Preliminary Comments of the European Data Protection Supervisor on:
- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Preparing the next steps in border management in the European Union", COM(2008) 69 final;
- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Examining the creation of a European Border Surveillance System (EUROSUR)", COM(2008) 68 final;
- Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Report on the evaluation and future development of the FRONTEX Agency", COM(2008) 67 final.

I. Introductory remarks

I. A. The Communications and their relevance for the EDPS

The European Data Protection Supervisor (EDPS) has noted the publication on 13 February 2008 of three Communications from the Commission in the field of integrated border management:

1. The Communication "Preparing the next steps in border management in the European Union" puts forward suggestions for new tools that would form an integrated part of the European border management of the future, including:
   - proposals for the introduction of an entry/exit system, allowing the electronic recording of the dates of entry and exit of third country nationals into and out of the Schengen area;
   - proposals to facilitate border crossing for bona fide travellers, through the introduction of automated border crossing facilities for EU citizens and certain categories of third country nationals;
   - parameters for the possible introduction of an Electronic System of Travel Authorisation (ESTA).
2. The Communication "Examining the creation of a European Border Surveillance System (EUROSUR)" examines the parameters within which a European Border Surveillance System, focussing initially on the southern and eastern external borders of the EU, could be developed. It suggests a roadmap to Member States for gradually developing such a "system of systems" over the coming years. This Communication focuses on enhancing border surveillance, in particular in order to detect, identify, track and intercept persons attempting to enter the EU illegally outside border crossing points.

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 63
E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

3. The third Communication is a “Report on the evaluation and future development of the FRONTEX Agency”. It is less relevant for the EDPS since it does not mention processing of personal data.

The EDPS will address all three communications as a “package”; however, these comments will focus mainly on the first one since it is the most relevant in data protection terms. First general comments will be followed by more specific points (sometimes different for each Communication).

I.B. Purpose of the present comments

The EDPS certainly recognises the need for the development of a European model of integrated border management of the external borders of the EU. Improving management of migration flows and preventing illegal immigration and possible threats to the security of the EU, while facilitating border crossing for bona fide travellers, are all legitimate purposes.

On the other hand, several of the envisaged measures entail the processing of vast amounts of data, involving the collection, consultation and possible sharing or pooling of these data. The consequences of these processing operations may be far reaching for the persons concerned: *inter alia*, they may be refused entry to the EU territory and a great number may be subjected to more intrusive admission procedures at the border.

It is therefore crucial that the impact on the privacy rights of individuals concerned is adequately taken into account. A lack of data protection safeguards does not only mean that these individuals might suffer unduly from those measures, but also that the measures will be less effective, or even counter productive, by diminishing public trust in government action.

The EDPS advocates an approach whereby privacy is recognised as a significant factor in the achievement of the EU’s objectives. It involves the reflection of privacy concerns within the overall strategy, implementation of measures to adequately address privacy issues (possibly at a later stage when more precise proposals are put forward), and the integration of "privacy-sensitivity" in computer-based systems.

The present document is a selection of points the EDPS deems important in view of these objectives rather than an exhaustive analysis of the three communications.

II. General comments

II. A. On procedure

As underlined above, the envisaged measures (creation of an entry/exit system, registration of bona fide travellers, etc.) entail large processing operations of personal data, with significant invasions of privacy. It is thus very regrettable that the EDPS has not been consulted in the preparation of the communications or in the course of the impact assessment of the first communication. The national data protection authorities have not been consulted either. This gives the overall impression that this aspect was considered less relevant by the European Commission than purely technical aspects.

The EDPS expects to be consulted about any measures stemming from the communications and having an impact on privacy rights.

It should also be noted that the envisaged measures are in all likelihood going to be adopted after the entry into force of the Lisbon Treaty, with important consequences in terms of the involvement of institutional players. Therefore, full involvement of the European Parliament should be envisaged. It will also have consequences for the applicable law, with the lifting of the EU pillar structure. The EDPS welcomes these modifications which should ensure a better democratic participation and scrutiny in this important area.

II. B. On substance

1. Acceleration of proposals in this area

Regardless of the inherent merits of each proposal, the EDPS is concerned that far reaching proposals implying surveillance of the movements of individuals follow each other at an amazing pace. Many proposals have been or are about to be tabled in this area (SIS II, VIS, review of Eurodac Regulation, access of law enforcement agencies to these systems, PNR, etc.). All these proposed measures are intended to contribute to the monitoring of travellers before and upon entry to the EU (or Schengen) territory.

The sheer number of these proposals and the seemingly piecemeal way in which they are put forward make it extremely difficult for the stakeholders (European and national Parliaments, data protection authorities including EDPS, civil society) to have a full overview. This limits the possibility to contribute meaningfully. There is for instance a risk that Data Protection Authorities might find a proposal acceptable only to discover later that it would actually be unacceptable when considered in synergy with the other, more recent proposals.

The EDPS would like to see evidence that there is a master plan for all these initiatives, giving a clear sense of direction. Such a general plan would greatly help to analyse the impact of the totality of these measures on the travellers (in third countries, at entry or within the EU territory) and to design appropriate safeguards.

2. Lack of reliable evidence to support the need for new systems

Moreover, the need for such a massive volume of data collection in this area is not always supported by reliable data.

The impact assessment accompanying the first Communication repeatedly mentions that the figures it contains (rates of border crossings, number of illegal immigrants in the EU, number of persons entering the EU legally and overstaying their visa, etc.) are based on estimations or samples[1].

In other aspects, some bold statements are made, that are not based on undisputable evidence. The impact assessment study of the first communication[2] seems to establish a link between terrorism and illegal border-crossing. However, it also recognises that the majority of those refused entry are neither terrorists nor serious criminals, but only those without the appropriate travel documents. Therefore, claiming that an entry-exit system would

[1] Commission Staff Working document accompanying the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Preparing the next steps in border management in the European Union", Brussels, 13.2.2008, SEC(2008) 153, p.6.
[2] op.cit., in particular p.9.

significantly help reduce terrorism and serious crime may be more wishful thinking than reality.

The EDPS can readily admit the difficulties of gathering reliable data on phenomena such as illegal immigration or its link to terrorism. However, he underlines that in the absence of such data, measures taken to counteract these phenomena may be ineffective or inadequate and disproportionate. Heavy infringements on the privacy of individuals should be based on solid grounds demonstrating their need and with justification as to how extensive they should be. Whether the assertions made in the Communication would pass the test is doubtful.

3. Lack of evaluation of existing systems

The proposed measures also complement other systems already existing or planned. It should be noted, for instance that the entry-exit system will complement the VIS. However, the VIS is still far from operational. With a view to demonstrating the need for new measures, a thorough assessment of the effectiveness and weaknesses of existing databases should be conducted. The Commission should also rely on studies carried out in third countries about comparable systems in operation there.

The EDPS wants to draw the attention to the reports of the United States Government Accountability Office concerning the US-VISIT system. One of the most recent reports[3] expressed serious concerns about the prospects for successfully delivering an operational exit solution and underlined clearly the challenges of the building of such a system. Over 4 years, the American Department of Homeland Security has invested about $1.3 billion and delivered basically one-half of US-VISIT. Over the same period, US-VISIT has allowed to take action (including denial of entry) against a little more than 1.500 people. This suggests that the cost-effectiveness of such a system is not guaranteed and that economic aspects would also benefit from a careful consideration of experiences abroad.

Finally, an exhaustive privacy impact assessment for each new system would be absolutely necessary before any of these new systems are developed. An interesting methodology has been developed by the UK Data Protection authority in this respect[4].

4. Heavy reliance on biometrics

The entry-exit system as well as the ESTA proposal relies heavily on the use of biometric elements. Various reasons for this have been put forward: the use of biometric elements would enhance identification procedures, speed up border crossing, and would allow for easy interoperability between different systems. The Biometric Matching System is seen as the appropriate platform to realise this. The EDPS recalls some points he already underlined in previous opinions (VIS[5], SIS II[6] in particular) about biometrics.

Biometrics has some considerable advantages: data universality, distinctiveness, permanence, usability, etc. However, revocation of biometric data is almost impossible: the fingerprints or

[3] GAO, Testimony before the Subcommittee on Border, Maritime and Global Counterterrorism, Committee on Homeland Security, House of Representatives, June 28, 2007, "Prospects For Biometric US-VISIT Exit Capability Remain Unclear", GAO-07-1044T.

[4] http://www.ico.gov.uk/upload/documents/pia_handbook_html/html/1-intro.html

[5] Opinion of 23 March 2005 on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas, OJ C 181, 23.7.2005, p. 13.

[6] Opinion of 19 October 2005 on three Proposals regarding the Second Generation Schengen Information System (SIS II), OJ C 91, 19.04.2006, p. 38.

a face are difficult (but not completely impossible) to change. This positive characteristic from a number of perspectives leads to a major downside in case of identity theft: the storage of fingerprints and photographs in a database linked with a stolen ID could lead to major and permanent problems for the real owner of this identity.

It should also be reminded that the main advantages of biometrics are never absolute. This has a direct impact on the efficiency of the biometric enrolment and verification procedures planned. A certain percentage of persons concerned will not to be able to enrol (because they have no readable fingerprints or no fingerprints at all). In relation with the number of persons likely to be affected by the new systems foreseen by the Communication, this involves a considerable number of persons unable to enrol properly, with obvious consequences for the visa application and at the border checking.

In view of this, the development of the proposed systems (if realised) should allow for fall back procedures. They constitute essential safeguards for the introduction of biometrics as these are neither accessible to all nor completely accurate. Such procedures should be implemented and used in order to respect the dignity and the rights of persons who cannot successfully follow the enrolment process and to avoid transferring the burden of the system's imperfections onto them.

5. Interoperability and synergies between databases

The communication envisages synergies between the VIS, the entry/exit system and the Registered Traveller programme. It even considers a merging of the VIS and entry/exit databases.

The EDPS considers this as premature for the reasons mentioned above (points 1, 2 and 3), but also as inappropriate. While the EDPS agrees that databases must be put to the best possible use and that synergies may be envisaged for efficiency reasons, it must never be done at the cost of subverting the initial purpose for which data were collected and stored.

For instance, the VIS is a tool the main purpose of which is to implement the EU Visa policy and to fight visa shopping. An entry/exit system does not have the same purpose: it concentrates on the prevention of illegal immigration (when it is caused by overstaying). Therefore, the safeguards (such as those proposed by the EDPS for the VIS) may be relevant in one context but not in another.

For example, when databases are interlinked or merged, it raises questions about access to these databases. Law enforcement access to VIS could be legitimate under some circumstances and with specific safeguards. This does not mean that access to VIS merged with entry/exit would also be legitimate, since different categories of persons are concerned.

Therefore, when new systems are introduced, the legislator should make clear not only how they are going to operate, but also all the consequences they may have for existing systems, and allow the stakeholders (EP, EDPS, DPAs,…) to have a full overview.

6. Reversal of the presumption of innocence

The underlying assumption in the communications (especially in the entry/exit proposal) is worrying: all travellers are put under surveillance and are considered a priori as potential law breakers. For instance in the Registered Travellers system, only the travellers taking specific steps, through ad hoc registration and provision of detailed personal information, will be

considered "bona fide" travellers. The vast amount of travellers, who do not travel frequently enough to undergo such a registration, are thus, by implication, de facto in the "mala fide" category of those suspected of intentions of overstay.

This is contributing to an atmosphere of general distrust especially towards third country nationals, while it remains to be proved how significantly it will help in fighting terrorism. Such an observation has been made with regard to the EU-PNR system. Finally, it should also be noted that the intended measures may in effect be conflicting with the EU asylum policy, by deterring people to seek the protection they are entitled to in Europe under international rules of protection of refugees.

This is a delicate balance for the lawmakers to strike. These communications are part of a long series of proposals or measures intended to process data about innocent individuals. A broad reflection about this kind of proactive surveillance and its real usefulness in the fight against terrorism should be encouraged. The EDPS will further contribute to appropriate solutions, when presented with more precise proposals.

III. Specific points

1. Concept of overstaying: "Cart before the horses?"

The concept of “overstay” is central in the proposed entry/exit system. The main idea is to identify third country nationals who overstay their right to stay in the EU. This can certainly have positive effects. In particular it could deter third country nationals from overstaying because they would know that they are likely to be identified as overstayers automatically when their visa expires.

However, there is at present no consistent policy in Member States towards this phenomenon, in particular, no uniform sanction for this. At present, overstayers may be reported in the SIS under Article 96 of the Schengen Convention, with a view to be refused entry on the Schengen territory. This is probably seen as insufficient, hence the proposal for an entry/exit system.

However, building a large scale database without a consistent approach of the definition of an overstayer, of who is exempted under which circumstances (health, humanitarian,…) and of which sanctions could apply is problematic. It will categorize very different persons as overstayers. Individuals will not have enough legal certainty about what it means to be flagged as an overstayer. Developing a consistent policy towards this phenomenon would be a necessity.

2. Consistency with other systems

The Communication on Eurosur raises issues of consistency with existing systems. It affirms that it is not going to replace other instruments, but to make a better use of them. However, the communication mentions repeatedly that one of the aims of Eurosur is to help identifying illegal immigrants coming to the EU by sea. One can wonder how this identification will be realised. These persons can only be identified if they already have been in EU before (through Eurodac, SIS or VIS).

In this case, it is difficult to see what Eurosur will bring as added value to the systems in place. If the persons concerned have never been in Europe before, no database can help

identifying them. Therefore, it should be clarified whether a new database is envisaged or alternatively, what is meant by identifying.

3. Great number of officials with access

The communications advocate better information sharing or pooling without being specific about it. Although this is not unusual or inappropriate for communications, it also fails to highlight some obvious down sides.

Without entering into too much detail, the EDPS wants to underline that many envisaged measures would entail access to a great amount of information by a great number of officials, whether in third country consular posts, at border crossings or in immigration authorities. This is likely to make traceability of consultations difficult and can lead to security problems, as illustrated by an increasing number of reports of security incidents. Proper safeguards should be foreseen when access is granted to databases.

As far as law enforcement access is concerned, the Commission had expressed its view in a previous communication on interoperability of databases. The Commission said 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. The EDPS supported this analysis[7]. It is an element which the EDPS will carefully analyse when needed.

4. Supervision

Data protection supervision mechanisms must be put in place in an appropriate manner. The EDPS underlines the difficulty of supervising large-scale international, interconnected databases. The layered supervision model put in place for SIS II and VIS offers a valuable approach for this, but should be allowed some time to develop in practice and demonstrate its effectiveness.

Done at Brussels on 3 March 2008

Peter HUSTINX
European Data Protection Supervisor

[7] http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2006/06-03-10_Interoperability_EN.pdf