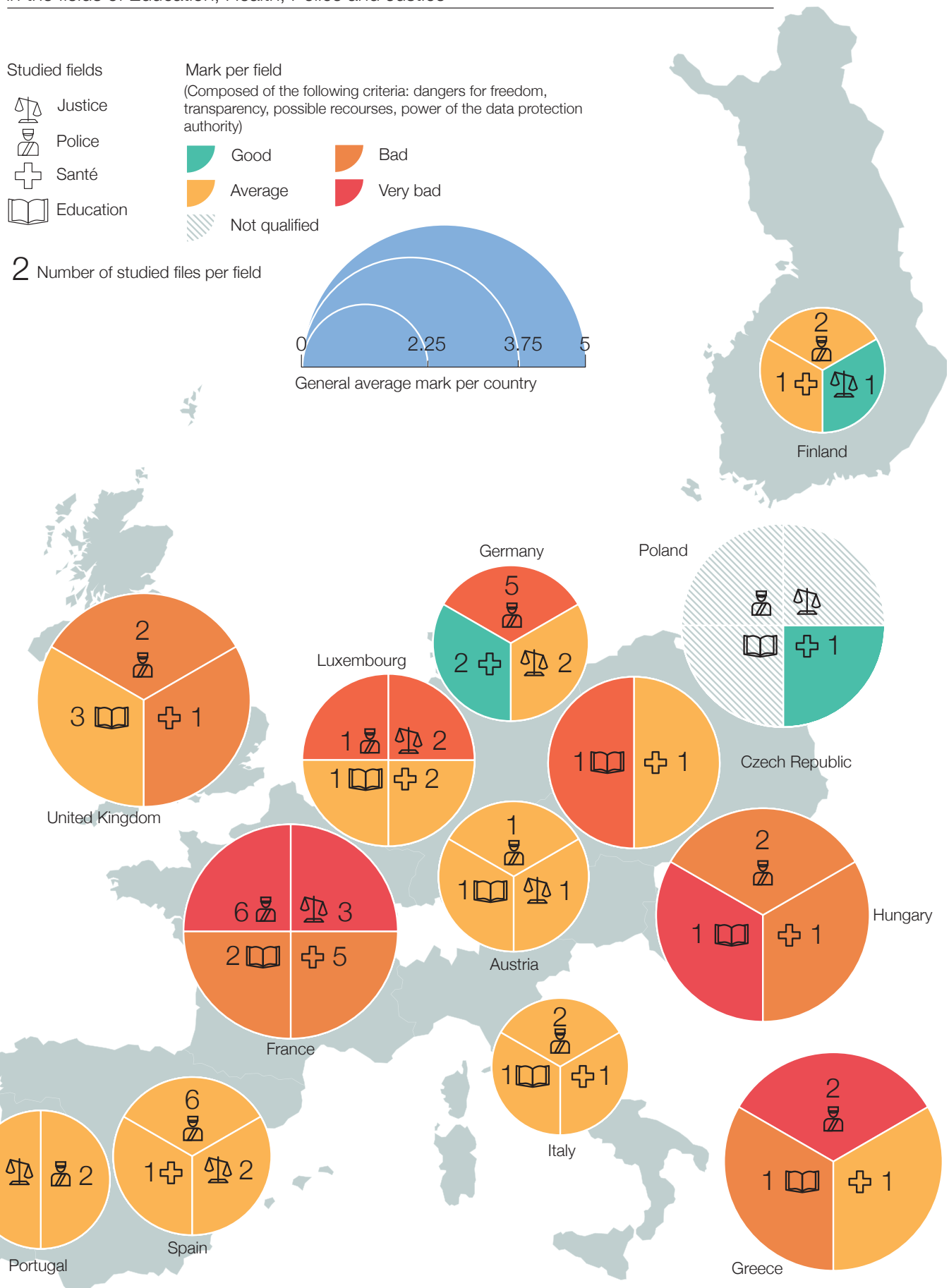
Humanistische Union

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 filing
in 14 European states
in the fields of Education, Health, Police and Justice



CONNECTIONS WITH THE EUROPEAN SYSTEMS

The data provided by Member States for the systems SIS II, VIS and Eurodac are fed by files collecting these data at national level.

Schengen Information System II (SIS II)

SIS II gathers biometric identification elements of missing persons, wanted persons (so as to extradite them, judge them…), persons under surveillance and identification elements of stolen items and cars. This system arouses an abundance of fears, especially concerning its high technological capacity requiring very good skills, its practical purpose which is to reject "foreigners", and the fact that people do not know they are registered in SIS II.

Eurodac System

Eurodac enables the identification and control of asylum seekers and illegal immigrants on the EU territory, persons highly vulnerable, through the comparison of their ten fingerprints with those saved in the system. This system is supposed to "efficiently" implement the regulation indicating which State is responsible for the examination of an international protection request (Dublin III Regulation). Eurodac is by now accessible to police authorities and to Europol, stigmatizing this group of people already vulnerable.

VISA INFORMATION SYSTEM (VIS)

Visa information system (VIS) is aimed at identically controlling in EU states the entrance in the Schengen area of foreigners subject to visa requirement, and targeting those who would "forget" to leave at visa expiry. This system is based on the comparison of biometric data, especially the ten fingerprints gathered in the system with those of the visa applicant.
It contains biometric data (prints, photo) and biographic data (name, job, expected duration of stay, goal of the travel…). The ten fingerprints are saved for five years for a visa that lasts only 3 months.

EUROPEAN CRIMINAL RECORDS INFORMATION SYSTEM (ECRIS)

ECRIS was implemented in order to facilitate the cooperation between judicial authorities of Member states with a view to exchanging information within criminal investigations and judicial procedures.
ECRIS is not a centralized database at European level. It organizes the consultation of criminal records from a Member state to another one. However, exchange of data is made in a framework where the definitions of crimes and offences, the inscription of convictions in records and their access are not the same in all European countries. Therefore, it could lead to discriminations.

How to protect your personal data?

Personal data processing shall not involve a violation of the right to privacy. Basic principles must be respected, such as the principles of finality, proportionality, and loyalty. If you think you may have been unfairly registered in a file, you can address to the owner of the file or, in some case, to your data protection Authority (DPA, see their name and address on the following page).

DATA PROTECTION AUTHORITIES

Austria: Österreichische Datenschutzbehörde / Austrian 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 Länder
www.bfdi.bund.de

Greece: Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα / Hellenic Data Protection Authority
www.dpa.gr

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 on files of the Police, Customs, Intelligence Service, Army and Justice (see Article 17.2 of Law of 2 August 2002).
www.cnpd.public.lu

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

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

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