Council of the European Union

Brussels, 8 July 2014
(OR. en)

11337/14

Interinstitutional File:
2013/0057 (COD)

LIMITE

FRONT 139
VISA 160
ENFOPOL 193
CODEC 1534
COMIX 351

OUTCOME OF PROCEEDINGS

From:	Working Party on Frontiers/Mixed Committee (EU-Iceland/Liechtenstein/Norway/Switzerland)
On:	18 June 2014
Subject:	Access for law enforcement purposes to the Entry/Exit System

The Working Party examined the Presidency note (doc. 10720/14) with regard to access to EES for law enforcement authorities (hereinafter LEA) at its aforementioned meeting.

The discussion was focused in particular, on a number of queries addressed to delegations, as spelled out in the Presidency note. The outcome of this debate could be summarised, on the basis of the answers given to the questions under each thematic chapter in the Presidency note, as follows:

A) Purpose limitation

Access for LEA as from the start of the operations of the EES / provision for such access as a secondary objective

A vast majority of delegations (**IT, NL, ES, BG, RO, FR, PL, SK, PT, AT, NO, LV, SI, BE, CZ, HU, SK** confirmed clearly their wish to have access for LEA from the outset of the functioning of EES, as an ancillary objective, in the future Regulation.

DE, SE, DK were not yet in a position to confirm whether they would prefer access for LEA from the beginning of the EES or as of a later stage. **DE** and **SE** pointed out, however, that if they were to accept the access from the outset, they would be positively inclined towards having it as a secondary objective.

Provision for access for LEA only for the purpose of prevention, detection and investigation of terrorist offences and other serious criminal offences

With regard to this question, **IT, NL, ES, BG, RO, FR, SK, PT, NO, SI, CZ, HU** confirmed their agreement with the purpose limitation in question, along the lines with what applies at other large data banks, such as VIS and EURODAC. **PL** pointed out, that, in addition to these purposes (which were acceptable to this delegation), it would be worthwhile to consider allowing access for other objectives (e.g. for tracking down kidnapped or missing persons - especially minors and unaccompanied minors, or persecuted persons who have absconded). **AT, LV, BE** endorsed this suggestion, suggesting that the issue could be further elaborated at a workshop.

Cion expressed strong concerns against expanding the scope of the access beyond the prevention, detection and investigation of terrorist offences and other serious criminal offences. It would be open, however, for discussing this issue (possibly in the context of a workshop). **Cion** also recalled that there are certain other issues which need to be reflected upon, such as the type and the number of fingerprints that would eventually be needed in the context of the EES, and acknowledged that issues such as that regarding minors should be carefully analysed.

B) Authorities, procedure and conditions for access to the EES for LEA

How to decide on the authorities which would be granted access to the EES for LEA and whether such access should be limited to the data that would be strictly necessary

A vast majority of the delegations stressed their wish to maintain their autonomy in appointing the competent authorities for managing EES, along the lines of similar frameworks (VIS and EURODAC - see below for the exact preferences of the delegations which took the floor between the two systems) and in the light of the recent Court of Justice case law.

IT pointed out that examples could be drawn form the nomination of the designated and the verification authorities in the VIS and EURODAC Regulations; **FR, NL, LV** indicated that the relevant provisions of the future EES Regulation could be based, mutatis mutandis, on the EURODAC Regulation, which is more recent than the VIS.

HU emphasised that the EURODAC Regulation may not be the best example to follow for the EES, because it considered as rather complicated and overburdened the procedure adopted in that legal instrument. In the same vein, **NO, BG, ES, RO, DE, PT, SE, CH** pointed out that VIS is much closer to EES as a starting point in order to set the conditions for access than the EURODAC, which was built on a different legal framework.

Access of EUROPOL to the EES

IT, FR, HU, NL, NO, BG, ES, RO, PT, LV, SE, CH confirmed their positive stance concerning granting access for EUROPOL to the EES. As regards the starting point for setting up the conditions for such access, these delegations reiterated their respective preferences for VIS or EURODAC (see above).

C) Data to be accessed

Access of the responsible authorities to all data stored in the EES, or under limitations in the light of the purposes for which access would be granted

ES, NO, BG, AT, NL, PT, IT, LV FR, SK (the last two delegations expressed certain concerns, but were broadly in favour of unlimited access), pointed out that access should be given, in principle, to all data, once the relevant conditions will be met. **IT** further elaborated that the sole possible restriction could be in relation to the scope of the data along the lines of Art. 6 of the VIS Regulation.

RO indicated that access should be given to all data contained in draft Art. 11 of the EES proposal, but needed to further reflect regarding data under draft Art. 12 thereof). **PT**, **DE,** although also favourably inclined towards granting access to all data, pointed out that particular attention should be paid to the relevant case - law of the Court of Justice and the views of the European Ombudsman with regard to the issue (both make explicit reference to providing for access to the data which is strictly necessary).

D) Retention period

ES, IT, AT, RO, BG, PL, NL, FR, PT, LV (the last two delegations with certain qualifications - see below) pointed out that there should be a uniform retention period (of five years, mainly for the sake of consistency with VIS) for all the purposes (included access for LEA) that are likely to be included in the scope of the EES. **SE** was also in favour of a uniform retention period and queried the **Cion,** whether it would be practical to maintain different ones. **Cion** pointed out that a five-year general retention period, which would be modulated on the basis of the access criteria, could be a worthwhile basis for further reflecting on the architecture of such access.

BG, SK proposed clarifying that the five-year period should start from the last exit from the Schengen of the person concerned. In the same context, **SK** suggested examining whether a maximum period from the entry (e.g. twenty years) would be appropriate to provide for. **LV** suggested providing for a ten-year retention period for the visa overstayers.

With regard to the purposes of examining visa applications - point b) and applications for RTP - point c), **PT** suggested providing for a retention period of less than five years (because it will be possible to interview the applicant). **PL** suggested waiting for the Study results before reaching a well-justified decision on the issue. **NL** emphasised that the recent judgment of the Court of Justice in Joint Cases C-293/12 and C-594/12 dealt with a different kind of data from the ones which will be included in the scope of the EES. In this vein, **FI, FR** indicated that a brief retention period (e.g. a six-month one) would not be sufficient for a proper implementation of an access for LEA system in the context of EES.

NO, SK, FR suggested deciding first on the overall length of the retention period for the different types of data and afterwards providing for granting access in accordance with the relevant specific purpose of each request.

CLS emphasised that that the access for LEA should be built in a well-structured way, on the basis of the aforementioned Court ruling (whose subject-matter, as **CLS** acknowledged in agreement with **NL**, has certain differences vis-à-vis the EES scope). **CLS** further recalled the basic parameters of such access regarding the justification (real need) of providing for it, as well as the requirement for clearly-defined conditions and safeguards and for the most suitable means of access for the specific context of EES, taking into account, in particular, the data protection framework. **CLS** also pointed out that the special status of the associate countries should be taken into consideration in the construction of the access for LEA in the EES.

NO, ES underlined that in the future consultation of the EES data base for law enforcement purposes no options should be excluded a priori. **Cion** pointed out that, given that in the EES there will be information which will not be retrievable from other data bases, the remarks of **NO** and **ES** could be taken into consideration, but always in compliance with the data protection principles.

E) Other issues

Delegations agreed with the **Pres.** that there are other issues in relation to access to LEA, as those set out under this paragraph, which could be examined at a later stage by delegations.

By way of conclusion, the **Pres.** asked delegations to submit further suggestions in writing by 30 June 2014.