PUBLIC CONFERENCE

Filing, Inform Citizens: Passport for the Protection of Personal Data

- Report

9 April 2014 held at the European Economic and Social Committee – Brussels

Opening Speech

Mr Peter MORGAN - EESC INT Section Vice-Chairman

Regarding the regulation proposal on data protection, standards are higher and there are more powers to the regulator. The focus, in the 2012 opinion, on the effectivity of the framework is positive. However some elements must be reconsidered (i.e. child protection, organisation of one-stop-shop). What can be noticed today is that data created by individuals get into public domain. Data can be uncontrollable.

Presentation of the project and of the communication tools

The project is innovative as it focuses on **data collection in the public sector**, a topic which is poorly studied. Therefore, an inventory was led covering 14 EU countries* and the EU level information systems with the objectives **to inform and raise awareness among citizens** on public data collection in the fields of police, justice, health and education. The idea is to inform them on the use made of their personal data, the related risks of the use of these files, the appeals available in case of misuse of their data and the roles of Data Protection Authorities (DPAs). Equally, the objective is **to inform decision-makers on the findings.** The inventory has been followed by the creation of analytical tools (14 monographs so one per studied country, an analysis of European information systems – SIS II, VIS, EURODAC, ECRIS - and a comparative overview of these practises). Resulting of the previous stages, two communication tools were created: a quiz available on the partners' websites and a "passport" informing about the risks associated to these files. Finally, the project includes a dissemination stage through the organisation by the partners of press conferences (or events) and training (or information) sessions. The dissemination will also include communicating to a wide audience by using the communications tools as well as to policy makers and Institutions through a more targeted communication.

**** The countries studied are:*** *Austria, Czech Republic, Finland, France, Germany, Greece, Hungary, Italy, Luxembourg, Poland, Portugal, Slovenia, Spain and the United Kingdom.*

Overview of the project findings and recommendations

Public data files in the field of EDUCATION in Europe and data protection

One of the specificities of educational files is that the **data subject is a minor.** However, data collected during childhood can impact **at adulthood**.

The education files studied for the project contain **sensitive data** such as disabilities, religion (e.g. Austria, Greece, Hungary, Italy), ethnicity, job and parents' level of incomes (e.g. Luxembourg). As such, people should be aware that misuse of educational files can lead to **discrimination** or **stigmatisation**.

The partners noticed that the **risks** often lie **in the use of the files** and **the implementation of the law** and not in the law itself, but also in the **level of centralisation** of the data which differs from one country to another. Several other risks were identified such as the **length of data storage** (e.g. unlimited retention period in the UK) and the lack of **anonymization**.

Recommendations by the partners of the project:

- ➔ Data **should not be identifiable** at national level.
- ➔ **Data storage should be limited** and **less sensitive data should be used**.
- ➔ **To oblige Institutions to inform** both students (including at higher level education) and their parents on data protection and on the internal systems.
- ➔ **The need to raise awareness** among people on data collection in the education field.

Public data files in the field of HEALTH in Europe and data protection

Health data are **collected for different purposes**: to increase the effectiveness of public health services, to improve the coordination between practitioners, for a better follow-up of patients cares or to monitor the health status of the population. **Data access** differs from one country to another: it can be given only with the patient's consent; medical record can be open only upon patient's request; access can be made by electronic cards. Besides, having medical records can be compulsory and files can be centralised in national databases.

Observations: the data are not properly **anonymized** and the **data access** is too widely open while these accesses are not traced. There is a risk of **discrimination** (refusal of bank loans, denial of employment, higher rates of insurance…) or **potential violations of medical confidentiality** as well as a **risk of loss of trust** between the patient and the practitioner. The data storage can be risky (use of cloud, centralised databases…). There is a potential risk to breach the **patient's freedom of choice** (e.g. Finland is about to end paper prescription) as well as interconnection risks related to the use of a single multipurpose national identification number.

Recommendations by the partners of the project:

- ➔ **Restrict the use of electronic medical records** only for patients who require expensive, heavy and long-term treatment and give the choice to other patients (paper prescription…);
- ➔ Give the choice to **patient to decide who can access his/her data and which data**
- ➔ **Patients should be informed** that their medical data are recorded and that they need to provide explicitly their **consent**.
- ➔ Archived data must be protected by specific measures, including **encryption**.
- ➔ Banks, insurers, employers and laboratories **should not access centralized databases**, and no data should be transmitted to private companies regardless of the purpose.
- ➔ The data used for statistical purposes must be anonymised and the operations irreversible.
- ➔ Before any implementation, all data systems must be reviewed by independent studies.

Public data files in the field of JUSTICE[1] in Europe and data protection

The files studied are of **various** types. The most common one is the **criminal record.** There are also **fingerprints and biometric files** which are shared between the police and justice actors. Some of them intend to facilitate the functioning of criminal proceedings (e.g. CASSIOPE for France and some Spanish files). Some files are not judicial ones but contain judicial information. When shared (for example with police, customs, the Ministry of Interior), some of these files can exceed justice power's remits. These databases can also be used for **scientific research**.

The **European Criminal Records Information System** (ECRIS) is a decentralised information technology system and not a database which aims at creating a **standardised European format** of transmission of information on convictions. **Several problems were identified**, such as the absence of standardization of infringements, the national criminal records systems are different (i.e. different issues regarding their possible access by judicial or police authorities, by convicted persons themselves, by third parties) and the correspondence tables are unclear while Member States did not translate their national offences.

Several fundamental rights are under threats: rights to **privacy**, to **personal data protection** (i.e. some countries register in the criminal records the names of the parents or the guardianship of the convicted person), to **work**, to **free choice of employment**, to **not be discriminated**, to **social rehabilitation** (i.e. candidates for employment may be required to provide an extract from their criminal record), to **equality** (i.e. ECRIS concerns EU citizens and not third countries nationals, an extract of criminal records can be less comprehensive for an employer who is not from the country of the candidate making it unequal for another candidate of her/his country).

Recommendations by the partners of the project:

- ➔ The right of access of data subjects should be improved: **they must know the complete content of their criminal record** (i.e. including entries limited to the court)
- ➔ **Monitoring the access and use of the data**: established protocols for data item transmitted to third parties (i.e. the cases of Germany, Austria, Finland) should be generalised in all States as well as consultations should be recorded (absent in Luxembourg).
- ➔ **Ensure the effectiveness of the action of the DPA when persons appeal to them**

POLICE public data files in Europe and data protection

Files with different purposes can be included in this field **which encounters several issues.** Data collections are **made at a large scale** and include a **very broad range of data**. Besides, the data can be **shared at the European level**. Mistakes at national level lead to mistakes at the European one. In addition, the **length of data storage** can be criticized. In the UK, the storage was unlimited until it has been decided that the storage for unconvinced persons was not justified[2].Therefore, the **principle of**

[1] For the project, are considered justice files the ones managed by Justice Courts.
[2] Since 2012.

proportionality is threatened. The issue of the **consent** is also at stake. A database cannot be legitimised simply because the data collection is consented (consent can be given under pressure or under threat). There is also a high degree of **lack of transparency**, notably in the *German Counter Terrorism Database* as data are shared between the police and intelligence services which for the latest, not very transparent. The **inclusion criteria** are also a matter of concerns. In Germany a single suspicion could cause the registration in the database, but this practice has been limited by a judgment of the Constitutional Court[3]. Regarding, **DNA files**, in **France**, one database was originally designed to identify sex offenders, but its scope has been expanded and now applies to protesters and thieves. **Fingerprints** can be recorded including for **precautionary reasons**. They are normally collected for **administrative reasons**, but some countries use them to build a **database**.

Recommendations by the partners of the project:

- ➔ Informing citizens: **of the extent of police databases** in Europe, they do not only concern criminals and there are possibilities of mistakes that could lead to **discrimination**.
- ➔ **A close eye must be kept on these files**
- ➔ A **regular monitoring of the use of these information** should be made. In Spain, there are **forms that facilitate access to data**, this practise should be implemented in all Member States.
- ➔ **Access to personal data** and **possibility of correcting them** must be facilitated
- ➔ Ensure the possibility of **access to justice** and **to lodge a complaint** (anti-terrorist purpose cannot justify every data collection)
- ➔ Collection of genetic and biometric data for ID documents and the collection performed during police investigations must be **separated**.

Panel: Improving data protection and the European legal framework

Mr Dimitrios DROUTSAS, *Member of the European Parliament*

The final proposal of the European Commission of **two legal instruments,** and not **a single one** for the reform of the Directive 1995 is regrettable as the Member States actually do not want any change in the public sector when it comes to personal data protection. The European Parliament took advantage of the "Snowden effect" to send a strong message to the national governments **in October 2013** (at the LIBE Committee) and in **March 2014** (at the Plenary Session) by voting the « package » of the data protection reform **before the end of the legislative mandate** of the European Parliament. The work of the European Parliament was constrained by a **heavy lobbying** and the Member States acted in a **counter-productive way**. Now, the negotiations process is in the hands of the Council, and **Member States are lagging behind**.

Three principles must be highlighted:

- Strengthening further the **rights of the individual**

[3] http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg13-031en.html.

- Take care of **entrepreneurship**
- To **be really strict against the "giants"**, those who can really play with citizens' data. There would be **sanctions** and **fines** against firms that infringe the regulation.

Mr Peter HUSTINX, *European Data Protection Supervisor*

Data protection is part of the **Lisbon Treaty** (Article 16[4]) and the **Charter of Fundamental Rights of the European Union** which is binding for all institutions and the Member States.
The European Court of Justice (ECJ) delivered on 8 April 2014 **two judgments** (on DPA independence and on the invalidation of the data retention Directive) that have an impact on European law and national legislation regarding data protection and fundamental rights. These cases highlight the **limits** of what can be done by the European legislator when it does not respect fundamental freedoms principles. Now, the Commission may make a **new and improved proposal** of a data retention directive which limits may be set by the judgment. Unfortunately, a decision made by the ECJ is not enough. An agreement on a new framework is needed. Regarding sanctions, former rules must be implemented; there is a need of more obligations, responsibilities, control and supervision. We need to think at the level of the European continent since internet does not stop at the borders of the 28 Member States.

Ms Marie-Christine VERGIAT, *Member of the European Parliament*

It is good news that the partners are trying to **educate on the topic of data protection** since there is a **lack of information on the matter**. There is currently an important debate at the European Parliament about the **EU / U.S. agreements**. We had the opportunity to put pressure on the U.S. and force them to respect the rights of European citizens, but the European Parliament did not take the chance. The **legislation on data protection that the European Parliament adopted in March is on the right tracks**, but Member States are lagging behind. The **ECJ decision of 8 April** is important as there are **important issues** around this matter.

Ms Irina VASILIU, *Policy Officer Data Protection Unit, European Commission*

In 2012, the Commission considered necessary to **recast the European framework for data protection to face technological and societal changes**. There was a need to cope with a **growing awareness on the part of individuals and businesses** added to a feeling of **loss of control** and **lack of transparency**.
In the new regulation, the logic of the Directive 95 was kept (explicit purpose, determined and adequate data collection). The principle of **transparency was added**, **the limitation principle is clearer** and the data controller **has a global responsibility**. The Commission proposal is to **strengthen the rights of individuals**: **consent** must be explicit, informed and free; the **right to information** (i.e. on data retention period, on right to complain, on international transfers) and the **right to data access** must be strengthened. Besides, the **right to be forgotten**, that was intensively discussed, should be ensured. The proposal has also **increased the responsibility** of the controller and its subcontractors. Their **obligations are clearly defined**: notification in case of data breach; to implement the concepts of privacy by design and privacy by default; obligation to make a prior impact analysis to treatments that involve risks; obligation to have a delegate to data protection in some situations. Finally, the role of **DPAs should be strengthened** and independence should be

[4] « Everyone has the right to the protection of personal data concerning them », Consolidated version of the Treaty on the Functioning of the European Union.

increased. Regarding the **Directive for police and judiciary authorities**, it concerns domestic and cross-borders data processing. The conditions and criteria are harmonised. **Special arrangements** are included to take into account the special nature of law enforcement activities, including a distinction between different categories of data subjects (i.e. witnesses and suspects) or between levels of reliability and accuracy of personal data. The **European Commission supports** the key principles of the European Parliament proposals voted in March 2014.

The data protection authorities and supervisory bodies: effective capacity to protect the personal data of the citizens?

Recommendations by the project consortium, addressed to supervisory bodies

- The negligence of the Member States is such that it is important to **review the control and the role of data protection authorities** because they are currently **inefficient**.
- They are **not transparent** and procedures to access them remain **unclear**. Citizens must have the means to enforce the law if it is not applied properly.
- The minimum requirement is that **they are politically, economically and financially independent.**
- DPAs must have **more resources**, and that they are **consulted** on any legislation. If this is not the case, they should at least have an *ex ante* role, i.e **be proactive and produce reports**.
- **Awareness is required for citizens and professionals**; **target groups** should be approached and **stimulating public debates** should be organized. DPAs must intervene in the field of **education** to train teachers and students on data protection.

Mr Wojciech Rafał WIEWIÓROWSKI, *Inspector General for the Protection of Personal Data for Poland*

DPAs are effective but DPAs' agents are aware that there have been a lot of criticisms from NGOs and institutions.

The size of a DPA differs from one country to another: the **Irish DPA** is one of the smallest DPAs, only 22 staff members, but it is one of the leaders in dealing with data protection since several big companies are settled in Ireland. **The Polish DPA is composed of 123 staff members** but the number remains the same since 2007 while **its amount of work has increased** (i.e. two times more complaints, four times more requests for texts interpretation, more areas of work covered). **There is a lack of means** (financial and human means). Apart from the Article 29 Working Party, DPAs cooperate in several other groups (i.e. Working Party on Information Security and Privacy, Global Privacy Enforcement Network). This cooperation can take the shape of a real legislation implementation or of a soft cooperation. We are currently moving from a soft cooperation to a new set with a stricter enforcement model, but there are still difficulties.

Mr Giovanni BUTTARELLI, *Assistant European Data Protection Supervisor*

The Directive 1995 reform package should give a **clearer definition** of the **notion of personal data** and the vote of the European Parliament goes in that direction.
The decision of the ECJ states that the collection of information and data traffic interferes with the right to privacy. Therefore measures must be taken no matter what access law enforcement bodies have. It must be ensured that the processing of personal data is **transparent**, even for surveillance activities, and actors should be accountable. **National security** should not only refer to what is completely national but include the notion of "**third countries**". The **EU must find a way to intervene in this area** and rebuild **trust between the EU and the USA**.
A data supervisor must be **independent** as it has to be proactive, to translate requirements onto responsibilities and internal policies. Seeing its powers and duties, the EDPS has to be **selective**, as some complaints are not of general interest and answering them takes time. Every DPA needs to have **a programme which will be made transparent** and act in order to enhance its capacities. By making an inventory it must be clear in which areas supervisory bodies can intervene in which fields they can act and in which fields they can not.

Elements for the future:

- To adopt a regulation that **permits supervisory bodies to be competent in cross-border cases**: coordination process must be engaged, it is the DPA of the main concerned State main which will take a decision in agreement with the other DPAs.
- Supervisory bodies' **independence should be strengthenedµ**

A review of the legal framework that will apply to institutions will be submitted to the European Parliament and the Council for approval (around June 2014).

Closing speech

by *Mr Georges DASSIS – EESC Group II Chairman*

At the European level, we must **push for a Europe that goes back to its core values** whose Human Rights belong to. It is regrettable that there is **no real European policy on data protection**. The directive is good but it is not enough. **Member States must agree on definitions**. The EESC acts and influences the European Commission to fulfil its role of initiating legislations. The EESC **demand that citizens have the possibility to go to the Commission** to complain and that the Commission should be obliged to respond these requests.

For further information: info@aedh.eu

An event hosted by

European Economic and Social Committee

Project co-financed by
Directorate General Justice