Council of the European Union

Brussels, 8 October 2015
(OR. en)

12531/15

Interinstitutional File:
2013/0057 (COD)

LIMITE

FRONT 205
VISA 320
ENFOPOL 267
CODEC 1272
COMIX 454

NOTE

From:	Presidency
To:	Working Party on Frontiers/Mixed Committee (EU-Iceland/Liechtenstein/Norway/Switzerland)
Subject:	Access for law enforcement purposes to the EES

In the context of the meeting of the Strategic Committee on Immigration, Frontiers and Asylum (SCIFA) on 24 September 2013, a large majority of delegations agreed that access to the Entry-Exit System (EES) for law enforcement authorities (LEA) should be provided as of the start of the operation of the future system. It was further agreed that such access should be introduced as an ancillary objective in the draft Regulation and should be purpose - limited to the prevention, detection and investigation of terrorist and other serious criminal offences. SCIFA invited the Working Party (WP) on Frontiers to proceed further with this matter on the basis of the guidelines agreed during the above meeting.

Since then, the WP has pursued work with a view to ensuring that the introduction in the EES of access for LEA would serve the aforementioned purpose, while such access would be constructed under the appropriate conditions and guarantees and in full compliance with the principles of necessity and proportionality as spelled out by the ECJ case-law. To this effect, this issue was presented and discussed at several meetings of the WP on Frontiers, focusing on legal and practical questions, and delegations were asked to provide practical examples based on their experiences from the use of own national EES or other systems such as VIS, which would justify and corroborate the granting of access to LEA. It could also be recalled that COREPER, on the occasion of the adoption of the political guidelines for the Smart Borders pilot project in December last, mandated the WP on Frontiers to focus on the issue of access for LEA as an important policy element.

The former Latvian Presidency submitted to this WP doc. 8743/15, which included a number of questions raised by the Commission as part of the proportionality test. The WP took note of these concerns at its meeting of 22 May 2015.

At the experts' meeting convened by the Commission on 9 July 2015, a thorough exchange of views took place on the basis of a questionnaire that had been sent to the participants, with relation to, among other things: i) the possibility of the use of the future EES as a criminal identification and investigation tool, ii) the data that should be inserted in the system, the data to be used for searches of the system and the data that should be obtained as a result of a hit, iii) the minimum retention period for access to LEA purposes and, iv) the possibility of transfer of EES data to third countries in the context of the fight against terrorism and serious crime. The conclusions drawn from this meeting could be useful to the Commission in its preparation for the impact assessment and further on the submission of its new EES proposal.

In light of the above-mentioned considerations and in order to provide the Commission with the views of this WP on the important parameters of the access for LEA in the preparation of the new EES proposal, the Presidency suggests the following as a way forward: on the basis of the work already done by the former Italian Presidency, certain ideas are submitted regarding the necessary elements for future provisions along with a list of safeguards that need to be enshrined in accordance with ECJ law case requirements in relation to the setting up of EU big scale data collection systems.

Delegations are therefore invited to discuss the suggested elements concerning access for LEA to the EES and the list of the relevant conditions and safeguards which will need to be met. It should also be taken into account that these elements are not exclusive and further issues may need to be addressed (such as the transfer of data to third countries) in the access for LEA framework.

Preliminary requirements:

Before the adoption of legislative provisions allowing access for LEA to the EES, a preliminary test - the so-called "Schecke test"[1]- should be carried out on the basis of the relevant ECJ case-law in order to balance the different interests at stake. This right balance should be struck between, on the one hand, the objectives of general interest recognised by the Union regarding the fight against terrorist offences and other serious criminal offences, including the fundamental rights attached to these objectives, and, on the other hand, the fundamental rights linked to the right to respect for private and family life and the right to protection of personal data for the persons concerned. In the context of the same test, it should also be confirmed that there cannot be any alternative and less intrusive measures, which would affect less adversely the data protection rights and which could still contribute effectively to the crime-fighting objectives.

Suggestions with regard to the elements of substance of the future provisions, along with the ECJ case-law tests

1. In the context of the provision on the subject matter of the future EES Regulation, the conditions under which Member States' designated law enforcement authorities and the European Police Office (Europol) may obtain access for consultation of the EES for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, should be clearly defined. It is noted that, in accordance with the relevant ECJ case law, these access conditions and procedures should be spelled out in a precise way so as to protect the persons concerned against their arbitrary application.

[1] Named after the Joined cases C-92/09 and C-93/09, Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen. Protection of natural persons with regard to the processing of personal data, resulting from Articles 7 and 8 of the Charter of Fundamental Rights of the EU.

2. In relation to the purposes of the future EES Regulation, the aforementioned purposes should be clearly and narrowly defined so as to be limited to specified terrorist offences and other serious criminal offences, and should be subject to clear-cut conditions (as discussed below). Particular attention, in accordance with the case-law, should be given to check if any elements of such definition would be left at the discretion of the Member States.

3. As **regards the designated authorities**[1]**,** Member States should nominate them with a view to entitling special units to obtain access for consultation of the data stored in the EES, pursuant to the future Regulation. These designated authorities could be authorities of the Member States which are responsible for the prevention, detection or investigation of terrorist offences or of other serious criminal offences. Each Member State should keep a list of the designated authorities, which should be duly notified. For the same purposes, each Member State should designate one or more operating units,[2] or central access points[3] also duly notified, through which access would be done and which should ensure that the conditions to request access to the EES laid down in the relevant provisions would be fulfilled.

Appropriate attention should be paid to ensure that the central access points act independently when performing their tasks.

Important concerns include the following:

– whether there are any criteria, conditions for the Member States as to what authorities may be designated for the purpose of access (e.g. related to the adequacy of their scope of competences to the purpose);

---

1 This term is used mutatis mutandis on the basis of Art. 5 of the Eurodac Regulation (Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013).

2 See Art. 5(3) of the Eurodac Regulation.

3 See Art. 3(3) of the Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the VIS for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences.

– whether the designation of different entities should be made separately for each of the purposes;

– whether intelligence agencies or other specific types of administration units should be authorised to act as designated authorities;

– the need to clarify the national procedure of designation of the authorised authorities/entities (which body will designate them);

– whether a list of such entities should be public and be updated regularly;

– whether there should be any limitation/definition of who (within the authorised authority) would have access to the data;

– what guarantees should apply for the independence of the verifying/authorising authority.

The provisions regarding the designated authorities and the respective case-law tests should apply by analogy to **Europol**.

4. With regard to the granting of access to EES of the LEA, the aforementioned operating units should submit a reasoned electronic request to the central access points for access to specific sets of data stored in the EES. Upon receipt of a request for access, the central access point(s) should verify whether the relevant conditions for access are fulfilled. If this is the case, the duly authorised staff of the central access point(s) should process the requests and transmit the data accessed to the operating units in a secure way. In exceptional cases of urgency, a faster procedure with an ex-post verification could be followed. The future EES Regulation should set out a general framework and leaving details to be defined in national law.

In accordance with the ECJ case-law, it should be considered whether the request for access, as well as the urgency of the case, have to be motivated specifically.

5. With regard to the conditions that should be met for access to EES of the LEA, the following issues should be stressed:

– access for consultation must be necessary for the aforementioned purposes, which means that there must be an overriding public security concern which makes the searching of the database proportionate;

– access for consultation must be necessary in a specific case;

– there are reasonable grounds to consider that consultation of EES data will substantially contribute to criminal investigations or criminal intelligence operations[1] related to terrorist offences and other serious criminal offences.

– a prior search has been conducted in national databases and international data systems which are considered less intrusive and are technically available, unless the Member State concerned will be able to justify that there are reasonable grounds to believe that it would not contribute to the criminal investigation.

In accordance with the ECJ case-law, the threshold, in terms of factual basis for showing suspicion of committing a crime, required in order to grant the requested access, should be clarified.

In the same context, the EES data that could be consulted by the LEA shall also be limited and clearly defined, as well as the exact kind of searches that should be allowed. It should also be considered to introduce the possibility of searching the EES for the entry/exit records, in duly motivated cases, even if the identity of the person has been established in national databases already.

Furthermore, in relation to whether the consultation of the EES could, in the event of a hit, give access to all of the aforementioned data stored in the EES, the following issues should be clarified in accordance with the ECJ case law:

[1] See definitions in Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the EU.

– what kind of access to give, once the requesting authority is cleared for access;

– whether access would be provided to the whole EES, or there would be a "hit based' access limited to the records concerned;

– whether there should be any procedures on "false" hits and their follow-up.

6. With regard to the retention period of data in particular for law-enforcement purposes, the following elements could be considered:

– the length of the retention period, limited to what it is strictly necessary for the purposes of the EES;

– the start of running of the retention period, the possibility to extend the time-limit and if possible, under which situations;

– whether there should be an automatic deletion by the central system of the data or a specific action of some authority ("owner" of the record) would be required;

– whether the retention period of different categories of data could depend on and be adapted to their relevance/usefulness for a given purpose;

– the question of what should happen to data once the data subject acquires international protection, residence permit, becomes member of family of an EU citizen or EU citizen himself; etc.;

– whether the period of accessibility of data should depend on the purpose for which it will be sought (i.e. shorter for less crucial purposes e.g. border management, fighting illegal immigration and longer retention periods with regard to serious crimes e.g. terrorism). In the same context, whether alternative solutions, such as masking of data for a certain period and access only for specific purposes, should be considered in this context;

– whether, after a defined (retention) period, the data should be: (i) accessible only upon a specific authorisation or judicial order? (ii) irrevocably anonymised? or (iii) irreversibly deleted/destructed?

Delegations are invited to consider the above issues, with a view to enhancing the discussion on the issue of access to the EES for LEA and assisting the Commission in its preparation of the future proposal.