EUROPEAN DATA PROTECTION SUPERVISOR

PRESS RELEASE

Monday 13 March 2006

Interoperability of databases: EDPS raises concerns on principal issues and calls for a better analysis

The European Data Protection Supervisor (EDPS) has issued comments on policy options for the interoperability of databases in the area of Justice and Home Affairs, as presented in a recent Communication of the European Commission. Although not properly defined in the Communication, it is clear that 'interoperability' raises a number of questions in relation to data protection which need a better analysis. The EDPS also strongly discourages the use of biometric data, such as fingerprints - or perhaps even DNA - as a unique identification key. The accuracy of biometrics is overestimated in this respect and it will facilitate unwarranted interconnection of databases.

Peter Hustinx, EDPS, says: *"The Commission argues that interoperability is a technical rather than a legal or political concept. This is confusing and only serves to avoid fundamental issues. Interoperable systems increase the risks for citizens, if such systems allow for new access to their personal data. It is essential to examine this more carefully and not hide it as a technicality".*

In his initial comments to the Communication, the EDPS underlines that he needs to be consulted on any legislative proposals that may stem from it. He also makes some specific observations, such as welcoming the Commission's analysis that there shall be a much higher threshold for access when internal security authorities query databases in other domains than when they query criminal data bases.

The EDPS regularly issues opinions on proposals for legislation that relate to data protection. When necessary, the EDPS also reacts to other related documents, such as Commission Communications, because of their possible long term policy impact.

The comments are available on our website:
http://www.edps.eu.int/legislation/Comments/06-03-10_Comments_interoperability_EN.pdf

For more information, please contact the EDPS Press Service at: +32 2 283 19 00

EDPS - the European guardian of personal data protection

www.edps.eu.int

Comments on the Communication of the Commission on interoperability of European data bases

Brussels, 10 March 2006

Postal address: rue Wiertz 60, B-1047 Brussels, Belgium
Office: rue Montoyer 63, Brussels, Belgium
E-mail: edps@edps.eu.int - Web site: www.edps.eu.int
Tel.:+32-2-283 19 00 - Fax:+32-2-283 19 50

Comments on the Communication of the Commission on interoperability of European data bases

The European Data Protection Supervisor (EDPS) has noted the publication on 24 November 2005 of the Commission's Communication on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs (hereinafter, "the Communication")[1].

The EDPS welcomes any initiative, such as this Communication, which aims to improve the efficiency of EU large scale IT systems, to better protect the fundamental rights of the individual and to stress the need for in-depth impact assessments related to the development of these systems.

The EDPS has however some concerns regarding this Communication, both general and specific, which are underlined in this document.

A. General comments on the concept of interoperability

This Communication focuses on technical and organisational aspects of the concept of interoperability. However, the EDPS does not fully share the view that "interoperability is a technical rather than a legal or political concept". Indeed, it is obvious that making access to or exchange of data technically feasible becomes, in many cases, a powerful drive for de facto acceding or exchanging these data. One can safely assume that technical means will be used, once they are made available; in other words, it is sometimes the means that justify the end and not the other way around. This can lead to subsequent demands for less stringent legal requirements to facilitate the use of these databases: legal changes quite often confirm practices which are already in place.

The EDPS regrets that the concept of interoperability is not given an unambiguous and clear meaning in this Communication. The debate on interoperability has not led to widely shared conclusions and the notion ought to be better clarified.

Interoperability is mentioned not only in relation to the common use of large scale IT systems, but also with regard to possibilities of accessing or exchanging data, or even of merging databases. This is regrettable since different kinds of interoperability require different safeguards and conditions. This is for instance the case when the concept of interoperability is used as a platform of other proposed measures aiming to facilitate the exchange of information. The EDPS opinion on the principle of availability[2] emphasised that although the introduction of this principle will not lead to new databases, it will necessarily introduce a new use of existing data bases by providing new possibilities of access to those data bases. This is one of the main reasons why the concept of interoperability has to be examined very carefully.

[1] http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/com/2005/com2005_0597en01.pdf
[2] http://www.edps.eu.int/legislation/Opinions_A/06-02-28_Opinion_availability_EN.pdf

Moreover, this Communication intends to propose new objectives for large scale IT systems which go beyond their original purpose and will therefore automatically require a new and complete analysis of their impact on the protection of personal data. In this context, the EDPS stresses that interoperability of the systems must be implemented with due respect for data protection principles and in particular the purpose limitation principle. Any limitation to the principles of data protection shall constitute an exception and shall only be implemented subject to strict conditions and with the necessary safeguards, technical or otherwise.

These considerations confirm once more the clear need for a legal framework on data protection in the third pillar that is fully consistent with the principles of data protection under the EC Treaty and that is applied effectively to guide developments such as those discussed in the Communication. In the following paragraphs the EDPS will address the main questions arising from the Communication. Other related questions have been addressed in his previous opinions on Access to VIS[3] and Data protection in the Third Pillar[4].

The EDPS is available to provide further guidance on concrete proposals and expects to be consulted in any case where Commission action stemming from this Communication, falls within the scope of Article 28 (2) of Regulation 45/2001.

B. Use of biometrics as primary key

1. One of the basic components of a database is a unique number also defined as a primary key and produced for every item on which information is gathered and stored. As an illustrative example, the number of the visa sticker which will be a part of the future VIS might be used as a primary key and all the information collected for a visa application will be linked to this unique number. This primary key is usually seen as a critical feature in the interoperability of databases, as the way these keys are defined varies from one database to another. Restrictions on the sharing of primary keys are often used as an efficient data protection tool. Interoperability is still possible in this case, but only if implemented through a less direct and better supervised process.

   The use of biometric data, such as fingerprints or perhaps even DNA, as a primary key is promoted in this Communication. According to the EDPS, this use would not be compatible with the delicate balance referred to in part 2.1 of the Communication. These kinds of primary keys will offer the possibility to merge two and more databases in close to real-time and with very little effort. As it has been stated in the study for the Extended impact assessment of the Visa Information System[5], in a report commissioned by the European Parliament[6] as well as in previous opinions of the EDPS[7], biometrics are based on probabilities

[3] http://www.edps.eu.int/legislation/Opinions_A/06-01-20_Opinion_access_to_VIS_EN.pdf
[4] http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2006/c_047/c_04720060225en00270047.pdf
[5] Study for the Extended impact assessment of the Visa Information System, EPEC final report, December 2004
[6] Study commissioned by the LIBE committee of the European Parliament, *Biometrics at the frontiers: assessing the impact on Society*, February 2005, Institute for Prospective Technological Studies, DG Joint Research Centre, EC.
[7] http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2005/c_181/c_18120050723en00130029.pdf http://www.edps.eu.int/legislation/Opinions_A/05-10-19_Opinion_SISII_EN.pdf .

and will not deliver the unambiguous key that is by definition required for primary keys of databases. This is likely to result in a breach of the principle of data quality.

2. Some of the potential scenarios described in this Communication envisage a pool of EU databases or even, in the case of fingerprints or DNA, of Member States databases. With these prospects, the aim of this Communication shifts from the notion of interoperability between databases to the concept of interconnected databases.

   Technically allowed and catalysed by the use of biometric data as primary key, a new trend emerges. This trend, illustrated by very different projects like the Prüm Convention and the future European driving licence database, will lead to decentralised systems consisting of constellations of databases which will work more like peer to peer networks than centralised systems. The fact that the primary key can be generated *naturally* (in the case of biometric data) and is not produced by each system (in the case of a unique identifier) will also facilitate the growth of this pool of databases with the addition of a great diversity of databases using the same easily and freely accessible primary key.

   This aggregation of databases also increases the risk of "function creep" when the interlinking of two databases designed for two distinct purposes will provide a third one for which they have not been built, a result which is in a clear contradiction of the purpose limitation principle.

   This trend will eventually be detrimental to the harmonisation of personal data protection rules in the EU. In particular, it will affect a harmonised implementation of data protection rights, by lessening the possibility of an effective and consistent supervision at both the EU and member states levels.

C. Specific comments

1. It is regrettable that the protection of personal data has not been explored sufficiently as an inherent part of the improvement of the interoperability of relevant systems. The EDPS suggests adding to this Communication a more consistent analysis on data protection, including privacy-enhancing technologies to improve both effectiveness and data protection.

2. The EDPS agrees wholeheartedly with the Commission's view that under-exploitation of existing systems is regrettable, and that a better use of those systems is a priority. Before creating new databases or new functionalities, investments should be made in ensuring full use of already existing databases. The EURODAC inspection recently conducted by the EDPS with the cooperation of the Commission's services aims not only at supervising the proper use of the central system but also at providing recommendations for improving its protection and its efficient use.

3. The Communication calls for better coherence as regards input of data categories in information systems, which is to be welcomed. For instance, the harmonisation of criteria for alerting individuals in SIS II also serves the interests of the data

subject in increasing the legal certainty. This is recommended in relation to alerts on unwanted aliens in the EDPS opinion on SIS II[8].

4. The EDPS addressed the access of law enforcement agencies to VIS data in an opinion issued on 20 January 2006[9]. He welcomes the Commission's analysis in point 6 that the threshold for authorities responsible for internal security to query databases which register "innocent" people should be much higher than the threshold for querying criminal databases. This is certainly supported by the EDPS should new instruments on access to these databases be proposed. It is an element which the EDPS will carefully analyse when needed.

5. As to the existence of an entry-exit system of third country nationals, it should be noted that the Extended impact assessment study[10] concerning the establishment of the VIS rejected the idea of such a system, in favour of the one which is proposed today. If the Commission intends to change its approach to this subject, it would entail the need for a new impact assessment strongly justifying why an option discarded one year ago (i.a. for its "extensive impact on human rights") is now considered desirable.

6. The management of the systems by a "single organisation" as referred to in the EDPS opinion on the VIS constitutes a great challenge which will only be addressed with an exhaustive and clear description of its tasks supported by proper resources.

7. It is regrettable for such a sensitive document that the concept of Automatic Fingerprint Identification System (AFIS) is wrongly described (part 5.3.1) as a combination of "all fingerprint data currently only available...". It is a (software) tool for identification, not a database in itself. On the other hand, the concept of AFIS is properly used as a good example in part 5.4 related to architectural and organisational changes.

8. The brief demonstration of the proportionality principle on DNA is incomplete and cannot lead to a *simplistic* conclusion that this principle will be respected. The purpose of the storage, its duration, the condition of access, etc. shall also be taken into account in the analysis of this principle. As already said, the EDPS strongly advises against using biometric data, and in particular DNA, as a primary key for these databases, considering the risks presented by this option. Some general requirements for legal instruments laying down exchanges of DNA data are also suggested in the EDPS opinion on the principle of availability. These requirements have to be taken into account in the present context as well.

Done at Brussels on 10 March 2006

Peter HUSTINX
European Data Protection Supervisor

[8] http://www.edps.eu.int/legislation/Opinions_A/05-10-19_Opinion_SISII_EN.pdf
[9] http://www.edps.eu.int/legislation/Opinions_A/06-01-20_Opinion_access_to_VIS_EN.pdf
[10] idem as 4