Council of the European Union

Brussels, 27 April 2018
(OR. en)

8242/18

Interinstitutional Files:
2017/0351 (COD)
2017/0352 (COD)

LIMITE

COSI 87	**DATAPROTECT 71**
FRONT 112	**VISA 97**
ASIM 45	**FAUXDOC 32**
DAPIX 118	**COPEN 116**
ENFOPOL 185	**JAI 338**
ENFOCUSTOM 73	**CT 58**
SIRIS 43	**COMIX 225**
SCHENGEN 15	**CODEC 633**

NOTE

From:	Presidency
To:	Delegations
No. prev. doc.:	15119/17 + COR 1, 15729/17 + COR 1
Subject:	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration) - Presidency non-paper

INTRODUCTION

The Working Party on Information Exchange and Data protection (DAPIX): Interoperability between EU information systems ('the Working Group') carried out an article-by-article examination of the above legislative proposals ('the draft Regulations') during 7 meetings held on 8-9 January, 22-23 January, 15-16 February, 12 March, 26 March and 17-18 April 2018.

In order to provide political guidance on the ongoing examination of the draft Regulations, Ministers held a policy debate at the March JHA Council.

The texts of the two draft Regulations were dealt with in four readings within the Working Group. Revised versions of the draft Regulations, including several compromise and editorial proposals, were presented by the Presidency.

During the Working Group meetings, the impact assessment concerning the two draft Regulations were examined. The EDPS opinion[1] was also presented and discussed.

Europol, Frontex and eu-LISA were invited to attend some of the Working Group meetings in order to reply to specific questions raised by Member States regarding the interoperability between EU information systems.

During the discussions in the Working Group meeting on 17-18 April, a large number of Member States asked the Presidency to convene an additional meeting in DAPIX format before handing over the file to JHA Counsellors level, to further discuss some outstanding issues. The Presidency made the utmost effort to organise a meeting that will take place on 2 May 2018. In order to foster the discussion, several points are outlined below. The Presidency invites you to give feedback on each of these points during the upcoming meeting, so as to facilitate and make more efficient further discussions at JHA Counsellors level.

1. EES PROCESS AND INTEROPERABILITY

In December 2017, Regulation (EU) No 2017/2226 establishing the Entry-Exit System (EES) entered into force. In accordance with that Regulation, a designated Smart Borders Committee within the Commission started working. The Committee gathers Member States' representatives who assist the Commission with the development and technical implementation of the EES. Their expert opinion on practical aspects of the implementation of EES is taken into account in the Committee.

[1] Doc. 8036/18.

In recent Working Group meetings, Member States made a number of proposals for substantial changes in relation to interoperability that will impact the EES process in practice, for example the proposal to change EES to reduce the response time of the systems by parallel searches in VIS and EES, or the cashing of fingerprint identification results.

These suggested changes cannot be achieved through consequential amendments for interoperability purpose. Moreover, such substantial changes made during the development phase of EES may lead to significant delay in the start of operation of the system. At the same time, there is no guarantee that they will deliver the desired result/effect, but it is quite clear that this will lead to higher complexity and additional cost for development.

It should also be noted that the parallel alphanumeric querying of both VIS and EES via the ESP is already provided through the draft Regulations but could be highlighted specifically in the EES and VIS consequential amendments if needed. As regards the cashing of fingerprint identification results in order to be re-used in the MID, this will not be necessary. Indeed, this can be clarified by adding a sentence in Article 27 to the effect that whenever a biometric search (identification) is performed, the individual file is either created or updated, thereby launching the MID process in parallel. This will only be possible when the ESP and the MID are available. Therefore, EES will be developed in the absence of the ESP, of the shared BMS and of the MID/CIR.

To what extent do you agree with the Presidency approach of <u>not</u> considering requests for substantial changes to the EES Regulation during the development phase of the system but clarifying in the EES text how the ESP and MID will interact in the EES process?

2. DATA RETENTION OF RED LINKS

At the Working Group meetings, several delegations asked for a longer data retention period for the red links, while the Commission opposed such proposal. The Presidency has already increased the data retention period by including a new paragraph in Article 23 stipulating that "*where a red link is stored in the MID, the linked data referred to in Article 18(1), (2) and (2a) shall be stored in the CIR for as long as the corresponding data are stored in at least one of the information systems from which the linked data originates*". In effect, this would lead to a data retention period of 10 years, if the data originates from ECRIS. Providing for a fixed period in the legislative act was not chosen as a possible solution because every fixed period should be well-justified in order not to be assessed by the Court of Justice of the European Union as arbitrary and disproportionate. Therefore, the Presidency has suggested linking the retention period with the retention period of the systems from which the data originate.

To what extent do you share the view of the Presidency on a more flexible data retention period? If not, what is the preferred period for data retention of red links in your view? What could be the justification for that term? What other options do you find feasible?

3. AUTOMATED ADDITION OF DATA TO A SIS ALERT IN CASE OF A RED OR WHITE LINK

When querying the SIS Central System, users are informed if red or white links exist. However, when querying N.SIS, police officers may not see that information. There are several possible solutions to this issue that were presented by Member States. One of them includes automated copying of data from CIR to the SIS alert. This raises certainly technical, legal and data protection concerns. For instance, not all Member States operate national SIS copies and there are no guarantees that N.SIS can process an increased volume of data. Moreover, this also raises data protection issues connected to the automatic copying of data, as well as the use of data for a different purpose that require appropriate legislative amendments in different acts.

For these reasons, the Presidency is of the opinion that the automated addition of data to SIS alerts in the case of red or white links is not the best solution. We believe that SIRENE Bureaus may use an additional SIS category data in case of red links to address the issue. That category will also appear when police query N.SIS and consequently full information will be made available through SIRENE.

What other possible solutions to the above-mentioned problem do you envisage?

4. LOGS

In the current Presidency compromise text, information contained in logs is treated differently at different levels. At central level, this information contains only the name of the Member State authority that queried the systems, while the individual user name is not accessible. At national level, Member States shall keep logs of all data processing operations including the name of the Member State authority that queried the systems, as well as the number allowing the identification of the official who carried out the query. Several comments were made by Member States that suggested changes to this set-up. One proposal is based on the idea that logs of data processing operations from intelligence services are to be regarded as sensitive information that should not be made available to the central level. Another suggestion was for logs to make it possible to establish the justification and the identification of the person who consulted or disclosed personal data, and the identity of the recipients of such personal data at national level.

What is your position on the content of logs? What should be the difference in the content of the logs at central and national level?

5. THE ROLE OF THE ETIAS CENTRAL UNIT AFTER THE TRANSITIONAL PHASE

According to the last Presidency compromise text, the ETIAS Central Unit is responsible for the verification of the colour of a link and for fingerprint/ dactyloscopic verification of a hit triggered in different systems during the transitional phase prior to the start of operations of the MID (i.e. dealing with the legacy data). These tasks require significant resources and will have financial impact for Frontex. Some comments were made during the Working Group meetings to provide for the extended involvement of the ETIAS Central Unit for interoperability purpose also after the transitional phase.

To what extent can you agree with the extended involvement of the ETIAS Central Unit for interoperability purpose? What should be the separation of tasks for verification of the colour of a link and dactyloscopic verification of a hit between Member States and the ETIAS Central Unit after the transitional phase? Which other tasks can you identify for Frontex in relation to interoperability?