European Commission - Fact Sheet

Smart Borders Package: Questions & Answers

Brussels, 6 April 2016

Smart Borders Package: Questions & Answers

The Smart Borders Package:

What are the elements of today's Smart Borders package?

The Smart Borders package includes: a Communication on 'Stronger and Smarter Information Systems for Borders and Security'; a Regulation for the establishment of an Entry-Exit System; a proposed amendment to the Schengen Borders Code to integrate the technical changes needed for the Entry-Exit System.

What is the purpose of the Smart Borders package?

The Smart Borders package will modernise the Schengen area's external border management by improving the quality and efficiency of border crossing processes. It aims to help Member States deal with increasing traveller flows, without necessarily increasing the number of border guards, and to promote mobility between the Schengen zone and third countries in a secure environment, while contributing to the fight against terrorism and serious crimes.

In 2015, more than 50 million non-EU nationals visited the EU for tourism, business or educational purposes, accounting for more than 200 million border crossings at the external borders of the Schengen area. EU citizens accounted for around 400 million external border crossings.

Are these proposals a response to the refugee crisis and recent terrorist attacks?

The Smart Borders package is not a direct response to the refugee crisis, although it contributes to the overall strengthening of our border management. The Entry-Exit System deals with the recording of short-term legal stays of third country nationals, which is not the most common path of entry for asylum seekers. At the same time, the Entry-Exit System will contribute to the fight against irregular migration (e.g. the phenomenon of 'over-stayers'). The access to the Entry-Exit System by law enforcement authorities will constitute an additional instrument to prevent and combat terrorism and serious crime, by tracking travel patterns and combatting document and identity fraud.

The Communication on Stronger and Smarter Information Systems presents the way forward on how information systems can be developed to ensure that border guards and police officers have the necessary information at their disposal to enhance external border management and internal security in the EU.

What are the links between the proposals and the European Agenda on Migration and the European Agenda on Security?

In 2015 the revision of legislative proposals on Smart Borders was announced in both the European Agenda on Migration and the European Agenda on Security.

The European Agenda on Security underlines that common high standards of border management are essential to prevent cross-border crime and terrorism. It underlines that the revised proposal on Smart Borders will help to increase the efficiency and effectiveness of border management. It also underlined the importance of ensuring better information exchange, including through keeping existing instruments under review and filling gaps in coverage.

The European Agenda on Migration stresses that in order to manage the external Schengen borders more efficiently there is a need to make better use of the opportunities offered by IT systems and technologies. It refers to the three existing systems: Eurodac (to deal with the administration of asylum), VIS (for managing visa applications) and SIS (for sharing of information on persons and objects for which an alert has been created). The Entry-Exit System represents a new tool for increasing the efficiency of border crossings and facilitating crossings for *'bona fide'* travellers, whilst at the same time strengthening the fight against irregular migration by creating a record of all cross-border movements by third country nationals.

The Communication on Stronger and Smarter Information Systems for Borders and Security builds on the synergies between the two Agendas.

The Communication on 'Stronger and Smarter Borders':

What is the purpose of the Communication?

The Communication on 'Stronger and Smarter Information Systems for Borders and Security' explores how information systems can become more effective and efficient to enhance external border management and internal security in the EU. The Communication looks at ways to improve existing systems, identifies gaps where they exist, and highlights the crucial importance of interoperability (while respecting data protection safeguards).

What are the main information systems for border management in the EU?

The three main centralised information systems developed by the EU in relation to borders are the Schengen Information System (SIS), EURODAC, and the Visa Information System (VIS).

These three systems are complementary, and - with the exception of SIS – primarily targeted at third country nationals.The systems also support national authorities in fighting crime and terrorism. This applies in particular to the SIS as the most widely-used information-sharing instrument today. Information exchange for these systems is carried out in a secured dedicated communication infrastructure called sTESTA

In addition to these existing systems, the Commission proposes to establish a fourth centralised border management system, the Entry-Exit System (EES), which is expected to be implemented by 2020, again addressing third-country nationals.

Additional existing instruments for border management are Interpol's Stolen and Lost Travel Documents (SLTD) database and the Advance Passenger Information (API) that collects information on passengers ahead of inbound flights to the EU. These instruments are relevant to both EU citizens and third country nationals.

Specifically for law enforcement, criminal investigation and judicial cooperation purposes, the EU developed decentralised tools for information exchange, namely (i) the Prüm framework to exchange DNA, fingerprints and vehicle registration data, and (ii) the European Criminal Records Information System (ECRIS) to exchange national criminal record information. ECRIS enables the exchange of information, through a secured network, on previous convictions handed down against a specific person by criminal courts in the European Union.

Europol supports the exchange of information between national police authorities as the EU criminal information hub. The Europol Information System (EIS) provides a centralised criminal information database for Member States to store and query data on serious crime and terrorism. Focal Points at Europol provide subject-focused analysis work files with information on ongoing operations in Member States. Europol’s Secure Information Exchange Network Application (SIENA) allows Member States to exchange information in a swift, secure and user-friendly way with each other, with Europol, or with third parties that have a cooperation agreement with Europol.

An additional set of personal data processing systems that will be developed across Member States is the Passenger Name Records (PNR). PNR data consists of booking information provided at the time of booking and check-in.

Finally, customs authorities are also a crucial actor in the multi-agency cooperation at the external borders. They have various systems and databases which contain data on movements of goods, identification of economic operators and risk-related information that can be used to reinforce internal security

Figure 1 *Schematic overview of the main information systems for border management and law enforcement - see attachment.*

How can information systems for border management be further improved?

The current architecture for border control and security in the European Union is marked by fragmentation due to the different contexts in which the systems have been developed. Information is stored separately in various systems. There is inconsistency between databases and access to data diverges between different relevant authorities. This can lead to blind spots notably for law enforcement authorities. It is therefore necessary and urgent to work towards integrated solutions for improved accessibility to data for border management and security, in full compliance with fundamental rights.

A number of information systems already provide border guards and police officers with relevant information. These systems should become complementary. Overlaps should be avoided and any existing overlap should be eliminated. Existing gaps in the EU's architecture of data management need to be addressed.

Where necessary and feasible, information systems should be interoperable. Simultaneous searches of systems should be facilitated by establishing a single search interface at national level which respects the different purposes for access and authorised access, to ensure that all relevant information is available to border guards and/or police officers when and where this is necessary for their respective tasks.

How will respect of fundamental rights, data protection rules and the principle of purpose limitation be guaranteed?

Full compliance with fundamental rights and data protection rules requires well designed and correctly-used technology and information systems.

Technology and information systems can help public authorities to protect the fundamental rights of citizens. Biometric technology can reduce the risk of mistaken identities, and of discrimination and of racial profiling. It can also contribute to addressing protection risks for children such as children going missing or falling victims of trafficking, provided it goes hand in hand with Fundamental Rights safeguards and protection measures. It can reduce the risk of people being wrongfully apprehended and arrested. It can also contribute to increasing the security of citizens residing in the Schengen area as it will help in the fight against terrorism and serious crime.

All information systems must comply with data protection principles and the requirements of necessity, proportionality, purpose limitation and quality of data. Safeguards must be in place to ensure the rights of the data subjects in relation to the protection of their private life and personal data. Data should only be retained for as long as necessary for the purpose for which they were collected.

Purpose limitation is a key principle of data protection. With the new comprehensive framework for the protection of personal data in the EU in place and considering the significant developments in technology and IT security, the principle of purpose limitation can be more easily implemented at the level of specific access and use of data stored in compartments within one system.

'Data protection by design' and 'Data protection by default' are driving principles of EU data protection rules. When developing new instruments that rely on the use of information technology, the Commission and eu-LISA will follow this approach.

The requirements of the Charter of Fundamental Rights and in particular the new Data Protection reform instruments will guide the Commission in addressing the gaps and shortcomings in the area of data management for border control and security. This will ensure that further development of information systems in these areas will be in line with the highest standards of data protection.

A revised proposal for a Regulation for an Entry-Exit System and a revised proposal for a Regulation amending the Schengen Borders Code:

What is the Entry-Exit System?

The proposed Entry-Exit System will apply to third country nationals - both visa-required and visa-exempt travellers - admitted for a short stay (maximum 90 days in any 180 day period) in the Schengen area. The system will collect data (identity and travel documents) and register entry and exit records (date and place of entry and exit) to facilitate border crossing of *bona fide* travellers and identify over-stayers. The Entry-Exit System will also record entry refusals.

What are the objectives of the Entry-Exit System?

The Commission has proposed the establishment of an Entry-Exit System to:

- modernise external border management by improving the quality and efficiency of the Schengen Area external border controls;
- help Member States dealing with ever increasing traveller flows without having to increase the number of border guards;
- systematically identify over-stayers (individuals remaining in the Schengen Area after the end of their authorised stay); and
- reinforce internal security and the fight against terrorism and serious crime.

What will the Entry-Exit System deliver?

The new System will provide:

- precise information in a rapid and automated way for border guards during border checks, replacing the current slow and unreliable system of manual stamping of passports; this will allow for a better monitoring of the authorised stay as well as more efficient border checks;
- information to border guards on entry refusals of third country nationals and enable entry refusals to be checked electronically in the Entry-Exit System;

- precise information to travellers on the maximum duration of their authorised stay;
- precise information on who has over-stayed beyond their authorised stay, which will support controls within the territory, apprehension of irregular migrants and the return process;
- precise data to assess the number of over-stayers per nationality, which is an important factor in deciding to impose or lift visa obligations on a third country;
- automated border controls for third country nationals under the supervision of border guards, by abolishing the manual element of stamping of passports.

As regards access for law enforcement purposes, the Entry-Exit System will:

- support the identification of terrorists, criminals, suspects and victims;
- provide a record of the travel history of third country nationals including criminal suspects, perpetrators or victims. It would thus complement the information in the SIS.

Why are the proposals being revised and what are the main differences with the 2013 proposals?

The main differences between the revised proposals and the 2013 proposals are:

Architecture of the system: only one system is proposed, the Entry-Exit System.

Interoperability between the Entry-Exit System and VIS (Visa Information System): in order to achieve more efficient and rapid border checks a connection will be established between the central systems of the Entry-Exit System and the VIS with direct access between them defined for specific purposes.

Biometric identifiers: while the 2013 Entry-Exit System proposal relied on ten fingerprints, the revised Entry-Exit System proposal uses a combination of four fingerprints and the facial image as biometric identifiers. Biometrics are used from the start of operations of the System. Considering the expected size of the Entry-Exit System, the choice of biometric identifiers allows for sufficiently accurate verifications and identifications while keeping the amount of data to a reasonable level.

The facilitation of border crossings: the approach for facilitation is based on the implementation of self-service systems and e-gates, which allows third country nationals to initiate the procedure for border clearance, to be completed by providing additional information to the border guard on request. The use of these accelerators is optional for Member States, open to most of the travellers and does not require the development of any new system.

Personal data protection: there is a significant reduction in the volume of personal data recorded in EES: 26 data items are to be recorded in Entry-Exit System instead of 36 under the 2013 proposals.

The data retention period: The retention time for stored data is five years for all purposes. The five year data retention period reduces the re-enrolment frequency and is beneficial for all travellers, while allowing the border guard to perform the necessary risk analysis required by the Schengen Border Code before authorising a traveller to enter the Schengen area.

Law enforcement access: from the start of operations, Member States' law enforcement authorities and Europol will have access to the EES, under strictly defined conditions.

The costs: in the 2013 proposals, €1,1 billion was set aside as an indicative amount for the development of an Entry-Exit System and a Registered Traveller Programme. For the revised proposal the amount needed has been estimated at €480 million.

How will the Entry-Exit System facilitate border crossing for travellers?

To reduce border crossing time for third country nationals and workload for border guards, the Entry-Exit System proposal gives Member States the possibility to automate most data- and information-capturing steps as well as data verifications. By using **self-service kiosks** travellers can verify whether their data are still recorded in the System, have their picture taken (or alternatively one fingerprint checked) and answer a set of questions. Once the travel document is scanned in the self-service kiosks all mandatory checks are triggered versus security databases.

The traveller is then guided to a border control lane where the border guard has in the meantime received the answers from the security databases, the confirmation of the traveller's identity, the remaining duration of stay of the traveller and the traveller's answers to the set of questions formulated in the self-service kiosk. The border guard may ask further questions before deciding to grant (or refuse) access to the Schengen area.

The benefit for travellers is the automated preparation of the border check before they reach the border guard, whereas previously they would have been simply standing in line and waiting. The overall benefit for all travellers, including the ones not using the kiosks, is that queues become shorter once a sufficient number of travellers go through pre-clearance at a kiosk. The advantage for border guards is that the automation of these steps, which today take between one third to half of the time with the traveller, are removed and that he/she can concentrate on assessing the individual's situation.

Moreover, Member States may create national registered traveller's programmes on a voluntary basis. The proposal describes the conditions these programmes must meet. These essentially consist in pre-vetting frequent travellers to a specific country (or airport) in the Schengen area. Their border control check then becomes limited to verifying their identity and nationality, the validity and authenticity of the travel document, the validity of their registered traveller's status, the validity of their visa where applicable and the verification that they are not likely to jeopardise the public policy, internal security, public health or international relations of any of the Member States (in particular by consulting Schengen Information System (SIS) alerts) and, where applicable, the validity of their visa or residence permit and that the maximum duration of authorised stay has not been exceeded.

What are the consequences of abolishing the current passport stamping obligation?

As a general rule, third country nationals fulfilling entry conditions have the right to enter for a short stay of up to 90 days within any 180 day period. Currently the stamping of the travel document indicating the dates of entry and exit is the sole method available to border guards and immigration authorities to calculate the duration of stay of third country nationals and to verify if someone is over-staying. These stamps can be difficult to interpret: they may be unreadable or the result of counterfeiting. Similarly, it is difficult for consulates having to process visa applications to establish the lawfulness of previous visas on the basis of stamps present in the travel document. As a result, the whole procedure is considered error prone and not always systematically implemented.

The introduction of the Entry-Exit System ensures:

- precise information, rapidly delivered on demand to border guards during border checks, by replacing the current slow and unreliable system of manual stamping of passports; this allows for both a better monitoring of the authorised stay as well as more efficient border checks;
- information to border guards on entry refusals of third country nationals and allows for entry refusals to be checked electronically in the Entry-Exit System;
- precise information to travellers on their remaining authorised length of stay to cover their intended stay in the territory of a Member State easily accessible via a website;
- the possibility for using automated border controls for third country nationals under the supervision of the border guards.

What is the interoperability between the Entry-Exit System and the Visa Information System (VIS)?

The Entry-Exit System will be used by the same authorities that are already using VIS (in particular consular posts and border control). The Entry-Exit System Regulation provides for the possibility that the central Entry-Exit System accesses VIS and that reciprocally VIS accesses EES. This reduces the duplication of personal data processing in accordance with the 'privacy by design' principle.

Which biometric identifiers will the Entry-Exit System use?

For visa holders, the Entry-Exit System stores only their facial image (as their fingerprints are already registered in the VIS). For visa exempt travellers the System uses a combination of four fingerprints and the facial image as the biometric identifiers. This choice of biometric identifiers allows for accurate identification of travellers and results in a reduction of the data recorded in the system while speeding up border controls and enabling a wider use of self-service systems at border crossing points.

How does the Entry-Exit System ensure data protection?

The data stored in the EES is protected against the risk of abuse, as access to the Entry-Exit System is restricted to specific persons within designated competent authorities. The transfer of data to third parties, whether private or public entities, is prohibited, and all data processing is done by the EU Agency for the Operational Management of large-scale IT Systems (eu-LISA) or by the Member States. Furthermore, strong safeguards and mechanisms are in place for the effective protection of the personal data rights of travellers:

- travellers have the right of access, rectification and deletion of their personal data stored in the System;
- the supervision of the Entry-Exit System is ensured by both the European Data Protection Supervisor and the independent national supervisory authorities;
- the Entry-Exit System will be built in accordance with the principles of data protection by design and by default.

How will the new system improve security for EU citizens?

Access to the Entry-Exit System will be granted to law enforcement authorities in order to:

- support the identification of suspects, perpetrators or victims of terrorist offences or of other serious criminal offences in specific cases,
- provide a record of the travel history of third country nationals admitted or refused for a short stay in the Schengen area, including perpetrators, suspects or victims of terrorist offences or of other serious criminal offences.

In general, identification is essential for law enforcement authorities in their mission to prevent and combat terrorism and other serious crime. While data on EU citizens exists in different databases in Member States that are in general accessible to law enforcement authorities, there is an information and verification gap concerning third country nationals who are not covered by the Visa Information System (VIS). The use of Entry-Exit System data for identity verification would reduce the identification and verification gap concerning third country nationals who are not in the VIS.

The Entry-Exit System contains reliable data on entry and exit dates of all third country nationals admitted for a short stay in the Schengen area. It will therefore meet the need of Member States' law enforcement authorities and Europol to complement their existing criminal intelligence sources with the dates and locations of entry and exit from the Schengen area in duly justified cases.

What happens next with these proposals?

The legislative proposals of the Smart Borders package will now be transmitted to the European Parliament and Council for adoption. The Commission counts on the co-legislators' support for a rapid adoption of its proposal by the end of 2016, and invites Member States to start taking the necessary steps for the future Entry-Exit System to come into effect by 2020.

The Communication on 'Stronger and Smarter Information Systems for Borders and Security' is the beginning of a process for which the Commission will set up an Expert Group on IT Systems and Interoperability at senior level with EU agencies, national experts and institutional stakeholders. Following the findings of the Expert Group, the Commission will present further concrete ideas to the European Parliament and the Council as basis for a joint discussion on the way forward. The Commission will also seek the input of the European Data Protection Supervisor and national data protection authorities.

The goal should be the development of a joint strategy to make data management in the EU more effective and efficient, in full respect of data protection requirements, to better protect its external borders and enhance its internal security, for the benefit of all citizens.

MEMO/16/1249

Press contacts:

Markus LAMMERT (+ 32 2 298 04 23)
Natasha BERTAUD (+32 2 296 74 56)
Tim McPHIE (+ 32 2 295 86 02)
Tove ERNST (+32 2 298 67 64)

General public inquiries: Europe Direct by phone 00 800 67 89 10 11 or by email

Attachments

Smart Borders Questions and Answers - graphic.pdf