



Formal comments of the EDPS on the European Commission Public Consultation on smart borders¹

Context

The European Commission launched a Public Consultation on the Smart Borders Package from 29/07/2015 to 29/10/2015. According to the Commission², the aim of the public consultation is to collect views and opinions to underpin the on-going impact assessment of the 2013 Smart Borders Package and the policy preparation of the revised proposals that will be tabled by the Commission. An impact assessment (including the impact on fundamental rights) will be carried out by the Commission for the revised proposals, to which this consultation will contribute. This will build on previous Commission work such as:

- a Technical Study³ and a Costs Study⁴, completed in October 2014; and
- a testing phase⁵ that will be completed by end of November 2015.

The Smart Borders 2013 Proposals are still before the European Parliament and the Council. As presented by the Commission in the European Agenda on Security and the European Agenda on Migration⁶, the Commission announced its intention to present revised proposals by early 2016. This follows discussions in the European Parliament and the Council⁷ which raised a number of technical, operational and cost concerns.

The European Parliament also expressed concerns⁸ relating to fundamental rights and in particular the right to personal data protection, should law enforcement access to the Entry-Exit System (EES) be granted.

Scope of the EDPS comments

The EDPS aims at advising the Commission services in the drafting of new proposals with regard to the data protection implications. The EDPS will reply to those questions from the COM public questionnaire that are relevant in this respect (see the Specific comments below, p. 5).

These formal comments build on the series of the EDPS interventions on the smart borders package such as: April 2013 EDPS Workshop on smart borders⁹, EDPS Opinion on smart

¹ http://ec.europa.eu/dgs/home-affairs/what-is-new/public-consultation/2015/consulting_0030_en.htm

² http://ec.europa.eu/dgs/home-affairs/pdf/20150724_1_consultation_on_sb_background_rev_en.pdf

³ http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_technical_study_en.pdf

⁴ http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_costs_study_en.pdf

⁵ <http://www.eulisa.europa.eu/AboutUs/SmartBorders/Pages/default.aspx>

⁶ http://ec.europa.eu/dgs/home-affairs/pdf/20150724_1_consultation_on_sb_background_rev_en.pdf

⁷ <http://data.consilium.europa.eu/doc/document/ST-17060-2014-INIT/en/pdf>

⁸ <http://www.europarl.europa.eu/EPRS/EPRS-AaG-559476-Smart-borders-package-FINAL.pdf>

⁹ https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/PressNews/Events/2013/13-04-10_Summary_smart_borders_final_EN.pdf

borders of June 2013¹⁰, Working Party 29 (WP 29) Opinion¹¹ to which the EDPS contributed, presentations before LIBE¹² and other staff level informal meetings with DG HOME held in 2013 - 2015).

GENERAL COMMENTS

The EDPS recognises the need for new EU steps in improving border management of the EU external borders and the fight against irregular immigration, as well as at enhancing cooperation among immigration authorities, to cope with the new challenges and modernise existing systems.

However, as confirmed in the EDPS 2013 Opinion on Smart Borders¹³, the proposed EES scheme constitutes an interference with the respect for private and family life. Indeed, as mentioned, it is evident that the routine storage of data on individuals relating to their entry to and exit from the territory of the European Union will often and in many different ways also reveal information about their private and family life.

The EDPS has supported and commented the Smart Borders Package inviting for a thorough reflection on such new systems, to duly take into account both the costs for privacy and data protection and the effectiveness for border control and public security.

To sum up, fundamental rights should not bear the costs of a perceived need to accelerate border crossings.

“Smart borders” for all?

Data protection plays an important role since the planned EES will lead to the use of personal data of *all* third-country nationals¹⁴ entering and exiting the European Union¹⁵. Thus, the EU’s information systems containing biometric information will be significantly expanded. In addition, the possibility is also foreseen for personal data being accessible to law enforcement and security authorities.

¹⁰https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2013/13-07-18_Smart_borders_EN.pdf

¹¹http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp206_en.pdf

¹²<http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+COMPARL+LIBE-OJ-20150223-2+02+DOC+XML+V0//EN>

¹³ See EDPS Opinion of 18 July 2013, §22.

¹⁴ The EES proposal is distinguishing between Visa holders who are exempted and Visa exempted travellers who will be asked to give their fingerprints. See Article 11 and 12 of the EES Proposal: http://ec.europa.eu/dgs/home-affairs/doc_centre/borders/docs/1_en_act_part1_v12.pdf

¹⁵ And possibly to all EU citizens. See the Letter from the President of the Council of the EU to the European Council on the JHA Council from 8-9 October where this possibility is mentioned: *“Moreover, the Council underscored that enhanced security and facilitation of border crossings by bona fide travellers can be obtained via an adequate use of technologies at EU’s external borders. In this respect, we look forward to the new Smart Borders package, to be proposed by the Commission in the coming months. The importance of giving law enforcement authorities access to such technical solutions, of guaranteeing the interoperability of such technical systems with SIS and VIS and of making use of biometry is widely recognized. It was mentioned that such technical solutions could also be explored for EU citizens, to address security challenges.”* <http://www.statewatch.org/news/2015/oct/eu-council-jha-presidency-to-summit-letter.pdf>

The use of biometric data (See also below the Specific comments on this, p. 5)

Biometric data¹⁶, by their very nature, are directly linked to an individual. The WP 29 analysed at length the developments in biometric technologies¹⁷ where it has mentioned that biometric data changes irrevocably the relation between body and identity, because they make the characteristics of the human body ‘machine-readable’ and subject to further use. This requires a higher level of protection when processing biometric data.

The EDPS recalls¹⁸ that there is a need to demonstrate that the use of biometrics (facial image and/or fingerprints) in this context, which represents a separate interference with the right to respect for private life, is "necessary in a democratic society" and that other less intrusive means are not available. Thus, biometric data should only be introduced after an evaluation of the system after some years of operation¹⁹. This evaluation which is to be done after the smart borders systems start to operate and all interested stakeholders will be able to make an assessment would provide a factual basis of whether the objectives could also be achieved with or without the collection of biometric data.

Proper evaluation of existing policies and instruments

Existing policies and instruments have been thoroughly debated not only by the EDPS in his reactions on smart borders but also by the WP 29²⁰ or the European Parliament and by the national parliaments. Criticism and concerns have included the proportionality and necessity tests, the reliability of statistics, the “overstayers” nationalities and numbers and the relation with other large-scale IT systems such as the VIS.

While the EDPS welcomes the safeguards made in the Proposals and recognises the efforts made by the Commission, necessity remains a fundamental issue in relation to the fundamental rights at stake, in the global context of existing schemes and border policies.

As mentioned in the EDPS 2013 Opinion²¹, an EES should not be created before a thorough evaluation of existing systems is performed, in order to ensure consistency and avoid repeating difficulties encountered in the past. In this regard, a number of uncertainties remain:

- One of the EES goals is to identify those who overstay their legal stay in the Schengen area but the FRONTEX numbers on the detections of illegal stay²² show that the majority of the overstayers are coming from those countries where a visa is needed to enter the EU and where the VIS can be used in identifying them²³.

¹⁶ Biometric or biometric systems are methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioural traits : <https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/72>
See also the definition given by the WP29 in its Opinion 3/2012 on developments in biometric technologies, p.3.

¹⁷ See WP29 Opinion 3/2012 on developments in biometric technologies.

¹⁸ See EDPS Opinion of 18 July 2013, §60.

¹⁹ See also WP29 Opinion on smart borders, p. 10.

²⁰ See WP29 Opinion on smart borders.

See also the results of the Interparliamentary Committee Meeting, European Parliament - National Parliaments, Smart Borders Package: European challenges, national experiences, the way ahead.

<http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+COMPARL+LIBE-OJ-20150223-2+02+DOC+XML+V0//EN>

²¹ See EDPS Opinion of 18 July 2013, §38.

²² Frontex, Annual Risk Analysis 2014, p. 52 and FRAN Quarterly, April-June 2015, p. 26.

²³ See Articles 18-20 of VIS Regulation: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32008R0767>

- The Commission has argued that the EES will make for more efficient border crossings by replacing the current procedure of stamping (see also below the Question on Stamping, p. 10). However, an EU Presidency Questionnaire²⁴ on the consequences of the abolition of stamping, revealed several Member States concerns notably on the possible total loss of records, the need to obtain a travel history as a mean of evidence, how to separate the third country nationals who are exempt from stamping/registration in the EES, impact on the third country nationals who have long term visas, long term permission or permanent resident permit etc. Moreover, another EU Presidency questionnaire²⁵ shows that all 28 Member States that responded think the most effective way for ascertaining overstay cases are stamps and national entry/exit systems (or similar), as well as the Schengen calculator.
- Another purpose of the EES is to identify undocumented migrants and contribute to an effective return. As stated in the WP 29 Opinion²⁶ there is some added value in the data that the EES will make available to identify undocumented migrants. However, this added value is seriously weakened by the fact that similar data available in the VIS is likely to target a larger number of “overstayers” and the fact that identity verification in itself is not a means to effective return.

Taking into account the various concerns expressed by different stakeholders, the EDPS recommends the Commission to have a specific “How the *status quo* could be improved” Policy Option in the new Impact Assessment²⁷. This should basically reply to the question on how the current system could be improved also in relation to the use of existing systems (such as the VIS in the case of “overstayers” and how can the current stamping system and the Schengen calculator be improved²⁸).

Law Enforcement Access (See also below the Specific comments on this, p. 9)

The EDPS emphasises the fact that solid evidence is needed to prove the necessity of law enforcement access; evidence that access to data stored in the EES is a key to the investigation or the resolution of a case and not rather circumstantial²⁹. This evidence was not presented in the initial 2013 Smart Borders Proposals so the EDPS recommends the Commission to provide solid evidence on the need for law enforcement access in the new Impact Assessment.

²⁴ Presidency Note to the Delegations, *The consequences of the abolition of the stamping*, 7592/15, LIMITE, JAI 199, FRONT 68, COMIX 146, Brussels, 1 April 2015: <http://www.statewatch.org/news/2015/jul/eu-passport-stamps.htm>

²⁵ Presidency Note to Working Party On Frontiers, *Overstayers in the EU*, 8744/15, FRONT 98, Brussels, 20 May 2015, p. 4: <http://www.statewatch.org/news/2015/jul/eu-council-overstayers-in-the-eu-8744-add1-15.pdf>

²⁶ See WP 29 Opinion, p. 9.

²⁷ The 2013 EES IA analyses a Baseline scenario on how would things evolve without EU intervention but do not refer specifically to a “status quo” policy option and instead addresses policies options based on a core system where EES was included from start and . See p. 23-28. http://ec.europa.eu/dgs/home-affairs/doc_centre/borders/docs/1_en_impact_assessment_part1_v4.pdf

²⁸ http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/border-crossing/docs/short_stay_schengen_calculator_user_manual_en.pdf

²⁹ For more details about how quantitative and qualitative information provided by Member States on the need for law enforcement access on telecom operators data retention should be interpreted see the EDPS Opinion on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC).

https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2011/11-05-30_Evaluation_Report_DRD_EN.pdf

The principle of purpose limitation is one of the key notions of EU data protection law as was reminded in recent European Union case law. In this context, the *Digital Rights Ireland*³⁰ ruling of the Court of Justice of the European Union (CJEU) and the recent ruling of the CJEU of 6 October 2015 in the Maximilian Schrems v Data Protection Commissioner³¹ case are fundamental in assessing the revised Smart Borders legislative proposals. In particular, the precise added value of such access compared with access to already existing biometric databases should be identified, and it should be demonstrated that the necessity overrides the intrusion in the family life of individuals. The persons whose data would be stored in the EES are in principle not suspected of any crime and should not be treated as such, since the system is in the first place designed mainly as a calculation tool for the duration of stay of third country residents.

The question of law-enforcement access has to be addressed considering the primary purpose of the system, bearing in mind that such a purpose has significant implications on the system design. An EES purely designed to calculate stay and detect and deter overstay, would look different from one that which also meant to be used as a general law-enforcement tool. Therefore, the system should not be designed having in mind a possible law enforcement access as long as this necessity has not been solidly proved.

In the event that access for law enforcement authorities proves to be necessary, strict conditions are needed, such as the condition that requests for data should be proportionate, narrowly targeted and based on suspicions as to a specific person.

SPECIFIC COMMENTS

The EDPS herewith contributes to those Commission public consultation questions that are relevant from a data protection perspective. The Public Consultation on smart borders may be consulted at this link:http://ec.europa.eu/dgs/home-affairs/what-is-new/public-consultation/2015/consulting_0030_en.htm

The use of biometric identifiers

Question

What kind of biometric identifiers would you prefer to be used?

- ***No biometrics at all, only alphanumerical data (for example, your name, surname and travel document number) (EDPS choice)***
- *Fingerprints only*
- *A combination of facial image and a limited number of fingerprints*
- *Facial image only.*

Answer

Consistent with his 2013 Opinion³², the EDPS advises on an *ex ante* evaluation to be performed, and on the introduction of possible safeguards, rather than on taking already now a definitive decision to introduce biometrics in the system. Recalling the Technical Study which

³⁰ CJUE, *Digital Rights Ireland ltd*, 8 April 2014, in joined cases C-293/12 and C-594/12.

³¹ CJUE, Maximilian Schrems v Data Protection Commissioner, C-362-14, §91-95.

³² See EDPS Opinion on smart borders, § 61.

explored different options³³ for introducing a transitional period for the use of biometrics (fingerprints) in the EES - as foreseen in the 2013 EES legislative proposal³⁴, the EDPS recommends the Commission that the system relies on the alphanumeric data of the travel documents, while the use of biometric characteristics is introduced only after a transition period if proved to be necessary.

Question

Do you think that the use of biometric identifiers could jeopardise or improve the reliability of border checks?

- *Jeopardise*
- *Improve*
- *Not sure (See EDPS comments below)*

Answer

This depends on the accuracy of the system used to match biometric information. According to the Technical Study, the total number of border crossings in 2025 is estimated at 887 million. If we assume that the system matching biometric information will match individuals incorrectly to the tune of 1%³⁵, on such a large scale, 8.870.000 travellers would be affected. These mistakes could lead either to situations where the traveller is blocked at the border (because of low quality of fingerprints taken initially etc.) or in being incorrectly identified as a person of interest.

The EDPS recognised³⁶ on several occasions, the advantages provided by the use of biometrics, but also stressed that these benefits would be dependent on stringent safeguards being applied. Thus, we proposed a non-exhaustive list of common obligations or requirements which need to be respected when biometric data are used in a system³⁷, such as:

- 1) A targeted impact assessment on the use of biometrics, including the effect on the overall process when biometric matching fails.
- 2) A carefully designed enrolment process to provide maximum assurance of the quality of the biometrics being registered in the system.
- 3) A clear description of the level of accuracy of the system including reasoning on what type of performance metric is being considered.
- 4) Fallback procedures in case of failure of or errors in the use of biometrics.

These elements will help avoid that the third country national is to carry the burden of imperfections of the system, such as the impact of misidentification or failure to enrol.

³³ See Technical Study, p. 178.

³⁴ Article 12 (5) of EES Proposal. “For a period of three years after the EES has started operation only the alphanumeric data referred to in paragraph 1 shall be recorded”.

³⁵ The system which is gives 99 % of correct results will most probably be assessed as effective from technical point of view.

³⁶ See for example EDPS Opinion on standards for security features and biometrics in passports and travel documents issued by Member States:

https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2008/08-03-26_Biometrics_passports_EN.pdf

³⁷ See EDPS Opinion on SIS II:

https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2005/05-10-19_SISII_EN.pdf

In conclusion, the EDPS is recommending to the Commission a rigorous impact assessment on biometrics to be included in the new Impact Assessment, in addition to the Chapters on Biometrics tackled in the Technical Study³⁸.

Registered Traveller Programme (RTP)

Question

The 2013 proposal for the Registered Traveller Programme proposes setting up a programme to enable pre-vetted non-EU citizens to benefit from facilitations at borders. This will make it easier and quicker for these pre-vetted frequent travellers to cross borders. The Commission is analysing potential simplifications to this approach. To what extent do you consider that there is a need for a process to accelerate border crossings by non-EU citizens at the Schengen area's external borders?

- *To a great extent*
- *To some extent*
- *To a small extent*
- *Not at all*
- *I do not know (see EDPS comments below)*

Answer

The EDPS considers that if replies indicate a need to accelerate border crossing, this does not constitute as such a basis for any form of RTP. Consent of the traveller is presented as the ground legitimising the processing of personal data. However, consent cannot be considered as being given voluntarily and freely if the only alternative is long queues and administrative burdens. Risks of discrimination should be also prevented: the vast amount of travellers who do not travel frequently enough to undergo registration or whose fingerprints are unreadable should not be *de facto* in the 'higher-risk' category of travellers.

Question

Another faster border crossing process could be envisaged for those travellers entering the Schengen area for a short stay and whose passport data and biometric identifiers had already been registered in:

- *the Visa Information System for travellers holding a short-stay visa;*
- *the Entry/Exit System for visa-exempt travellers whose data has been registered during a previous journey, if the retention period has not yet expired.*

These travellers would be able to benefit from a faster process without needing to submit any application. This process would be available at those border crossing points equipped with self-service kiosks. Some elements of the border checks (passport control, biometric verification, answering questions...) could be performed using self-service kiosks. The decision to authorise or refuse entry would be taken by a border guard who may also need to talk to the traveller for additional verifications.

Do you consider that the process to accelerate border crossings described above should be available for the two categories of travellers listed?

³⁸ See the Technical Study, p.149-192.

Answer

This question raises the issue of the compatibility of the re-use of data collected in the context of VIS or EES for a new purpose. As stated in the WP 29 Opinion on purpose limitation³⁹, further processing for a different purpose does not necessarily mean that it is incompatible: compatibility needs to be assessed on a case-by-case basis. A substantive compatibility assessment requires an assessment of all relevant circumstances. In particular, account should be taken of the following key factors:

- the relationship between the purposes for which the personal data have been collected and the purposes of further processing;
- the context in which the personal data have been collected and the reasonable expectations of the data subjects as to their further use;
- the nature of the personal data and the impact of the further processing on the data subjects;
- the safeguards adopted by the controller to ensure fair processing and to prevent any undue impact on the data subjects.

Visa holders can be checked at external border crossing points by the border guards for the sole purpose of verifying their identity and/or the authenticity of the visa and/or whether the conditions for entry to the territory of the Member States in accordance with Article 5 of the Schengen Borders Code are fulfilled (Article 18 VIS Regulation). One of the purposes of the VIS Regulation is to facilitate checks at external border crossing points. If registration in VIS results in a faster crossing this should not raise a compatibility issue, on the other hand if this results in the registration of the data in a new data base, the compatibility of this new purpose should be assessed accordingly.

Data retention

Question

The 2013 Entry/Exit System proposal sets a limit to how long data can be kept after its collection at the entry and exit of the Schengen area's external borders:

- 1) A maximum retention period of 181 days after exit (91 days if the traveller has been absent from the Schengen area for 90 days). This retention period enables enforcement of the rule authorising non-EU citizens to stay in the Schengen area during 90 days within any period of 180 days.*
- 2) A data retention period of five years for a person who has overstayed (i.e. remains in the Schengen area beyond the authorised period of stay). This data retention period aims to support the identification of the person and the return to his/her country of origin.*

The Commission is evaluating whether these retention periods should be adapted in its new proposal.

Concerning the data retention period for the Entry/Exit System for non-overstayers, would you be in favour of:

- *A maximum data retention period of 181 days starting from the exit date. This period is sufficient to calculate the duration of authorised short stays in the Schengen area. (EDPS choice)*

³⁹http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

- *A longer data retention period, to speed up border controls as a traveller returning to the Schengen area during the data retention period would not need to re-enrol under the Entry-Exit System, since his/her personal data is still stored in the system and can be reused.*

Concerning the data retention period for the Entry/Exit System for people who overstay, would you be in favour of:

- *A data retention of five years following the last day of the authorised stay*
- *A data retention longer than five years*
- *A data retention shorter than five years*
- ***Other (Please see EDPS comments below)***

Answer

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. The EDPS is in favour of preserving the period of data retention as proposed in the 2013 EES Proposal as for a maximum of 181 days (Article 20), as this is the period needed for the purpose of calculating the authorised stay in accordance with the Schengen Border Code.

As regards people who overstay, the EDPS recalls⁴⁰ the recommendation for the legislator to better justify in a recital of the announced revision of the EES Proposal the need for keeping the data for such a long period of time, or limit this period in a substantive manner. This recommendation is based on the fact that we have not received evidence⁴¹ on the assessment criteria to determine a 5 years retention period for the overstayers. The fact that this period might be linked with other retention periods such as that established for the VIS⁴² or to the possible retention times for law enforcement purposes do not satisfy, in our opinion, the retention limitation test.

Law Enforcement Access

Question

The 2013 Entry/Exit System proposal provides that the option for law enforcement authorities to access data will be evaluated two years after the system enters into operation. For its forthcoming revised proposal, the Commission is analysing whether law enforcement authorities should have access to the system, and if so, under which conditions. This analysis will address the necessity, appropriateness, and proportionality of this option and be accompanied by a fundamental rights impact assessment.

Would you favour granting law enforcement authorities access to the data stored in the Entry/Exit System for the purpose of preventing, detecting or investigating terrorist offences or other serious criminal offences? This access would be granted under strict legal prerequisites in full compliance with fundamental rights.

- *Yes*
- *No*

⁴⁰ See EDPS Opinion on smart borders, §76.

⁴¹ See the EES Impact Assessment, p. 29 and the alternative data retention options analysed in the Technical Study, p. 218-227.

⁴² *Ibid*, p. 221.

- *Not yet. The issue should be evaluated two years after the implementation of the Entry/Exit System. (EDPS choice)*
- *No opinion / Not sure*

If law enforcement authorities had access to the Entry/Exit System data, which of the following conditions should be implemented to mitigate the impact on fundamental rights and in particular on data protection? (You may tick more than one box)

- *Access should be limited to the prevention, detection or investigation of terrorist offences or other serious criminal offences.*
- *There should be reasonable grounds to consider that the specific envisaged consultation of the*
- *Entry/Exit System data will substantially contribute to the prevention, detection or investigation of any of the terrorist or serious criminal offences in question.*
- *Searches should only be possible in specific cases under clearly defined circumstances. The proposal should exclude searches on a systematic basis.*
- *The data should be accessible for law enforcement purposes for a predefined limited period of time.*
- *A court or an independent administrative body should verify in each case if the required conditions for consulting the Entry/Exit System for law enforcement purposes are fulfilled.*
- *Access to the Entry/Exit System should only be possible if prior searches in more restricted databases (e.g. Member States' criminal databases) do not provide sufficient results.*
- *No opinion / Not sure*
- *Other (Please see EDPS comments below)*

Answer

The EDPS is in favour of preserving the initial provision of the Commission 2013 EES Proposal [Article 46(5)] as to have an evaluation after two years after the system has been put in place. Thus, the ordinary system will be tested for its reliability and efficiency and only then the discussion on the necessity of law enforcement access could be explored. The EDPS recommends the Commission to carefully evaluate the difference between *statements* and real proof of necessity given by Member States. The statements on the necessity should be supported by clear evidence and not circumstantial discussions.

However, if such an access was to be approved by the legislator with concrete evidence, strict conditions are needed, such as an access to data that is proportionate, narrowly targeted and based on suspicions as to a specific person and where a court or an independent administrative body will assess the necessity for accessing the data. The *Digital Rights Ireland* judgement⁴³ proved crucial in providing the legislator specific criteria when assessing the necessity and proportionality of legislation impacting adversely on personal data.

Stamping

Question

Currently, stamping the passport is the only method of indicating the dates and locations of entry and exit. The stamps are used by border guards and immigration authorities to

⁴³ CJEU, *Digital Rights Ireland Ltd*, 8 April 2014, in joined cases C-293/12 and C-594/12, § 58-68.

calculate the duration of the stay of non-EU citizens and to verify compliance with the rules on short stay (authorised stay of 90 days within any period of 180 days). This calculation method is time-consuming and difficult, particularly for frequent travellers. In addition, maintaining the quality and security of stamps requires both resources and efforts, as they can be subject to counterfeiting and forgery.

The 2013 proposals provide for the abolishment of the stamping of passports of non-EU citizens crossing the external borders of the Schengen area. The Commission would like to gather views on the consequences of such abolition.

If stamps on passports were discontinued for short-stay travellers who are not EU citizens, would it be necessary for public authorities other than border management authorities to have access to the information that the stamps currently provide (date and location of entry into/exit from the Schengen area)?

- *Yes*
- *No*
- *Not sure (EDPS choice)*

Answer

The EDPS recognises the legitimacy of trying to improve the administration of border crossings. However, the abolition of the stamping will require additional safeguards in the interest of the traveller who no longer has a clear view on the checks being made by the authorities. Indeed, the current system allows the stampings from the passport to be kept by the holder and be checked when the person decides to travel. With the removal of stampings a new process will be in place where authorities will have the control of administering the entries and exits that will be stored in an EES database. This of course poses different questions on how the data related to the entries and exits will be stored, used and accessed by authorities.

If the decision on switching to such a system is taken, the EDPS recommends to the Commission to envisage a transitory period to be applied in order to address all concerns already raised by the Member States⁴⁴ and put in place strict safeguards for data protection for the new system (retention periods in accordance with the purpose of Schengen Border Code, allowing access only to competent authorities, putting in place security standards etc.).

Conclusion

The EDPS remains available to the European Commission for further expertise on data protection. We recommend the Commission to also involve the national Data Protection Authorities in the smart borders consultation.

Brussels, 03 November 2015

(signed)

Giovanni BUTTARELLI

⁴⁴ See the Presidency Note to the Delegations, *The consequences of the abolition of the stamping*, 7592/15, LIMITE, JAI 199, FRONT 68, COMIX 146, Brussels, 1 April 2015.