ARTICLE 29 Data Protection Working Party

Brussels, 12/06/2012
Just.c.3(2012)818678

Ms. Cecilia Malmström
Commissioner for Home Affairs
B - 1049 Brussels
Belgium

Subject: Smart Borders

Dear Commissioner Malmström,

The Article 29 Working Party (hereafter also we) certainly recognises the need for the development of a European model of integrated border management of the external borders of the EU. Improving the management of migration flows and preventing irregular immigration and possible threats to the security of the EU, while protecting the rights of persons seeking for asylum or humanitarian status and facilitating border crossing for travellers, are all legitimate purposes.

Having studied the Commission's Communication on "smart borders" and the plans for the legislative proposals for an Entry/Exit System (EES) and a Registered Travellers Programme (RTP), the Article 29 Working Party has serious questions as regards the necessity and proportionality of the smart border concept, in particular with respect to the EES. A scheme such as the EES would necessarily entail the collection and storage of personal data on a very large scale. At the same time, the Working Party requires that it should be better substantiated how the EES will contribute to reach the purpose of its establishment and provide the answer to the problem of "overstayers". The fact that the system would only provide more precise figures on "overstayers", without specific safeguards, regardless of the costs for establishing such a database, should be better assessed in line with the European Union's commitment to the protection of personal data, as expressed in Art. 8 of the European Charta of Fundamental Rights and Art. 16 of the Treaty on the Functioning of the European Union.

The timing of this intervention before the publication of legislative proposals aims to provide input at a point in time where the establishment of a smart border scheme and its possible modalities are still subject to consideration.

General remarks

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO59 2/13.

Website: http://ec.europa.eu/justice/policies/privacy/index_en.htm

First, there is a lack of reliable evidence to support the need for new systems. The need for such a massive volume of data collection in this area is not supported by reliable data. Far-reaching infringements on the privacy of individuals should be based on solid grounds demonstrating their necessity and with justification as to how extensive they should be. The Commission should also take into account studies carried out in third countries about comparable systems in operation there. Experience in the USA with US-VISIT, for example, did not provide solid evidence for the efficiency of similar systems.

Second, we are concerned about a lack of proper identification of the impact on basic rights, including the right of each individual to have his/her personal data protected, so far. This shortcoming should be addressed in the upcoming impact assessments and the legislative proposals, in line with the Union's stated commitment to fundamental rights.

Third, is not clear if all current instruments have been evaluated in order to identify all possible alternatives, including scalable or variable retention periods. The Article 29 Working Party holds that a proper and thorough assessment of the effectiveness and weaknesses of existing databases should be conducted; this assessment should incorporate their fundamental rights impact. All this is to be done before proceeding to further deployment and development of any of existing or planned components.

Fourth, it should 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 all over the world, it introduces the obligation to register in the CVIS 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 the EU territory for no more that three months out of six, thus requiring the stamping of the passport on exit. It is not clear then which will be the impact on a new databses rather than providing a system for linking the information between existing databases, even if not fully exploited so far.

Fifth, the systems could cast an "unpleasant shadow"[1] on the EU in its treatment of third countries nationals, in particular those in need of international protection, in the light of EU and ECHR legal requirements. A certain tension arises between the Commission's proposals and the tests of proportionality and fundamental rights as we mentioned above. As the Communication mentions, there is a big gap between removal orders issued and removal orders carried out. This seems to imply that there rather seems to be a problem in implementing removal orders of overstayers than in identifying them in the first place.

Sixth, we are convinced that the rights of data subjects should be clearly laid out and kept on mind throughout, taking into account impact on other fundamental rights at the same time.

To sum up, although the concrete details are not known yet, it is clear that the smart borders project would have significant impact on natural persons and their rights. New sets of personal data, including new types of unique biometric data, would be created and processed for the exclusive use by public authorities allowing for the control over people. Clear evidence on the necessity of such a large scheme is thus a must, as only then inevitable invasions of people's privacy could be justified.

---

[1] See also Opinion of Advocate General Poiares Maduro delivered on 3 April 2008 (1) Case C-524/06 Heinz Huber v Bundesrepublik Deutschland.

Therefore, the reasoning behind the Smart Border project needs to be appropriately explained, addressing comprehensively its impact on all fundamental rights. The Article 29 Working Party is convinced that necessity and proportionality testing will help to minimise invasions of privacy.

Notwithstanding our serious doubts as regards the necessity of an EES, we would like to make the following more specific comments:

Specific comments on EES

As regards the EES, it seems that the system would most likely include technical functionalities for processing biometric data (fingerprints and facial data) as well as a possibility for law-enforcement access, with the activation of both these features being subject to an evaluation a number of years after the start of the system. Also, transfers to third countries would be excluded.

First, 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 data must only be "*collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes*".[2] An EES with law enforcement access would pursue a dual purpose: preventing and detecting overstay as well as general law-enforcement functions. These two purposes would need to be appropriately assessed and justified separately: even if it is established that an EES would be necessary for the purpose of preventing and detecting overstay, this would not be a justification to grant law-enforcement access as well. We recommend to the Commission that the necessity of law-enforcement access would need to be established separately.

The subject of retention periods follows directly from this. 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, we consider that 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 should be given in establishing criteria to calculate the date of first entry in the Schengen territory based on the European Court of Justice jurisprudence[3].

As we understand, however, it is planned to introduce a possibility to access the data for law-enforcement purposes, for which longer retention periods might be necessary. Given that the main purpose of the EES would be detecting and preventing overstay, the necessity of retention periods should be assessed against this purpose.

A related question is which kinds of data would be processed in an EES - notably whether it will be alphanumeric data only, or also (possibly at a later stage) biometric data. While there are some possible benefits from including biometric data, the inclusion of such data would 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 would happen to persons whose biometric characteristics are not

[2] Article 6(1)(b) of Directive 95/46/EC, OJ L 281, 23/11/1995 P. 0031 - 0050.

[3] See Case 241/05 Nicolae Bot.

readable and the accuracy of the matching mechanisms. In the light of this, we would suggest starting the system without biometric functionality and only considering the introduction of such data after an evaluation of the system several years after its go-live. This evaluation would provide a factual basis as to whether the objectives can also be achieved without the collection of biometric data.

Given the substantive amount of data to be processed in the EES, its operation would need to be flanked by specific data protection safeguards. We recommend that these should among others include legal responsibility for unauthorized or unlawful access and use of the system, strict security requirements, logging of the system's use and regular audits.

Last but not least, if an EES will be introduced, the Working Party strongly advises that it should be subject to monitoring and periodic evaluations. The introduction of new features should be contingent on previous evaluation results showing that in their absence the system was not able to achieve its purposes. Any possible extension of the system to cover also EU citizens should be strictly ruled out.

Specific comments on RTP

It is our understanding that such a system would be voluntary to use and that it would offer quicker access to EU territory for registered users (e.g. by allowing them to use automated border gates or simplified checks similar to those carried out for EU citizens).

First, we invite the Commission to provide convincing evidence that such a programme would indeed significantly ease access to the EU for third-country nationals without placing an extra control burden on non-registered travellers.

As far as we understand, the RTP is also likely to include biometric data, which again raises the question of failure to enrol; fingerprints are the most widely used biometric identifier, yet there is a substantial group of persons whose fingerprints are not readable with current technology, for example due to medical conditions or hard manual labour. It should be assessed which fall-back options should be available for such persons.

The enrolment process also raises other general questions. As the RTP is meant to facilitate access for "low-risk travellers", the criteria used to assess this risk are very important. Vetting criteria should be clear and transparent, to ensure that applicants know what is happening to their data, as well as to prevent discrimination and inconsistent application. The final decision on whether or not to grant participation in the programme would have to be made by a human being and cannot be left to profiling algorithms or other technical tools. In order to be consistent, the criteria could be based on the criteria for issuing multiple entry visas.

The next issue to be addressed is the storage of this data. There are several possibilities available: central storage, a token system or a combination of the two. From the point of view of data protection, it would desirable to limit central data storage. A limited storage of data in a central system is likely to always be needed, for example for managing and revoking RTP membership. For most data -most importantly the fingerprints- storage on a token given to the registered traveller could suffice. Storing fingerprint data only on a token would also reduce the risk of abuse of the central database. We invite the Commission to consider all options for limiting the storage of personal data to the smallest amount possible. Related to this, retention periods should also be considered - these should be as short as possible.

Also in this case, the question of access for law-enforcement authorities is relevant, especially in combination with the EES. As the stated purpose of the RTP is to facilitate access to Union territory, access for law-enforcement purposes should be excluded as it is not relevant to this purpose (this does of course not exclude that the vetting criteria could include checking certain law-enforcement databases).

As recommended for the EES, the RTP would need to be subject to specific data protection safeguards, including among others strict security requirements, logging of the system's use and regular audits. Similar to the EES, monitoring and periodic evaluations should be foreseen.

Conclusions
In conclusion, it is clear that the smart borders project will have significant impact on natural persons and their rights. New sets of personal data, including new types of unique biometric data, will be created and processed for the exclusive use by public authorities allowing for the control over people. The Working Party has serious questions that a scheme such as the EES is necessary. If necessity could be demonstrated, effective safeguards, as outlined above, would be a must as only they are able to mitigate inevitable invasions of private aspects of people's lives.

The WP 29 requires and advises the Commission:
- Make a proper and thorough assessment of the effectiveness and weaknesses of existing databases should be conducted; this assessment should incorporate their fundamental rights impact.
- Undertake impact assessments based on the impact on basic rights, including the right of each individual to have his/her personal data protected;
- Reflect upon and address the above specific remarks made by WP 29 on both proposed systems.

In the spirit of good cooperation we invite you to our next meeting of the BTLE subgroup in early September to discuss implications of smart borders proposals and the way forward.

Should you need any further advice, please do not hesitate to contact us,

Yours sincerely,

On behalf of the Article 29 Working Party,

Jacob Kohnstamm
Chairman of the Article 29
Working Party