Entry/Exit System (EES)

2016/0106(COD) - 25/10/2017 - Text adopted by Parliament, 1st reading/single reading

The European Parliament adopted by 477 votes to 139 with 50 abstentions, a legislative resolution on the proposal for a regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011.

The European Parliaments position adopted at first reading, following the ordinary legislative procedure, amended the Commission proposal as follows:

Purpose: the proposed regulation aims to establish an Entry/Exit System (EES) for:

- the recording and storage of the date, time and place of entry and exit of thirdcountry nationals crossing the borders of the Member States at which the EES is operated;
- the calculation of the duration of the authorised stay of such third-country nationals;
- the generation of alerts to Member States when the authorised stay has expired; and
- the recording and storage of the date, time and place of refusal of entry of third-country nationals whose entry for a short stay has been refused.

Scope: in order to verify compliance with the provisions on the authorised period of stay on the territory of the Member States, the EES will apply to third country nationals crossing the external borders of the Schengen area, both those requiring a visa and those visa-exempt, admitted for a short stay of 90 days in any 180 day period.

The system will replace the obligation to stamp the passports of third-country nationals, which is applicable to all Member States.

Implementation: the amended text provides that the EES should be operated at the external borders of the Member States that apply the Schengen acquis in full. It will also be operated by Member States not yet applying the Schengen acquis in full, but for whom:

- the verification in accordance with the applicable Schengen evaluation procedure has already been successfully completed;
- passive access to the Visa Information System (VIS) has been granted;
- the provisions of the Schengen acquis relating to the Schengen Information System (SIS), have been put into effect in accordance with the relevant Act of Accession.

Accordingly, Bulgaria and Romania will operate the EES.

Data: the EES should record and process alphanumeric data and biometric data primarily for the purposes of improving the management of external borders, preventing irregular immigration and facilitating the management of migration flows. It will also be possible to access personal EES data in order to contribute to the prevention, detection and investigation of terrorist offences and of other serious criminal offences. Any search must be duly justified and proportionate in the light of the interest invoked.

Four fingerprints per visa-exempt thirdcountry national should be registered in the EES, if physically possible. The fingerprints of visa-holding third-country nationals should be checked against the VIS. The facial image of both visa-exempt and visa holding third-country nationals should be registered in the EES.

The data retention period is set at three years. If there is no exit record following the date of expiry of the period of authorised stay, the data shall be stored for a period of five years.

The use of the EES, including the capturing of biometric data, must be in accordance with the safeguards laid down in the Convention for the Protection of Human Rights and Fundamental Freedoms, in the Charter of Fundamental Rights of the European Union and in the United Nations Convention on the Rights of the Child.

Access to data: data stored in the EES will be accessible to border authorities, consular officers dealing with visas and authorities that check, within the territory of the Member States whether the conditions for entry to, or stay on, the territory of the Member States are fulfilled.

For the purposes of the prevention, detection and investigation of terrorist offences or of other serious criminal offences, Member States designated authorities and Europol may obtain access to the EES for consultation.

Technical architecture of the EES: the EES will be comprised of the following:

- a Central System (EES Central System) which operates a computerised central database of biometric and alphanumeric data;
- a National Uniform Interface in each Member State, enabling the connection of the EES Central System to the national border infrastructures in Member States in a secure manner;
- a Secure Communication Channel between the EES Central System and the VIS Central System;
- a secure and encrypted Communication Infrastructure between the EES Central System and the National Uniform Interfaces;
- a web service to allow: (i) thirdcountry nationals to verify at any moment the remaining authorised stay; (ii) carriers to verify whether third-country nationals holding a Schengen short-stay visa issued for one or two entries have already used the number of entries authorised by their visa;
- a data repository established at central level in order to enable the generation of statistics and reporting.

Eu -LISA shall establish a Secure Communication Channel between the EES Central System and the VIS Central System to enable interoperability between the EES and the VIS.

Communication of data to third countries: the amended text provides for the possibility of transferring personal data obtained by Member

States to third countries: (i) in an exceptional case of urgency; (ii) where there is an imminent danger associated with a terrorist offence or where there is an imminent danger to the life of a person associated with a serious criminal offence. An imminent danger to the life of a person should be understood as covering a danger arising from a serious criminal offence committed against that person such as grievous bodily injury, illicit trade in human organs and tissue, kidnapping, illegal restraint and hostage-taking, sexual exploitation of children and child pornography, and rape.

Such data should only be transferred to a third country if the reciprocal provision of any information on entry/exit records held by the requesting third country to the Member States operating the EES is ensured.