Working Party on FRONTIERS
19 November 2015
Venue: Justus Lipsius, Rue de la Loi 175, Bruxelles

Giovanni BUTTARELLI
European Data Protection Supervisor

A Data Protection perspective on the Smart Borders Package - focusing on the possibility of law enforcement authorities' access to border data

Dear Ms Chair,

Honourable Members of the National Delegations,

I give warm thanks to the LU Presidency for inviting me here. I consider this debate with the national delegations on the smart borders package as fundamental in addressing the complex nature of this file.

I would take this opportunity to express my deep solidarity with the French delegation, the French Republic and the French people in these hard times after the tragic recent events in Paris.

Let me go straight to the point. With your permission, I will touch upon the whole package of smart borders in the introduction and then elaborate more on the specific details of the possibility of law enforcement access to border data.

I would like to remind to those not aware that the EDPS has been involved in the smart borders debate from a long time already. We have published in the past several Opinions[1] related to the subject.

I am here as a colleague who has a continuous expertise on data protection but not only.

You are all aware that I represent an independent institution. We are not *a priori* in favour or against any measure. But we do take extremely seriously our mission of advising the institutions on the implications of policies which have a more serious impact on the rights to privacy and data protection. In full respect for the role of the legislator in assessing the necessity and the proportionality of the proposed measures, the EDPS analyses their implications for the protection of the personal data of individuals and their privacy, taking into account the existing data protection and privacy legislative framework and case-law. This analysis relates to our mission to advise the institutions on the data protection implications of their policies, particularly when they have a more serious impact on the rights to privacy and data protection. This is what we have said publicly in our EDPS PNR Second Opinion[2] and I consider this *mutatis mutandis* applicable to the Smart Borders system.

The project to develop an electronic system to control entries and exits to the EU territory is not new. I recognise the need for new 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.

1

- Opinion of the European Data Protection Supervisor on the proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States (2008/C 200/01) ;
- Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on migration (7 July 2011) where we had several comments on the announced smart borders proposals (EES and RTP);
- In 2013 we have released a more specific Opinion on the smart borders legislative proposals and we have continued to follow and be involved at staff level in the course of developing the Technical Study and the Pilot test. Before that, we have organised a Round table with various stakeholders dedicated specifically to the smart borders issue in April 2013 on which results we have built our Opinion above mentioned.
- WP29 Opinion on Smart Borders (2013). The EDPS has contributed to this document.
- EDPS Formal Comments on the Commission Public Consultation on Smart Borders.

[2] https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-09-24_PNR_EN.pdf

Why data protection is also relevant here

Data protection plays an important role here since the planned 'Entry-Exit System' will lead to the fingerprinting of *all* third-country nationals entering the European Union, by thus significantly expanding the EU's biometric information systems. In addition, there is also the possibility of law enforcement access. Notwithstanding the recent discussion[3] to extend smart borders to EU citizens, which if put into practice will change fundamentally the scope and implications of the system.

General comments on the whole Smart Borders package

Let me first develop few general comments on the smart borders package and then touch upon the law enforcement aspects as explored in the current Presidency Note subject to discussion today.

The main purpose of EU border security is to safeguard European values and interests, among which are fundamental rights, rule of law, and the freedom of movement. Border management uses large collections of personal data. This architecture has to achieve apparently contradicting purposes: to facilitate mobility while keeping borders safe, with low costs, error free and fully respecting fundamental rights (dignity and protection of personal data).

As you know, the Commission will come up with a revised package quite soon (beginning of 2016) which is supposed to take into account the comments made by various stakeholders, including the EDPS.

We are following the Pilot testing phase (which should be completed by end of this year) and the political negotiations. In this sense, I would like to encourage you to reflect on the relation between the deployment of new IT technologies and the need for clear objectives to be set in the law for the use of these technologies.

I would like to mention that I had two meetings this year with Mr Garkov, the eu-LISA Director, to analyse the different legal perspectives in processing data concerning identifiable individuals. We've also been in contact with national DPAs on this matter, as they are in charge of supervising the activities of the national competent authorities in the Pilot test and would do the same for any future EES and/or RTP. In addition, I would also like to encourage the national

[3] 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."*

delegations here today to contact their national DPAs to work together on the new package to come.

At the beginning of November this year we have contributed to the Commission Public Consultation by providing EDPS Formal Comments where we suggested to the Commission *inter alia* that the new Impact Assessment should include also a Policy Option where we should find out why the current system cannot be "upgraded"/improved and be used in the future. I am not contesting that there might be a need for an EES and an RTP but just that I would be curious to see the arguments why the current system cannot be improved.

This remark on exploring the current situation at the borders is also based on your input and findings sent to the current and past Presidencies. I took note of various summaries and contributions from your national delegations related to the access for law enforcement authorities, abolition of stamping and its consequences or the issue of overstayers and I have observed that the majority of the Member States have numerous reservations on how the EES for example will work in practice when stampings will be removed not only for the calculation of the stay but also in connection with possible law enforcement access (for example today the border guards are able to follow the history of travelling by checking the stamps in the passport).

As said in our recent contribution on the Commission Public Consultation, with the removal of stampings a new process will be in place where authorities will have the control of administering the entries and exits which data 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 and to you to envisage a transitory period to be applied in order to address all concerns already raised by the Member States and put in place strict safeguards for data protection for the new system.

Another consideration that I am putting forward to you to reflect on is that is with regard to the possible use of biometrics in the system. Based on a consistent EDPS approach that biometrics should be only used after an *ex ante* evaluation, I would strongly encourage the EU legislator to recourse to biometric data only after demonstrating the need and after a transitory period if there is solid evidence to prove that biometrics are necessary.

According to the current RTP Proposal the system is to be established on a voluntary basis where frequent travellers will be offered the possibility to apply for a faster border crossing.[4] I would like to comment on the fact that it might be difficult to consider "consent" as being given voluntarily and freely if the only alternative is long queues and administrative burdens in place. We should avoid the risk of discrimination for the vast amount of travellers who do not travel frequently or those travellers whose fingerprints may be unreadable if we assume that biometrics will be used by the system.

[4] See the RTP Proposal.

The law enforcement aspect and smart borders: a data protection view

Let me say very clearly from the start that these comments are not implying that the EDPS is supporting law enforcement access to this system. These comments are with a view to help the Union legislator to draft and justify legislation in a way that satisfies the requirements of the Charter, as interpreted by the Court of Justice.

Indeed the recent rulings of the Court in *Digital Rights Ireland* and, recently, in *Schrems* confirm the importance of a high level of data protection especially in connection with law enforcement and national security. I will touch in more detail on these consequences below.

The EDPS acknowledges that Europe is facing serious terrorist threats and has to take meaningful action. The combat against terrorism and serious crime is a legitimate interest pursued by the legislator and the EDPS, as an EU independent supervisory institution, is not a priori in favour or against any measure.

In the event that access for law enforcement authorities would prove to be necessary (based on solid evidence), 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 on the questions raised by the presidency

Since you all have the latest Presidency Note on Access for law enforcement purposes for the EES, I propose to follow the questions related to it point by point and I will try to comment each one where relevant for data protection.

I. Preliminary requirements

With regard to preliminary requirements to be exercised before the adoption of a new legislative proposal, I fully agree with the Presidency that a preliminary test (the so called the "Schecke test") should be applied to the EES as regards the possibility of law enforcement authorities' access to EES data.

Such a massive collection of personal data within border area needs profound justification. This justification is not established if the retention of all such information is only considered "a useful tool" for law enforcement authorities or if it just "helps" solving serious crimes. Current European law – including the Charter of Fundamental Rights - requires that the retention of such data is proportionate and strictly necessary for the purposes envisaged by it.

(Strictly) necessary means that the purposes of the privacy invasive measure can only be reached by applying that specific measure. A measure is not strictly necessary if the same or comparable results can be achieved by less-privacy intrusive means. The European Courts in Strasbourg and Luxembourg have been very clear on this point.

Necessity should be supported by clear evidence. In this sense I took note of a Presidency Note from 2013 in which you had provided several arguments for granting access law enforcement

access. As a member of the Italian judiciary I cannot contradict the fact that these types of data (entries and exits, names, tracking routes etc.) might be useful in an investigation.

However, I come back to the fact that the large majority of travellers are not suspected of any crime so I would link the necessity of access to their data to a suspicion that triggers the need for investigation. Moreover, these checks will be added to the checks against VIS for visa holders and SIS for all travellers in case of any alerts issued.

Article 52 of the Charter foresees that any limitation on the rights under Articles 7 and 8 must be provided for by law. In this respect, the jurisprudence of the European Court of Human Rights confirms that the law must be sufficiently precise to indicate to citizens in what circumstances and on what terms the public authorities are empowered to file information on their private life and make use of it.[5]

To find the existence of an interference with the fundamental right to privacy, it does not matter whether the information concerned is sensitive or whether the persons concerned have been inconvenienced in any way in practice[6]. In the EES case the personal data[7] which will be processed will be both alphanumeric and biometric (fingerprints and facial image) so storing their data for calculating the stay or for law enforcement purpose is interference with the rights guaranteed by Article 7 of the Charter.

The retention of personal data in the EES will affect in a comprehensive manner, all persons crossing the borders, but without the persons whose data are retained being, even indirectly, in a situation which is liable to give rise to criminal prosecutions. It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime.

So, it seems that the retention of data for law enforcement purpose will apply to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime. I can imagine the risks for privacy and data protection of such a huge data not only in terms of managing such a vast amount of data but

[5] EDPS Opinion of 20 December 2007, §24.

[6] See to that effect Cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk and Others*, paragraph 75.

[7] See Article 11 and 12 of Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union: http://ec.europa.eu/dgs/home-affairs/doc_centre/borders/docs/1_en_act_part1_v12.pdf . The personal data to be included in the EES is the surname (family name), surname at birth (earlier family name(s)), first name(s) (given names), date of birth, place of birth, country of birth, nationality or nationalities and sex, fingerprints for third country nationals exempt from the visa obligation (after three years after the system starts to operate).

also what happens if the security of the system is breached despite security safeguards applied (see for example the Danish incident for SIS[8]).

Furthermore, the access of the competent national authorities to the data constitutes interference. The fact that data will be retained for law enforcement purposes and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance as in the data retention case.

The Court of Justice considered in the *DRI*[9] case every collection, use and transfer to another authority as being a separate interference with fundamental rights and therefore needing a separate justification. This is fundamental in the EES case since law enforcement authorities will have access to data originally not collected for those purposes.

II. Purposes of the future EES Regulation

On the question of the purposes of the future EE Regulation, I agree with the Presidency text the EES purposes should be clearly and narrowly defined so as to be limited to terrorist offences and a clear list of other serious criminal offences.

III. Designated authorities

On this point, I would underline again the importance of having an prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions.

The Court of Justice, in the reasoning of its *DRI* judgement, examined the fact that "*the access by the competent national authorities to the data retained was not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued ".*[10]

On the specific issue of transparency, I would encourage you to publish and make public the list with the designated competent authorities and that this list should be kept up-to-date.

[8] http://www.theregister.co.uk/2013/06/07/pirate_bay_founder_named_as_suspect_in_paneuropean_police_database_hack/

[9] *DRI* judgement, §35.

[10] *DRI* judgement, §62.

IV. Granting access to EES of the LEA – considering whether the request for access, as well the urgency of the case, have to be motivated specifically

As I have just mentioned earlier, the Court of Justice stated in the *DRI* judgment that an independent body should review the access to the data. I would see that this it is only possible only based on a justification provided both for ordinary and urgent cases. The criteria for treating a case as "urgent" should be clearly defined.

V. Conditions that should be met for access to EES of the LEA

In some references in the Presidency Notes circulated earlier or on the last one discussed today, Eurodac and VIS provisions have been mentioned as a possible model or re-usable for the EU legislator as regards the conditions for access for LE purposes.

I may say that I am reluctant about the compatibility of some the current set of provisions regulated by the Eurodac Regulation on access for law enforcement purposes.

The main justification is based on the fact that although the main purpose of Eurodac does not serve LE purposes, Regulation 603/2013 still establishes the possibility of access in specific cases to data that are stored up to 10 years for original asylum purposes, including minors' data. The stigmatising effect, the violation of the presumption of innocence, the very long storage period and the fact that the verifying authorities are not independent courts as required by the Court in the context of DRI judgments, represents elements of doubt as regards the compatibility of the current LE access to Eurodac data.

The same reasoning could apply to the VIS provisions[11] as regards the oversight of verifying authorities and transfer of data to third countries.

On the substance provided in the Presidency Note, I welcome the discussion on the conditions to have access after exhausting the searches also by conducting prior searches where less intrusive and technically available. In case that biometric (fingerprints) will be used I recommend you to take into account the consequences of having false matches when checking latent fingerprints which could lead to wrongful implication of innocent persons in criminal investigations.

Moreover, clear criteria are needed in order to ensure the link between a suspected person and the need to check his or her data against the EES system.

I am also in favour of explaining the issues of how to ensure follow-up after getting a hit from the system. The need for additional information should be clarified. The information to be

[11] See Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences.

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32008D0633

transmitted should be limited to the strict minimum necessary for the purpose for which access has been carried out.

VI. Data retention periods in particular for LE purposes

With regard to the retention periods, I would like to reflect with you if would not be possible to have a solution where the retention period for law enforcement purposes (if proved to be necessary) can only start after the border related purpose expired and there are suspicions that maybe a traveller is connected to a serious crime offence or a terrorist offence. This could mean different option to think of, such as flagging persons as "of interest", so that their data are prolonged in order to be kept for longer. In these cases a retention period based on criteria such as how much time an investigation is needed to solve a crime in the EU on average could be taken into account where there is a suspicion that someone is connected to criminal acts as mentioned above.

In the case of what happens to data once the subject has acquired international protection, residence permit or becomes a member of an EU citizen family, I would reflect on a solution which already exists in the Eurodac Regulation: the advance erasure procedure[12].

On the Presidency question of what will happen to the data after a defined retention period I would recommend it is irreversibly deleted since there is no purpose to keep it unless it is necessary to be prolonged criminal investigation purposes if in accordance with the EES Regulation. This is in line with the DRI judgement where the Court mentioned the EU law applicable did not require the irreversible destruction of the data at the end of the data retention period[13].

In conclusion on the LE issue, I would “provoke” you to consider keeping the current provision from the 2013 EES proposal as to have an evaluation of law enforcement access after two years after the EES system have been put in place. Then, the live system will be tested against its original purpose for its reliability and efficiency and only then the necessity of law enforcement access should be evaluated. In other words, only after it has been proven that the smart borders package works for its initial purpose, you can start thinking about using it for other purposes.

[12] See Article 13 Eurodac Regulation:

Advance data erasure

1. Data relating to a person who has acquired citizenship of any Member State before expiry of the period referred to in Article 12(1) shall be erased from the Central System in accordance with Article 27(4) as soon as the Member State of origin becomes aware that the person concerned has acquired such citizenship.

2. The Central System shall, as soon as possible and no later than after 72 hours, inform all Member States of origin of the erasure of data in accordance with paragraph 1 by another Member State of origin having produced a hit with data which they transmitted relating to persons referred to in Article 9(1) or 14(1).

[13] *DRI* judgement, §67.

Specific conclusions on the LE purposes

Let me recall the main ideas explored together today as regards the possibility of LE having access to smart borders data:

1. I am not favouring a particular position or decision and these remarks are without prejudice to the fact that EDPS expressed reservations on the LE access to EES.
2. Solid evidence required for proving the necessity. We took note of your efforts to provide statistics on the need for such an access and we look forward to the newly arriving Impact Assessment to see the evidence there.
3. LE purposes should be clearly defined.
4. Designated authorities should be reviewed by a court or an administrative body in line with the DRI judgment.
5. The criteria for treating a case as "urgent" should be clearly defined.
6. As regards the conditions of having access to the EES data, clear criteria are needed in order to ensure the link between a suspected person and the need to check his or her data against the EES system.
7. Data retention periods should respect necessity and proportionality principles. Once the purpose disappeared we should apply the DRI statement that data should be irreversibly destructed.

Final remarks

I welcome the debate on the smart borders with you; this will help better understanding the data protection perspective for this major legislative proposal(s).

Let me recall the need of cooperation with the national data protection authorities and that we are available for further expertise on data protection in the months to come. I also look forward to the final results of the Pilot Phase.

In the end, the key question is how to put forward a “smarter” borders package (better than first proposal) which should take the data protection principles and safeguards into account.

You have seen from my comments that while Europe is tempted now to *maximise* the collection of a huge amount of information concerning normal people to be used “just in case” the EU law architecture (EU Treaty and the Charter) is based on the principle of minimisation of large scale databases interfering with data subjects’ rights. The right balance in between those two trends is our common challenge.

I look forward to working with you more closely towards the right solutions.

I thank you very much again to the Presidency for inviting me here, the Council Secretariat and all delegations present here today. Last but not least, I give special thanks to the interpreters.