The Greens/European Free Alliance

An Emerging e-Fortress Europe? - Border Surveillance, Frontex and Migration Control

European Parliament, Brussels, 26 June 2012

Panel III: "Smart Borders", EU-PNR and Travellers' Surveillance

Peter Hustinx

European Data Protection Supervisor

Speaking notes

- Thanks for the invitation to address the most important data protection aspects of the various initiatives debated today.
- I would like to concentrate my remarks on **Smart Borders** and **EU PNR**.
- **EUROSUR** has also received our attention and we have issued formal comments in February 2012, stressing the need for specific safeguards when personal data are processed, which the rapporteur has taken into account.
- What do these initiatives have in common? After passing necessity and proportionality tests, they all share the need for specific safeguards.
- I want to refer briefly to how the Commission Communication on Smart borders, released in October 2011, is meeting data protection tests, and to the difficulties that arose during EU PNR negotiations with regard to privacy, and the way ahead from a data protection perspective.
- I welcome the release of the "Borderline" study presented earlier today. This is a good result of cooperation with academia, which allows a proper debate on this sensitive subject.

Entry/Exit System (EES)

- A few general remarks that could open the debate from a data protection perspective.

Assessment and evidence needed

- At this stage, there is a lack of reliable evidence to support the need for new systems. I understand the difficulties in getting such data, but nevertheless, the need for a massive data collection in this area should be supported by more reliable evidence.
- There is also a lack of proper identification of the impact on fundamental rights, including the right of each individual to have his/her personal data protected. This shortcoming should be addressed in the impact assessment that should accompany the legislative proposals – probably this fall – in line with the Union's stated commitment to fundamental rights.

Proper evaluation of existing instruments

- It should also be noted in this context that the entry-exit system is intended to complement the Visa Information System. However, even if this system is not fully operational, it introduces the obligation to register in the C-VIS the expiry date of the visa and information on extension granted of the same. The Border Code provides as well for the possibility of lawful stay of a foreigner on EU territory for no more than three months, thus requiring the stamping of the passport on exit. It is not clear which will be the impact of a new data system.

Law Enforcement Access

- The question of law-enforcement access and therefore the purpose of the system must be addressed. The purpose of the system has significant implications for its design. An EES purely designed to detect and deter overstay, would look different from one that is also meant to be used as a general law-enforcement tool to reconstruct e.g. travel routes. The principle of purpose limitation is one of the key notions of EU data protection law and its jurisprudence. It states that personal data must only be "*collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes*" (see Article 6(1)(b) of Directive 95/46/EC).

Retention periods

- The subject of retention periods is another very important issue related to data protection. If the purpose of an EES is to be limited to verifying whether third-country visa holders and visa exempted travellers leave on time or overstay, there is no need for long retention periods, and if adopted the system should only contain data which is necessary for verifying entry and exit. Careful analysis is required for establishing criteria to calculate the date of first entry in the Schengen territory, based on the case law of the European Court of Justice.

Biometrics

- While including biometric data may have some benefits, the inclusion of such data would also raise important questions. Notably, whether it is justified in relation to the purpose pursued, and the fact that for visa holders such data are already available (avoiding double storage), the question of what happens to persons whose biometric characteristics are not readable, and the accuracy of the matching mechanisms. I could imagine starting the system without biometric functionality and only considering the introduction of such data, in a second phase, after an evaluation of the system, several years after its go-live.

- These comments have been elaborated in a recent letter of WP29 to Commissioner Malmström on the Commission Communication. Further comments will follow from our side when a legislative proposal has come with a proper impact assessment.

Registered Travellers Programme (RTP)

- On RTP, let me now only focus on the general recommendation that it would also need to be subject to specific data protection safeguards with regard to the criteria used to assess "low-risk travellers", and the storage of data (central or decentralised). These safeguards should include strict security requirements, logging of the system's use and regular audits. Similar to the EES, monitoring and periodic evaluations should be foreseen.

EU PNR

- I am conscious of the fact that the EP has recently suspended its cooperation with the Council on EU PNR and four other JHA reports, until a satisfactory outcome has been achieved on "Schengen" governance. However, this remains a difficult and important subject.

- The fight against terrorism and serious crime is a legitimate purpose. However, the necessity, the proportionality and the effectiveness[1] of this specific measure is, quite frankly, an open question. The use of other less intrusive means, and improvement of existing instruments should be further explored.

- Without prejudice to the remarks on necessity and proportionality, and in view of the negotiations in the Council and the Parliament, I would like to mention some specific concerns:

    - The purposes of EU PNR should be much more limited. The current definition of “serious crime” is too wide and could also include minor crimes.

    - The possibility for Member States to include intra-EU flights would hamper the objective of harmonisation pursued by the Proposal and the principle of purpose limitation, which is required by the EU data protection law.

    - As regards retention periods, I would like to remind that "masked out" data are not anonymised and are therefore still personal data. Data of non-suspects should be deleted as soon as possible. And, even if masked out, they should only be accessed on a case-by-case basis and subject to a judicial decision.

    - I am also concerned about the use of PNR data for risk assessment purposes, as the databases and the criteria that will be used for those purposes are not determined yet, raising a risk of function creep and a lack of foreseeability[2].

[1] PNR data are not verified. Examples from the impact assessment include MS in which general PNR collection was not implemented at that time (e.g. Belgium).
[2] European Court of Human Rights, Rotaru v. Romania, No 28341/95, §§ 50, 52 and 55; and Amann v. Switzerland, No 27798/95, §§ 50 *et s.*

Conclusions

- As regards the Smart Borders package, I would expect the Commission to make a careful and thorough assessment of the effectiveness and weaknesses of existing databases; this assessment should incorporate their impact on fundamental rights.

- I am looking forward to the legislative proposals for the fall with some hope that our suggestions will be considered and acted upon by the EU legislator.

- As to EU PNR, I would still find it important to address the specific concerns raised, without prejudice to my remarks on necessity and proportionality.