EUROPEAN DATA PROTECTION SUPERVISOR

EDPS round table of the Smart borders package and data protection implications

Brussels, 10 April 2013

Venue: EDPS Building, Rue Montoyer 30, Brussels

- Summary of the meeting -

As part of his Strategy for excellence 2013/2014, the EDPS organised a workshop on 10 April dedicated to the Smart Borders package. The aim of the round table was to share experiences from countries that implemented similar systems and to have a debate on the implications for data protection of both legislative proposals.

The 28 experts from various stakeholders that included European Commission, European Parliament, Irish Presidency to the EU, European Union Agency for Fundamental Rights (FRA), USA Mission to the EU, Member States, national data protection authorities representing WP29, academics, and NGOs (Meijers Committee, CEPS), were welcomed by Peter Hustinx, EDPS and Giovanni Buttarelli, Assistant EDPS. On behalf of the EDPS, Hielke Hijmans moderated the round table.

This was the first expert's debate organised following the launch of the smart border package by the Commission on 28 March 2013. The Commission proposes an Entry/Exit System (EES) that will record the time and place of entry and exit of third country nationals travelling to the EU. The system will calculate the length of the authorised short stay electronically, replacing the current manual system, and will issue an alert to national authorities when there is no exit record by the expiry date. In order to complement this system, a Registered Traveller Programme (RTP) is proposed to allow frequent travellers from third countries to enter the EU using simplified border checks, subject to pre-screening and vetting.

I. USA and EU MS national experiences

The participants had a special interest for relevant experiences developed in the USA and in some Member States as regards implementation of similar systems.

USA

Since 2001 the U.S. government has increasingly relied on a combination of data analysis and physical inspection to better manage security at the US border, including

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30
E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

through more accurate and comprehensive assessments of risk that support the efficient movement of low risk travellers. The U.S. Department of Homeland Security (DHS) collects both biographic and biometric data for screening against various databases to identify known threats. This multilayered approach allows DHS to improve security and to minimize the likelihood that any single measure becomes a single point of failure or unduly delays bona fide travellers. The layers include the visa application process, the Electronic System for Travel Authorization (ESTA) check for nationals of the 37 partners participating in the Visa Waiver Program (VWP); Advance Passenger Information (API), Passenger Name Records (PNR) and the Secure Flight Program. DHS screens API across nine data sets: intelligence holdings; 2) outstanding criminal wants and warrants; 3) prior immigration or customs violation records; 4) visa refusal and revocation information; 5) records of individuals with known communicable diseases; 6) lost and stolen passport data; 7) visa issuance records; 8) US border crossing data. API has assisted DHS in identifying more than 5,000 air travellers with ties to terrorism. PNR is different than API and since 1992 has provided DHS with 3 additional screening functions: up to 4 days advance warning of intent to fly; identifies travel patterns used by terrorists; establishes relationships between travellers to find links between those who are known terrorists, and others who may not be known. The PNR agreement between the EU and the U.S. provides for the use of up to 19 types of data. For Secure Flight, in November 2010 DHS assumed responsibility from the airlines for terrorist watch list screening for all flights within, from or bound for the U.S. (including flights that fly over the United States.) DHS uses the passenger's name, date of birth and gender collected up to 72 hours before the flight. DHS screens over 2 million people each day.

- More specifically in line with the Smart Borders RTP and EES systems, DHS has a Global Entry program that allows pre-approved, low-risk travelers expedited clearance for entrance to the U.S. at selected airports. Currently EU nationals of the Netherlands may apply, as well as a limited number of citizens of Germany and the UK.
- Although the U.S. has not implemented an automated exit system at all ports of entry, which some have estimated to cost approximately $3 billion and may require over 3 years, it has a number of important pilots and processes to monitor exiting visitors.
- All passengers, U.S. citizens and visitors, must enter with passports, and data are compared against Department of State databases. For non-U.S. citizens, DHS officers collect fingerprints and a photograph that is screened against the DHS automated Biometric Identification System (IDENT) and matched with data previously collected from the traveler.
- DHS utilizes analysis of biographic and biometric data to verify that foreign visitors to the U.S. comply with admission requirements. In October 2012 the U.S. and Canada began an entry/exit pilot at four common land border sites. Entry information is exchanged so that a record of entry into one country could be considered as a record of exit form the other. The pilot will be expanded to all common land borders by June 2013 and will be fully operational by June 2014.

HU, FI and PL national EES

HU

The Hungarian Entry/Exit System is based on the Hungarian Police Law. The system is controlled by the Police authorities and only the Police have access to the system. The aim of this system is to control the period of person's stay in Hungary and it also seeks border control and works for law enforcement purposes. The retention period of the data from the system is 5 years. The Police have the right to transfer the data to national and foreign authorities who are seeking to protect human rights, to solve questions related with the migration and other legitimate purposes. According to the HU representative, the main shortcoming of this system is that it is based only alphanumerical data. Hungary does not have an ABC system and that the government intends to introduce automated system in the near future. It has been envisaged that Hungary would like to build the EU EES on the national system.

FI

FI representative explained the audience that since 1952 Finland gave the possibility for the residents of Scandinavian countries to cross the border without control checks by using cards. On the basis of this system the National Entry System was created and up to now there were no cases about the misuse of data. The FI expert noted that the Finnish Entry System has two purposes: border control and fighting crime. According to the expert, the main problems relating to the efficiency of the system are the use of alphanumerical data, the short staying period and the possibility for people to change their names (in this case the system cannot find out that a person has changed his/her name). As regards use of biometrics, FI representative mentioned that if Finland would have not joined the Schengen Area, the biometrical data would have been used now as before there were no technical possibilities for that.

PL

The PL representative explained that Polish Registration Travelers System collects data about citizens from third countries and includes such information as name, surname, date of birth, citizenship, border crossing times, vehicle in which the border has been crossed. Only border guards have the access to the system and can provide with information other authorities for legitimate purposes. The PL expert highlighted that the system does not include information about exiting the country, therefore the stay time cannot be calculated. The system has the aim to secure borders and control overstayers and does not use biometrical data because of financial costs and the requirements relating the Schengen Area. The PL representative underlined that if person's documents are lost or destroyed the system cannot identify a person. According to the expert, the access to the system for other authorities would be very useful because it would help to fight crimes. Poland signed up agreements with Russia and Ukraine relating the crossing of the border.

In conclusion, it seems that the main purposes of these 3 MS national systems are border control and under slightly different conditions can be used by law enforcement authorities. Main shortcomings are related to the sole use of alphanumeric data which raises problems where names are changed or passports are destroyed.

With the exception of a set of questionnaires sent by the CZ and FR Presidencies of the EU in 2008 to all MS, no independent evaluation has been carried out in these three MS as regards the effectiveness of their national EES

II. Open debate

A number of questions and concerns were raised about the impact of the proposed regulations on practical implications for data protection of the EES (compatibility with other systems such as VIS and SIS, role of biometrics, possible access of law enforcement authorities and transfer of data to third countries).

1. Debate on the EU EES

There was a fruitful debate on both the justification of the national proposed EES but also the criticism expressed towards its purposes.

To summarise, the arguments expressed by several participants to justify the need for an EES at EU level were:

- More reliable border checks;
- The proposed systems will asses if the Schengen area is working well or not and it will help to reveal how the crossing of borders can be facilitated;
- The proposed systems would eliminate suspicions that the citizens from third countries are dangerous, decrease the discrimination, help to check the number of overstayers in a Member State and help to shape risk factors;
- possibility to deduct overstayers inland;
- The requested data will be used for an effective border control, statistical purposes, fighting against crimes and they will be deleted from the system after six months.

Main lines of criticism were built on the following arguments:

- Concrete statistics needed before creating new systems;
- Enormous expenses for the collection of a big amount of data;
- Such proposed systems would create risk categories relating to a person's behavior and appearance.
- Function creep possibility;
- Additional safeguard and obligation for the Member States should be provided with regard to refugees(e.g. where residence permits are issued);
- The possibility to collect all data for statistical reasons may be disproportionate;
- Use of biometrics may be not proportionate.

2. Compatibility with other systems (VIS, SIS)

One question was about the issue of the authorities who are going to use the data, to have access to them and their competences related to that.

In this regard, the Commission raised the question if it is better to have one big system possessing all data or it is better to have many different national systems. The Commission highlighted that it does not understand the concern raised about interconnection as each system has its own separate rules.

3. Biometrics

One centralised system or not? One participant considered that it is more useful to have a centralised system because such systems can determine a person's identity immediately and it allows the officer to concentrate on concerned cases. It was also mentioned that the mismatches of the biometrical data in the system are very rare.

Finger hash exploratory discussion. One of the experts proposed that instead of the use of full fingerprints, hashes could be used which would reveal less information to the officers and the implementation would be cheaper. He explained that a hash is an alphanumeric string which is associated to a person when his fingerprints are registered in the system during the enrolment procedure, avoiding the need for registering biometric data; In case there is a need for verifying the identity of the person, a new hash can be obtained and matched against the one stored in the database . Even though the EES system is proposed to take 10 fingerprints, he noted that the use of a hash would be in line with the declared purposes for the system, while, at the same time, offering better protection for privacy and avoiding biometric data being compromised.

Following the debate, one expert introduced the idea of the need for a full set of fingerprints insofar it could be helpful when there is a need to compare the information included in the database against, for instance, a latent fingerprint found at a crime scene. In response to that, the expert proposing the use of hashing technologies pointed out that use of the data would not be in line with the purposes of the system as detailed in the current proposal.

According to the EES proposal, at the border gate, a number will be given related to the biometrical data but not all personal data.

4. Law enforcement authorities access to the EES

Several participants noted with scepticism the Commission trend to give access to law enforcement authorities for large IT systems. As one of the participants mentioned, history has shown that data collected for one specific purpose may be used further for other purposes (i.e. law enforcement); an example of this is Eurodac. An expert noted that the real problem is more about the purpose limitation (and not

about law enforcement access, since in most cases border control is exercised by law enforcement authorities). Therefore it might be more precise to speak about the "use of EES and RTP for law enforcement purposes with regard to the detection, investigation, prevention of criminal offences, etc".

Other experts highlighted that the Member States support the law enforcement access. Law enforcement authorities will be able to use the data from the system for immigrant control but not for their other tasks. All investigations which would consist of such data will be controlled by the prosecutor and it would ensure the legitimacy of the procedure. Also, the EES should be a useful system for law enforcement authorities but still it is not clear how often they will use the data for investigations of crimes and how many crimes will be solved. It has been mentioned that the EES could be used only for checking fingerprints.

In the USA out of 150,000 fingerprints, 7,000 were used for investigations of crimes, 600 suspected persons were identified and 10 persons were arrested.

Another participant said that if law enforcement access is granted, very strict conditions should be foreseen and referred on this to the recent WP29 Opinion 01/2013 providing further input into the discussions on the draft Police and Criminal Justice Data Protection Directive.

5. Transfer of data to third countries

One of the main concerns expressed was if the EES will include the information identifying asylum seekers (information about a person's request for the asylum or information about a refugee status).

As one of the participants noted, Article 27 of the EES proposal was copied from the VIS regulation and it requires a further discussion and an evaluation of the VIS experience.

Another issue raised was the question of scrutiny and oversight of data transmitted to third countries.

6. RTP

Even if the nature of the RTP is voluntary, there were some issues raised by participants on the need for proper safeguards, connection with EES and remedies within RTP proposed system.

One expert questioned if the statistics would help to identify cases of discrimination as the proposal gives a person the right to refuse to give their data to the system. It was mentioned that remedies are better formulated in the RTP proposal than in the EES proposal.

Another attendee noted that the proposed regulation leaves much room for interpretation by the Member States and some concepts are not very specified.

It was also highlighted that if one Member State decides not to allow a person access, he/she can go to another Member State as such a decision is not mandatory to all Member States.

Another issue discussed was that the audits will require many efforts by DPO's as they will have to carry out other audits as well, for this reason in the regulation a fixed time is not sufficient. A DPA representative suggested assessing if the DPO's are ready to carry out audits and proposed that they would have been carried out not more often that once every 4 years.

There was also some discussion on the impact assessment for the RTP system, in particular about the option for including all the information on a centralized system instead of using a separate token for the storing of data of the applicant. According to the EC, the option for a centralized system storing all the information would ensure that the registered traveler would be protected in case of losing the token by also avoiding the need for starting the enrollment procedure from the scratch. According to another expert, that reason – losing the token - seemed to be weak since it could be also applicable to any European citizen travelling with his/her national id card or passport, so the same need for a centralized system for protecting all the European travelers could apply by analogy.

It seems that RTP and EES will be connected.

Conclusion

Very interesting debate and much appreciated by the representatives of EU institutions involved in the negotiations but also by MS and DPA representatives.
The discussions revealed the complex nature of both proposals and certainly more time is needed to assess possible implications for data protection. Issues like compatibility with other system, use of biometrics and transfer of data to third countries could pose some risks to data protection and the respective provisions of the proposals will be analyzed thoroughly.

The EDPS will use the results of the meeting in his near coming Opinion.

Annex I - List of Participants

Name	Organisation
Mr. Peter Michael General Secretariat	Council of the European Union
Mr. William J. O'Dwyer Mr. Gerry McConnell Ms. Eileen O'Reilly Mr. Des Foley	Irish Presidency of the Council of the EU
Mr. Henrik Nielsen Head of Unit Border Management and Return Policy Mr. Martin Sustr Transeuropean Networks for Freedom and Security and relations with eu-LISA	European Commission DG Home Affairs
Mr. Jörg Huperz Policy Officer, Data Protection Unit	European Commission DG Justice
Ms. Katrin Huber Mr. Alin Cristian Mituta Mr. Christian Schimang Mr. Dalibor Sternadel	European Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE)
Mr. Adriano SILVESTRI Head of Sector Asylum, Migration and Borders Mr. Mario Oetheimer Head of Sector Privacy and Data Protection	European Union Agency for Fundamental Rights (FRA)
Mr. Manuel Gárcia Sanchez Agencia Española De Proteccion De Datos	Article 29 Working Party Borders, Travel and Law Enforcement Subgroup (BTLE)
Dr. Sergio Carrera	Senior Research Fellow and Head of the Justice and Home Affairs Programme Centre for European Policy Studies, CEPS

Name	Organisation
Mr. John W. Bird	Department of Homeland Security Attaché US Missions to the European Union and NATO
Mr. I. G. te Pas Executive Secretary Meijers Committe Ms. Dr. L. Marin Assistant Professor University of Twente Mr. Dr. R. Rijpma, Assistant Professor University of Leiden	Meijers Committee
Mr. Mika Rytkönen	Permanent Representation of Finland to the EU JHA Counsellor
Ms. Mónika Jenei	Department of European Cooperation Ministry of Interior, Hungary
Ms. Anna Zawila-Niedzwiecka	GIODO Bureau of the Inspector General For Personal Data Protection
Ms. Agnieszka Wawrzyk Counsellor	Permanent Representation of the Republic of Poland to the EU Justice and Home Affairs Unit
Mr. Tudor Bora	Permanent Representation of Romania to the EU JHA Counsellor
Ms. Janneke Timmer	EU-adviseur commissies V&J/I&A en OCW Tweede Kamer der Staten-Generaal
Ms. Daniela Kietz	Stiftung Wissenschaft und Politik Forschungsgruppe EU-Integration